

**НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет цивільної та господарської юстиції
Кафедра приватного права
Кафедра права інтелектуальної власності та патентної юстиції**

ІТ-ПРАВО, КІБЕРБЕЗПЕКА ТА ШІ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

**МАТЕРІАЛИ
Всеукраїнської наукової конференції**

28 березня 2026 р.

Одеса
Фенікс
2026

За загальною редакцією

доктора юридичних наук, професора **Є. О. Харитонова**,
докторки юридичних наук, професорки **І. В. Давидової**

Упорядники-укладачі:

Давидова І. В. — доктор юридичних наук, професор, професор кафедри приватного права Національного університету «Одеська юридична академія»;

Калітенко О. М. — кандидат юридичних наук, доцент, професор кафедри приватного права Національного університету «Одеська юридична академія»;

Бобейко Н. І. — лаборантка кафедри приватного права Національного університету «Одеська юридична академія».

ІТ-право, кібербезпека та ШІ в умовах гібридної війни :
I-92 матеріали Всеукр. наук. конф. (Одеса, 28 берез. 2026 р.) / за заг. ред.: д-ра юрид. наук, проф. Є. О. Харитонова, д-ра юрид. наук, проф. І. В. Давидової. Одеса : Фенікс, 2026. 300 с. DOI: <https://doi.org/10.32837/11300.33701>

ISBN 978-617-8763-22-0

Збірник містить матеріали доповідей, присвячені актуальним проблемам ІТ-права, кібербезпеки, цифрової трансформації суспільних відносин, правового регулювання штучного інтелекту та захисту інформації в умовах гібридної війни, які були оприлюднені на Всеукраїнській науковій конференції 26 березня 2026 року в Національному університеті «Одеська юридична академія».

Збірник спрямований на ознайомлення науковців, викладачів, здобувачів освіти, практикуючих юристів, фахівців у сфері інформаційних технологій і кібербезпеки з результатами сучасних досліджень щодо правових, організаційних і технологічних аспектів функціонування цифрового середовища в умовах сучасних викликів. Матеріали видання можуть бути використані в науковій, освітній і практичній діяльності, а також під час подальшого вдосконалення правового регулювання цифрових відносин і забезпечення кібербезпеки України.

342.95 : 343.32 (477) : 351.863

Матеріали видано за авторською редакцією.

Повну відповідальність за достовірність і якість поданого матеріалу несуть учасники Всеукраїнської наукової конференції, їхні наукові керівники, рецензенти і структурні підрозділи вищих навчальних закладів та установ, які рекомендували ці матеріали до друку.

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Всеукраїнської наукової конференції

Харитонов Є. О. – завідувач кафедри приватного права Національного університету «Одеська юридична академія», д-р юрид. наук, проф. (голова);

Федотов О. П. – начальник науково-дослідної частини, професор кафедри морського, митного та інформаційного права, д-р юрид. наук, проф. (заступник голови);

Харитонova О. І. – завідувачка кафедри права інтелектуальної власності і патентної юстиції, д-р юрид. наук, проф.;

Галупова Л. І. – доцентка кафедри права інтелектуальної власності і патентної юстиції, канд. юрид. наук, доц.;

Зубар В. М. – професор кафедри приватного права, канд. юрид. наук, проф.;

Калітенко О. М. – професорка кафедри приватного права, канд. юрид. наук, доц.;

Кривенко Ю. В. – доцентка кафедри приватного права, канд. юрид. наук, доц.;

Токарева В. О. – доцентка кафедри приватного права, д-р юрид. наук, доц.;

Бобейко Н. І. – лаборантка кафедри приватного права.

ПЕРЕДМОВА

Стрімкий розвиток інформаційних технологій, цифровізація суспільних відносин, поширення систем штучного інтелекту та зростання кількості кіберзагроз формують нові виклики для правової науки і практики. В умовах повномасштабної збройної агресії проти України та гібридної війни цифровий простір став не лише середовищем комунікації та економічної діяльності, а й ареною протиборства, де поєднуються інформаційні, технологічні, правові та безпекові аспекти. Саме тому особливій актуальності набувають питання правового регулювання інформаційних технологій, забезпечення кібербезпеки, захисту цифрових прав людини та визначення правових засад використання штучного інтелекту.

Збірник тез доповідей Всеукраїнської наукової конференції «ІТ право, кібербезпека та ШІ в умовах гібридної війни» об'єднав результати наукових пошуків провідних учених, викладачів, практикуючих юристів, молодих науковців і студентів закладів вищої освіти України. Конференція стала важливим майданчиком для фахового обговорення сучасних викликів та перспектив розвитку правового регулювання цифрового середовища в умовах воєнного стану та післявоєнного відновлення держави.

Висвітлено широкий спектр актуальних проблем, пов'язаних із розвитком інформаційного суспільства та цифрової трансформації правовідносин. Значна увага приділена питанням правового статусу штучного інтелекту, його участі у приватноправових відносинах, використанню штучного інтелекту у сфері правосуддя, охорони здоров'я, кіберрозвідки та кібербезпеки, а також проблемам відповідальності за шкоду, заподіяну системами штучного інтелекту.

Окремий блок досліджень присвячено викликам кібербезпеки в умовах гібридної війни, зокрема захисту персональних даних, цифрової ідентичності, протидії кібербулінгу, цифровому насиль-

ству, маніпуляціям інформацією, дезінформації та використанню цифрових платформ для вербування. Учасники конференції також розглянули можливості застосування OSINT-інструментів для виявлення фейкових новин, правові аспекти функціонування соціальних мереж, електронної комерції та цифрових комунікацій.

Вагоме місце у збірнику займають дослідження, присвячені цифровим активам, блокчейн-технологіям, смарт-контрактам, цифровим речам, DAO-організаціям, цифровій спадщині та іншим новітнім об'єктам цивільних прав. Автори аналізують трансформацію традиційних правових інститутів під впливом технологічних інновацій, проблеми адаптації цивільного законодавства до нових реалій та перспективи гармонізації національного законодавства із сучасними міжнародними стандартами.

Особливу цінність збірнику надає активна участь студентської молоді, яка представила власне бачення актуальних проблем цифрового права, кібербезпеки та штучного інтелекту. Молоді дослідники продемонстрували високий рівень зацікавленості сучасними тенденціями розвитку права та здатність генерувати нові ідеї щодо вдосконалення правового регулювання суспільних відносин у цифровому середовищі.

Організаційний комітет висловлює щиру вдячність усім учасникам конференції за їхній науковий внесок, активну участь у дискусіях та небайдужість до проблем, що постають перед правовою системою в умовах стрімкого розвитку технологій і триваючої гібридної війни. Переконані, що результати представлених досліджень сприятимуть подальшому розвитку наукової думки, вдосконаленню законодавства та формуванню ефективних механізмів захисту прав людини, суспільства і держави в цифрову епоху.

Бажаємо читачам плідної роботи, нових наукових ідей та подальших успіхів у дослідженні актуальних проблем ІТ-права, кібербезпеки та штучного інтелекту.

Євген ХАРИТОНОВ
Ірина ДАВИДОВА

Берназ-Лукавецька Олена Михайлівна
*кандидатка юридичних наук, доцентка,
доцентка кафедри приватного права Національний університет
«Одеська юридична академія»*

ВИНИКНЕННЯ КРЕДИТНИХ ВІДНОСИН В УМОВАХ ВОЄННОГО СТАНУ

Трансформація інституту кредитних відносин в умовах правового режиму воєнного стану виступає одним із найдинамічніших процесів сучасного цивільного та банківського права. Забезпечення стабільності фінансової системи та захист прав суб'єктів приватного права у цей період потребують гармонійного поєднання традиційних цивільно-правових доктрин із ефективними превентивними механізмами державного регулювання.

У воєнний період підстави виникнення кредитних зобов'язань загалом залишаються подібними до причин мирного часу: необхідність поповнення оборотних коштів, фінансування операційної діяльності компаній, задоволення споживчих потреб та придбання нерухомого чи рухомого майна фізичними особами. Однак, у таких умовах значно змінюється акцент на цільове призначення кредитів. Особливо важливим стає фінансування критично важливої інфраструктури, релокація бізнесу, відновлення пошкоджених виробничих об'єктів та забезпечення продовольчої й енергетичної безпеки країни. Ці процеси спричиняють зміщення приватного інтересу кредиторів і позичальників у сферу суспільної корисності.

Процес формування кредитних відносин зазнає значних змін, особливо на етапах переддоговірних відносин та укладення самого договору. Основною тенденцією є трансформація підходів до оцінки кредитних ризиків. Визначення правоздатності та фінансової стабільності позичальника ускладнюється зовнішніми чинниками, такими як форс-мажорні обставини, втрата майна чи тимчасова окупація територій. У зв'язку з цим до структури кредитного договору додаються спеціальні положення, які охоплюють питання кібербезпеки сторін, впроваджують спеціальні процедури іден-

тифікації та верифікації (в тому числі із використанням дистанційних засобів електронної ідентифікації) та містять чіткі умови щодо форс-мажорів та розподілу можливих ризиків і збитків.

Так, наприклад, Національний банк України (НБУ) впровадив правові механізми, які дають змогу банкам здійснювати повністю дистанційну ідентифікацію та верифікацію клієнтів. Це відкриває можливість для громадян відкривати рахунки чи оформлювати кредитні договори, не відвідуючи фізично банківське відділення. Ось як провідні українські банки застосовують ці інновації на практиці, використовуючи сучасні цифрові інструменти для реалізації такого підходу:

- верифікація через застосунок «Дія» (шеринг цифрових документів) [1]. Клієнт завантажує банківський додаток, проходить реєстрацію та надає згоду на передачу цифрових копій документів, таких як ID-картка або закордонний паспорт, через застосунок «Дія». Завдяки цьому банк одразу отримує зашифрований пакет підписаних даних, який фактично прирівнюється до вручення паперового паспорта касиру.
- дистанційна верифікація через BankID НБУ. А саме, новий банк запитує ідентифікаційні дані клієнта, зокрема ПІБ, паспортні дані та РНОКПП, у банку, де той вже успішно пройшов очну перевірку. Передача цієї інформації здійснюється через захищену Систему BankID НБУ з обов'язковим підтвердженням від самого користувача через його особистий інтернет-банкінг.
- метод розпізнавання обличчя (liveness detection / фотофіксація).

Система пропонує клієнту активувати фронтальну камеру смартфона та виконати кілька простих дій за інструкцією, що відображається на екрані, наприклад, повернути голову, моргнути чи посміхнутися. Штучний інтелект банку аналізує геометрію обличчя, зафіксовану камерою, та зіставляє її з фотографією з ID-картки, отриманою з державних реєстрів [2;3].

У зв'язку з цим до структури кредитного договору впроваджуються спеціальні умови, які враховують аспекти кібербезпеки сторін, особливі механізми ідентифікації та перевірки (зокрема, із активним використанням засобів дистанційної електронної ідентифікації), а також ретельно прописані застереження щодо форс-мажорних обставин і розподілу збитків.

Також, особливість кредитування під час війни полягає в активному державному регулюванні, спрямованому на зменшення фінансового навантаження на позичальника як слабшу сторону договору. Цей захист забезпечується через впровадження матеріально-правових преференцій та процесуальних гарантій.

Один із ключових механізмів – мораторій на нарахування штрафів, пені, інфляційних втрат і трьох відсотків річних за прострочення виконання зобов'язань, встановлений на рівні законодавства.

Ще один важливий аспект – реструктуризація боргових зобов'язань, яка передбачає зміну умов кредитування для постраждалих осіб, що зазнали матеріальних втрат унаслідок воєнних дій. Особлива увага приділяється заставному праву, а саме створенню спеціальних правил щодо звернення стягнення на заставне майно чи іпотеку. Це мінімізує ризик одностороннього відчуження майна позичальника з боку кредитора до завершення періоду воєнного стану або певного часу після його завершення.

Підсумовуючи, хотілося б зазначити, що під час війни кредитні відносини продовжують ґрунтуватися на договірній основі, однак вони функціонують у значно ризикованіших умовах та під сильним регуляторним впливом. Правове забезпечення цих відносин переходить від комерційних пріоритетів до більш комплексного підходу, орієнтованого на захист приватних прав громадян та підтримання макроекономічної стабільності країни.

ЛІТЕРАТУРА:

1. Ukraine's Diia App Updates Diia.Sign Creation with Biometric and NFC Requirements. URL: <https://mezha.net/eng/bukvy/ukraine-s-diia-app-updates-diia-sign-creation-with-biometric-and-nfc-requirements/>

2. Liveness Detection: захист від шахрайства в системах розпізнавання облич. URL: <https://evergreens.com.ua/ua/articles/liveness-detection-in-face-recognition.html>

3. Ю. А. Тимошин, С. П. Орленко. Алгоритм розпізнавання обличчя людей на базі згорткової нейронної мережі. Міжвідомчий науково-технічний збірник «Адаптивні системи автоматичного управління» № 1' (32) 2018 . URL: <https://ela.kpi.ua/server/api/core/bitstreams/2770e38c-c7f1-4d2d-9a2e-8c010a4f87ad/content>

4. Берназ-Лукавецька О.М. Цифрові технології у банківській сфері. Всеукраїнська наукова конференція: *«Одеські грудневі цивілістичні читання: Приватне право, як концепт в умовах війни, людський вимір»*, 12 грудня 2024 року, С. 34-36.

5. Берназ-Лукавецька О.М. Реструктуризація боргу в умовах воєнного стану Всеукраїнська науково-практична конференція *«Приватно-правові та публічно-правові відносини: модернізація розвитку в умовах воєнного стану»*: (м. Кропивницький, 18 жовтня 2024 року). С. 153-155. URL: <https://dnuvs.ukr.education/wp-content/uploads/2025/04/zbirnyk-18-zhovtnya-2024.pdf>

6. Кірсанов О.В. Деякі особливості укладання кредитних договорів : міжнародний досвід. *Науково-практичний журнал «Часопис цивілістики»* № 55, 2024 рік, С. 77-81. URL: <http://clj.nuoua.od.ua/archive/55/15.pdf>

7. Кірсанов О.В. Some features of the credit agreement under the conditions of the martial state. (Деякі особливості кредитного договору в умовах воєнного стану). *Роль та місце правоохоронних органів у розбудові демократичної правової держави*: матер. Міжнар. наук.-практ. інтернет-конф. 29 березня 2024 р. С. 409-412.

Бігняк Олександр Валентинович

доктор юридичних наук

Riga Nordic University

ТРАНСФОРМАЦІЯ ПРАВ УЧАСНИКІВ ТА ПРИХОВАНА ЦЕНТРАЛІЗАЦІЯ У СИСТЕМІ Вч ЯДУВАННЯ DAO

Децентралізовані автономні організації (DAO) позиціонуються в якості альтернативної моделі корпоративного управління, заснованої на токенозованому голосуванні та алгоритмічному виконанні рішень. В той же час, реалії функціонування DAO показують концентрацію фактичного контролю у вузького кола

власників governance-токенів (управлінських токенів), що ставить під сумнів реальну децентралізацію та робить проблему міноритарного захисту більш актуальною.

Мета дослідження – проаналізувати трансформацію прав учасників DAO з урахуванням судової практики та у світлі цивільної доктрини, а також обґрунтувати необхідність встановлення мінімальних стандартів добросовісного управління.

Участь у governance (врядуванні) при розгляді справи *Commodity Futures Trading Commission v. Ooki DAO* розглядалась в якості юридично значущого маркеру організаційної участі, що потенційно посилює ризики відповідальності учасників у конструкціях незареєстрованого об'єднання/партнерства [1]. Суд у справі *Samuels v. Lido DAO et al.* не відхилив позов до великих учасників, виходячи з можливості їх фактичної участі в управлінні через володіння значними пакетами токенів [2]. У Об'єднаному Королівстві Великобританії та Північної Ірландії рішення у справі *Tulip Trading Ltd v. Bitcoin Association for BSV & Others* засвідчило, що питання фідучіарних обов'язків у цифровому середовищі оцінюється в залежності від ступеня контролю та впливу [3].

Таким чином, критерієм, який можна зазначити визначальним, виступає не декларація «децентралізації», а реальний розподіл управлінських повноважень.

Предметні дослідження цифрових прав, облік та обіг яких здійснюється з використанням блокчейну, підкреслюють, що автоматизація управління не усуває потреби правових механізмів довіри та відповідальності [4, с. 44], [6, с. 534-536], [8, с. 12]. Концепція *lex cryptographia* фіксує зміщення регуляції до протоколів, однак не скасовує юридичних ризиків і конфліктів інтересів [4, с. 3-7]. У багатьох DAO модель «один токен – один голос» структурно сприяє концентрації впливу й ризику *governance capture* (узурпації механізмів врядування). Такий висновок узгоджується з теоретичними підходами до форми колективного ухвалення рішень, в яких пріоритет віддається не лише формальній кількості голосів, а і силі відповідних переваг [5, с. 2-4], [7, с. 1136-1137].

Імплементація не лише регуляторних норм, а і правозастосовчої практики щодо DAO у правову систему України потребує цивілістичної кваліфікації governance-токенів (управлінських токенів) і пов'язаних цифрових активів як об'єктів цивільних прав, а також визначення механізмів захисту учасників. Харитонов Є. О. та Харитонova О. І. обґрунтовують значення концепту приватного права, зокрема, як об'єктивної категорії, що має бути модернізованою з метою врахування дихотомії «приватне право – приватні права, оскільки саме останні (як права «приватної особи») належать до базових цінностей відкритого суспільства [9, с. 10]. І такі, наразі, тектонічні зміни щодо розуміння базових понять може стати надійним підґрунтям для належної реалізації приватно-правових механізмів у нових соціально-технологічних умовах, в тому числі у розвитку такого спеціального різновиду приватних прав як то права учасника DAO. Доктринальні підходи до комплексного оновлення цивільного законодавства України, зокрема щодо об'єктів цивільних прав у контексті цифровізації, ґрунтовно висвітлено у праці Н. С. Кузнецової [10, с. 10-12, с. 18]. Наголошується на об'єктивній необхідності приведення усталених цивілістичних конструкцій у відповідність до сучасних соціально-економічних реалій. Одним із ключових аспектів такого оновлення визначено трансформацію розуміння об'єктів цивільних прав під впливом процесів цифровізації. Дослідження розкриває специфіку інтеграції цифрових феноменів (зокрема, об'єктів віртуального середовища, цифрової інформації та віртуальних активів) у систему цивільного права, пропонуючи ефективні правові механізми їх обігу та захисту в умовах формування цифрової економіки. Однак, під час ознайомлення із цим стає очевидним, що цифровий феномен, лише, передбачає існування нової форми інструментів корпоративного управління, використання яких залишає ті ж самі проблеми захисту прав учасників, подібно до використання класичних.

Тобто інтеграція DAO-феномену у приватноправове поле України шляхом визначення правової природи цифрових об'єктів, критеріїв «активного учасника», мінімальних стандартів прозо-

рості та процесуальних моделей представництва DAO у спорах є актуальною [9, с. 5, с. 10-11], [10, с. 11-13, с. 15, с. 85].

На основі проведеного дослідження можемо запропонувати наступні висновки:

1. Судова практика демонструє перевагу функціонального критерію контролю над формальною «децентралізацією», що свідчить про зменшення об'єму суб'єктивних прав учасників [1]–[3].

2. Можна стверджувати про структурну схильність DAO до концентрації governance-влади (влади врядування), що підсилює ризики ігнорування інтересів міноритарних учасників, тоді як нелінійні механізми агрегування преференцій орієнтовані на точніше врахування сили інтересу учасників [5, с. 4-6], [7, с. 1145-1146].

3. Визначено мінімальні стандарти добросовісного управління, а саме: 3.1 прозорість процедур ухвалення рішень; 3.2 існування правил участі та розподілу впливу; 3.3 підзвітність активних учасників або осіб, що здійснюють вирішальний вплив; 3.4 добросовісність реалізації управлінських повноважень; 3.5 належне представництво DAO у приватно-правових і процесуальних відносинах.

ЛІТЕРАТУРА:

1. *Commodity Futures Trading Commission v. Ooki DAO* : U.S. District Court for the Northern District of California. Case No. 3:22-cv-05416. 2022.
2. *Samuels v. Lido DAO et al.* : U.S. District Court for the Northern District of California. Case No. 3:23-cv-06492. 2024.
3. *Tulip Trading Ltd v. Bitcoin Association for BSV & Others* : England and Wales Court of Appeal (Civil Division). EWCA Civ 83. 2023.
4. Wright A., De Filippi P., *Decentralized Blockchain Technology and the Rise of Lex Cryptographia* (March 10, 2015). *SSRN Electronic Journal*. 2015. 2580664.
5. Hassan S., De Filippi P. *Decentralized Autonomous Organization. Internet Policy Review*. 2021. Vol. 10, No. 2. P. 1-10.
6. Werbach K. *Trust, but Verify: Why the Blockchain Needs the Law. Berkeley Technology Law Journal*. 2018. Vol. 33. P. 487–550.
7. Buterin V., Hitzig Z., Weyl E. G. *Liberal Radicalism: A Flexible Design for Philanthropic Matching Funds. American Economic Review*. 2019. Vol. 109, No. 4. P. 1136–1167.

8. Zetzsche D. A., Buckley R. P., Arner D. W. The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. *University of Illinois Law Review*. 2018. No. 4. P. 1361–1406.

9. Харитонов Є. О., Харитонova О. І. Концепт «приватне право» та проблеми його реалізації. *Часопис цивілістики*. 2021. Вип. 41. С. 5–11.

10. Кузнєцова Н. С., Довгерт А. С., Хоменко М. М. Концепція оновлення Цивільного кодексу України: проблеми і підходи. Київ : АртЕк, 2020. 128 с.

Брага Аліна Анатоліївна

аспірантка кафедри приватного права

Національного університету "Одеська юридична академія"

ЦИФРОВА СПАДЩИНА, ЯК ВИКЛИК ДОКТРИНИ НЕСПАДКОВУВАНOSTІ ОСОБИСТИХ НЕМАЙНОВИХ ПРАВ

Сучасний етап розвитку приватного права характеризується глибинними трансформаціями, зумовленими цифровізацією суспільних відносин, що, у свою чергу, актуалізує необхідність переосмислення усталених цивілістичних категорій, зокрема у сфері спадкового права. Одним із найбільш дискусійних феноменів виступає цифрова спадщина, яка формується на перетині класичних правових конструкцій та новітніх технологічних реалій, що вимагає розроблення належного теоретико-методологічного підґрунтя її дослідження. У цьому контексті першочергового значення набуває уточнення понятійно-категоріального апарату, оскільки відсутність усталених дефініцій ускладнює як наукове осмислення, так і нормативне врегулювання відповідних правовідносин.

У науковій літературі цифрова спадщина зазвичай розглядається як сукупність цифрових активів, прав та інтересів, що належали особі за життя та підлягають передачі або управлінню після її смерті. [1; 2] Водночас таке визначення не є вичерпним, оскільки воно не враховує складну правову природу окремих елементів цифрового середовища, зокрема персональних даних, цифрової ідентичності, віртуальних облікових записів, результатів творчої діяльності, створених із використанням технологій штучного ін-

телекту, а також цифрових слідів, що формують так звану «постмортальну цифрову присутність» особи. Таким чином, цифрова спадщина повинна розглядатися не лише як об'єкт спадкового правонаступництва, але і як комплексне правове явище, що охоплює як майнові, так і немайнові елементи.

Методологічно дослідження цифрової спадщини потребує застосування міждисциплінарного підходу, що поєднує інструментарій цивільного права, інформаційного права, права інтелектуальної власності, а також елементів публічного права, зокрема у сфері захисту персональних даних. Такий підхід обумовлений тим, що цифрові активи нерідко мають змішану правову природу: з одного боку, вони можуть виступати об'єктами майнових прав (наприклад, криптоактиви, цифрові об'єкти в онлайн-середовищах), а з іншого – бути тісно пов'язаними з особистістю суб'єкта (акаунти в соціальних мережах, електронне листування, цифровий профіль), що традиційно відноситься до сфери особистих немайнових прав.

Особливої уваги заслуговує категорія цифрової ідентичності, яка у сучасних умовах набуває статусу самостійного об'єкта правового регулювання. Цифрова ідентичність охоплює сукупність даних, що ідентифікують особу в електронному середовищі, включаючи облікові записи, цифрові аватари, історію онлайн-активності, а також алгоритмічно сформовані профілі, створені з використанням технологій штучного інтелекту. У цьому аспекті постає питання про можливість та межі правонаступництва щодо таких елементів, оскільки вони поєднують у собі як майнові, так і глибоко персоналізовані характеристики.

Міжгалузевий характер проблематики цифрової спадщини проявляється також у необхідності врахування технологічних особливостей функціонування цифрових платформ та сервісів, які встановлюють власні правила доступу, передачі або блокування облікових записів після смерті користувача. У багатьох випадках саме умови користування (terms of service) визначають долю цифрових активів, що фактично призводить до «приватизації» регу-

лювання спадкових відносин транснаціональними корпораціями. Це, у свою чергу, ставить під сумнів традиційні засади автономії волі та рівності сторін у цивільному праві, оскільки користувач зазвичай позбавлений реальної можливості впливати на зміст таких умов.

У теоретичному вимірі дослідження цифрової спадщини також потребує переосмислення співвідношення між об'єктами цивільних прав та їх цифровими формами існування. Класичне розмежування речей, майнових прав та немайнових благ виявляється недостатнім для адекватного опису цифрових явищ, які можуть одночасно мати ознаки інформації, послуги та об'єкта права. Це обумовлює необхідність розроблення нових підходів до класифікації об'єктів цивільних прав із урахуванням їх цифрової природи.

Таким чином, теоретико-методологічні засади дослідження цифрової спадщини повинні базуватися на комплексному, системному та міжгалузевому підході, що дозволяє інтегрувати досягнення класичної цивілістичної доктрини з новими викликами цифрової епохи. Формування чіткого понятійно-категоріального апарату у цій сфері є необхідною передумовою для подальшого розвитку як наукових досліджень, так і ефективного нормативного регулювання відносин, пов'язаних із переходом цифрових активів та прав після смерті особи.

У контексті окреслених теоретико-методологічних засад особливої актуальності набуває проблема трансформації класичної доктрини неспадковуваності особистих немайнових прав під впливом цифровізації, яка істотно змінює саму природу зв'язку між особою та відповідними нематеріальними благами. Традиційно у цивільному праві виходять із того, що особисті немайнові права є тісно пов'язаними з особистістю їх носія, мають абсолютний, невідчужуваний та непередаваний характер і, як наслідок, припиняються зі смертю особи. Водночас розвиток цифрового середовища, у якому значна частина особистісної активності суб'єкта переноситься в онлайн-простір, зумовлює формування нових правових ситуацій, у яких повне припинення таких прав виглядає не лише функціонально неефективним, але й соціально небажаним.

Цифрові акаунти, електронне листування, профілі у соціальних мережах, хмарні сховища та інші елементи цифрової присутності особи містять значний обсяг інформації, що має як особистісне, так і майнове значення, а також безпосередньо пов'язана з інтересами третіх осіб – членів сім'ї, спадкоємців, контрагентів. У зв'язку з цим постає питання про можливість виокремлення у структурі особистих немайнових прав певних елементів, які, не змінюючи їх загальної правової природи, можуть набувати обмеженої спадкової трансмісії у вигляді похідних правомочностей. Йдеться, насамперед, про такі функціональні правомочності, як право доступу до цифрового акаунта померлої особи, право управління його вмістом, право на видалення інформації або, навпаки, на збереження та меморіалізацію цифрового профілю.

Зазначені правомочності не можуть розглядатися як пряме спадкування особистих немайнових прав у їх класичному розумінні, однак вони формують специфічний правовий інститут, який доцільно кваліфікувати як постмортальні цифрові правомочності, що мають допоміжний, сервісний характер і спрямовані на забезпечення належного балансу між пам'яттю про особу, її прижиттєвою волею та інтересами близьких осіб. У цьому сенсі відбувається своєрідна функціональна трансформація особистих немайнових прав, коли їх ядро залишається неспадковуваним, але окремі аспекти реалізації після смерті особи можуть бути делеговані або передані у межах спеціального правового режиму.

Особливої складності ця проблематика набуває у зв'язку з тим, що цифрові платформи фактично встановлюють власні правила щодо долі акаунтів померлих користувачів, передбачаючи, наприклад, можливість призначення так званих «контактів-наступників» або переведення профілю у меморіальний режим. Такі механізми, з одного боку, сприяють реалізації інтересів родичів та збереженню цифрової спадщини, але, з іншого боку, залишаються поза межами національного правового регулювання та ґрунтуються на договірних умовах, які не завжди відповідають принципам цивільного права. У результаті виникає ситуація, коли саме приватні корпорації визначають обсяг і зміст постмортальних

правомочностей, що ставить під сумнів ефективність державного правового регулювання у цій сфері.

Водночас не можна ігнорувати ризики, пов'язані з надмірною «спадковізацією» особистих немайнових прав, оскільки це може призвести до порушення принципу поваги до особистості померлого, зокрема у випадках, коли спадкоємці отримують доступ до конфіденційної інформації або здійснюють дії, які суперечать прижиттєвій волі особи. Саме тому ключовим завданням сучасної цивілістичної доктрини є вироблення таких підходів, які дозволяють поєднати збереження фундаментального принципу неспадковуваності особистих немайнових прав із необхідністю адаптації правового регулювання до реалій цифрового суспільства.

У цьому аспекті перспективним видається запровадження конструкції прижиттєвого волевиявлення особи щодо долі її цифрових активів і акаунтів після смерті, що може бути реалізовано як через інструменти спадкового права (заповіт, спадковий договір), так і через спеціальні цифрові сервіси. Такий підхід дозволяє забезпечити пріоритет автономії волі особи та мінімізувати конфлікти між спадкоємцями, а також між спадкоємцями та постачальниками цифрових послуг.

Отже, сучасні виклики для доктрини неспадковуваності особистих немайнових прав полягають не у її повному запереченні, а у необхідності її гнучкої трансформації, що передбачає виокремлення та нормативне закріплення обмежених постмортальних правомочностей щодо цифрових об'єктів. Такий підхід дозволяє зберегти ціннісне ядро класичної цивілістичної доктрини, водночас забезпечуючи її відповідність умовам цифрової епохи та інтегруючи у сферу ІТ-права і правового регулювання.

ЛІТЕРАТУРА:

1. Загоруй Л. М., Загоруй І. С. Цифрова спадщина: проблеми формування і перспективи. *Актуальні проблеми права: теорія і практика*. 2024. № 1 (47). С. 71-82.
2. Вовк М. З. Особливості правового регулювання спадкування цифрових активів та інтелектуальної власності в умовах розвитку блокчейн-технологій *Академічні візії*. 2024. Вип. 35. DOI: <https://doi.org/10.5281/zenodo.13903131>

Булеца Сібілла Богданівна
*докторка юридичних наук, професорка,
завідувачка кафедри цивільного права та процесу
ДВНЗ «Ужгородський національний університет»*

МІСЦЕ АНАТОМІЧНИХ МАТЕРІАЛІВ ЛЮДИНИ В МОДЕЛЬНИХ ПРАВИЛАХ РЕЧЕВОГО ПРАВА

Стрімкий розвиток біомедичних технологій, трансплантології, репродуктивної медицини та генної інженерії ставить перед сучасним правом нові виклики, які вимагають адекватного цивільно-правового регулювання. На сьогодні чинний Цивільний кодекс України (далі – ЦК України), попри свою прогресивність на момент прийняття у 2003 році, демонструє правовий аскетизм щодо об'єктів біомедичного характеру. Він фактично не містить положень, які б чітко визначали правовий статус анатомічних матеріалів людини (органів, тканин, клітин, ембріонів) як специфічних об'єктів цивільних прав. Це створює значний правовий вакуум у критично важливих питаннях, таких як правонаступництво, розпорядження біоматеріалами та захист прав особи на власні біологічні об'єкти після їх відокремлення від тіла.

У зв'язку з цим, обґрунтовано необхідність використання положень Модельних правил (Глава 15-1) як фундаментального кроку для гармонізації українського законодавства із сучасними біоетичними та міжнародними правовими стандартами. Актуальність теми зумовлена також здійсненням рекодифікації Цивільного кодексу, де межа між суб'єктом права та об'єктом права стає дедалі тоншою, а біологічна сутність людини потребує чіткої юридичної регламентації, зокрема в межах речового права.

Чинне законодавство України, закріплюючи у статті 177 ЦК України невичерпний перелік об'єктів цивільних прав (речі, інше майно, майнові права, результати робіт, послуги, результати інтелектуальної, творчої діяльності, інформація, а також інші матеріальні та нематеріальні блага), не надає прямої відповіді щодо правового режиму анатомічних матеріалів. Стаття 179 ЦК України визначає річчю предмет матеріального світу, щодо якого

можуть виникати цивільні права й обов'язки, проте традиційний поділ об'єктів цивільних прав на речі та нематеріальні блага виявився недостатнім для адекватного регулювання відносин, що виникають з приводу відокремлених частин людського організму. Відсутність чіткої самостійної категорії «анатомічні матеріали» створює правову невизначеність у питаннях володіння, розпорядження та правонаступництва щодо біологічних об'єктів.

Р.А. Майданик справедливо зазначає, що з метою системного і більш гнучкого регулювання відносин щодо анатомічних матеріалів людини в праві України доцільно передбачити їхнє широке (універсальне) трактування як будь-якого біологічного матеріалу тіла людини, включаючи людські тканини та клітини, гамети, ембріони та плоди, а також речовини, видобуті з них, незалежно від ступеня їхнього оброблення. У цьому контексті, пропонується Модельними правилами Глава 15-1 «Анатомічні матеріали людини» (статті 200-1–200-6) є не просто технічним доповненням, а глибоким правовим переосмисленням того, як право має реагувати на автономне існування частин людського організму. Це важливий крок у напрямку забезпечення правового захисту анатомічних матеріалів та визначення їхнього статусу в українському правовому просторі, що сприятиме розвитку біомедичної галузі та забезпечить більш чітке цивільно-правове регулювання.

Анатомічні матеріали мають унікальну природу, що вимагає особливого підходу до визначення їхнього місця в системі речових прав. Традиційні категорії речових прав, що регулюють обіг звичайних речей, не завжди повною мірою відповідають складнощам, пов'язаним з анатомічними матеріалами, враховуючи їхнє походження, призначення та потенційні етичні, моральні та правові обмеження. Проблематика визначення правового статусу анатомічних матеріалів виникає з питання, чи є вони «речами» в цивілістичному розумінні. З одного боку, вони можуть бути фізично відокремлені, зберігатися, транспортуватися та використовуватися в певних цілях. З іншого боку, їхній зв'язок з людським організмом, етичні аспекти та обмеження щодо комерційного обігу часто виводять їх за рамки звичайних товарів.

Варто відзначити, що відсутня єдина правова концепція на міжнародному рівні: національне законодавство різних країн демонструє різноманітність підходів до регулювання обігу анатомічних матеріалів, при цьому деякі країни допускають обмежений комерційний обіг, інші суворо забороняють його (як, наприклад, принцип «ні власності» у Франції чи аналогічні закони в Іспанії). Специфічні функції та призначення анатомічних матеріалів (наукові дослідження, медична освіта, трансплантація, діагностика) відрізняються від типового споживання або використання звичайних речей.

Таким чином, анатомічні матеріали не можуть бути повноцінно інтегровані в традиційну систему речових прав як звичайні речі. Їхній унікальний статус, етичні аспекти та суспільне значення вимагають створення спеціального правового режиму. Цей режим має бути гібридним, поєднуючи:

1. Принципи вилучення з комерційного обігу для органів та тканин для трансплантації, що були вилучені з людського організму та зберігають життєздатність. Їхній обіг має бути регламентований законом, обмежений цілями трансплантації та підпорядкований принципам безоплатності, добровільності та анонімності донора. Права на такі матеріали не можуть бути об'єктом відчуження, застави або інших цивільно-правових угод, що мають на меті отримання прибутку. Вони мають розглядатися як об'єкти, що перебувають під особливим державним контролем і регулюються нормами публічного права.

2. Спеціальне регулювання для наукових та освітніх матеріалів, діагностики (наприклад, біологічні зразки, препарати, фрагменти тканин, що втратили життєздатність). Цей режим «*sui generis*» передбачає допуск обігу таких матеріалів лише для некомерційних цілей, за обов'язкової наявності інформованої згоди донора, конфіденційності, анонімності, встановленої відповідальності та державного контролю.

Такий підхід дозволить уникнути комерціалізації людського тіла та його частин, одночасно сприяючи розвитку науки та меди-

щини. Особливої уваги заслуговує стаття 200-3 Модельних правил, яка регулює статус штучно створених матеріалів, визначаючи їх як обмежені в обороті речі, що містять генетичну інформацію. Це є прямим обґрунтуванням їхнього місця в системі речових прав, адже такі об'єкти створюються поза організмом, є результатом людської праці та технологій, а отже, тяжіють до категорії майна, хоча й вимагають захисту конфіденційності генетичного коду.

Наявні в нормативних актах визначення анатомічних матеріалів є фрагментарними. Стаття 200-1 Модельних правил вперше дає легальне визначення анатомічного матеріалу як об'єкта цивільних прав, охоплюючи не лише органи, тканини та клітини, але й штучно створені матеріали та фетальні субстанції, що відокремлені на законних підставах. Це важливе доповнення, оскільки відокремлена частина тіла, що зберігається в кріобанку або транспортується для трансплантації, фактично стає «річчю», хоча й з особливим статусом. Включення штучно створених анатомічних матеріалів відповідає викликам сучасної науки (виращування органів *in vitro*). Закріплення цієї норми у ЦК України дозволить чітко ідентифікувати суб'єктів та зміст прав, що виникають з моменту відокремлення матеріалу від організму.

Важливо, що стаття 200-5 Модельних правил прямо забороняє використовувати анатомічні матеріали як предмет забезпечення зобов'язань (застави), а також купівлю-продаж органів. Це не виключає їх із системи цивільного права, а лише встановлює спеціальний режим оборотоздатності, подібний до регулювання культурних цінностей або зброї. Обґрунтування місця цих матеріалів у системі речових прав базується на їхній фізичній дискретності (фізична відмежованість), цінності (медичній, науковій) та підвладності (можливість фізичного контролю). Без включення цих положень до ЦК України величезний масив відносин – від біобанкінгу до сурогатного материнства та регенеративної медицини – залишається поза межами системного правового регулювання.

Головною науковою проблемою є визначення місця анатомічних матеріалів у системі об'єктів цивільних прав. Модельні прави-

ла пропонують диференційований підхід, де стаття 200-2 вводить ключову для цивілістики концепцію дуалізму, визначаючи анатомічний матеріал одночасно як матеріальне немайнове благо та, за певних умов, як річ. Це розв'язує давню дискусію про «комерціалізацію тіла». Статус речі надається об'єктам, відокремлення яких є безпечним або відбувається природним шляхом (волосся, слина, молочні зуби, репродуктивні клітини). Визнання їх річчю дозволяє легалізувати цивільний оборот та застосовувати до них положення про речові права, що відповідає реальним потребам суспільства (наприклад, донорство сперми на договірній основі, продаж волосся, послуги кріобанків тощо).

Для анатомічних матеріалів, що використовуються для наукових досліджень, медичної освіти, діагностики (наприклад, біологічні зразки, препарати, фрагменти тканин, що втратили життєздатність), а також ті, що є продуктами відокремленими від тіла і не можуть бути трансплантовані, доцільно ввести особливий режим «*sui generis*». Цей режим має передбачати допуск обігу таких матеріалів лише для некомерційних цілей, з обов'язковою наявністю інформованої згоди донора, забезпеченням конфіденційності та анонімності, встановленням відповідальності та державним контролем. Проте для органів та тканин, що мають критичне значення для життя людини та глибокий зв'язок з ідентичністю особи (органи для трансплантації – серце, нирки), зберігається статус матеріального немайнового блага, що підкреслює їх зв'язок з людською гідністю, обмежує в обороті та виключає комерціалізацію.

Стаття 200-3 Модельних правил вводить категорію штучно створених матеріалів як обмежених в обороті речей. Оскільки такі об'єкти створюються поза тілом людини, вони за своєю суттю є результатом людської діяльності (технологічного процесу), що ще сильніше наближає їх до категорії майна. Однак наявність у них генетичного коду особи зумовлює необхідність спеціального режиму конфіденційності, що має бути відображено у ЦК.

Розглядаючи статтю 200-5 Модельних правил, ми бачимо чітку структуру здійснення прав володіння, користування та роз-

порядження, які встановлюють, що розпорядження здійснюють особи, пов'язані з об'єктом (донор, родичі), а фактичне володіння та використання – суб'єкти господарювання (клініки, лабораторії). Це класична розщеплена модель правомочностей, характерна для речових об'єктів. Обґрунтування місця анатомічних матеріалів у системі речових прав базується на їхній фізичній дискретності.

Анатомічні матеріали займають проміжне місце між суб'єктом (людиною) та об'єктом (реччю). Закріплення їх у системі речових прав обґрунтовується такими фактами:

1. Після відокремлення від організму матеріал стає фізично самостійним об'єктом.

2. Суб'єкти (медичні заклади, біобанки) здійснюють фактичне володіння цими об'єктами на законних підставах. Без цивільно-правової легалізації цього володіння будь-яке пошкодження матеріалу (наприклад, через відключення електрики в кріобанку) важко кваліфікувати як шкоду майну.

3. Модельні правила (ст. 200-5) прямо забороняють використовувати анатомічні матеріали як предмет застави (забезпечення виконання зобов'язань). Це специфічне «речове право», де пріоритетом є воля донора, а не ринкова вартість об'єкта.

4. Метою такого специфічного речового права є не майнова вигода, а збереження життя та здоров'я.

5. Стаття 200-2 Модельних правил прямо передбачає можливість переходу матеріалів у порядку спадкування. Це неможливо без визнання їх об'єктами речових прав.

Стаття 200-4 Модельних правил щодо ембріонів *in vitro* є революційною, оскільки вона виводить ці об'єкти з правового вакууму, називаючи їх матеріальним немайновим благом, яке може бути предметом договорів зберігання чи перевезення. Це де-факто визнання за ними статусу об'єкта, що перебуває під правовим пануванням певних осіб, що є фундаментальною ознакою речового права. Єдиним нормативним актом, що містить визначення ембріону, є Закон України «Про заборону репродуктивного клонування людини». На стадії створення ембріону *in vitro* та його кріокон-

сервації він є об'єктом цивільних прав, оскільки в стані кріоконсервації ембріон не розвивається, у ньому не відбувається жодних біологічних змін і процесів. Стаття 200-4 Модельних правил вирішує одну з найбільш контроверсійних проблем сучасності, визнаючи ембріон *in vitro* як матеріальне немайнове благо. Це дозволяє легалізувати договори щодо їх зберігання та транспортування, водночас забороняючи комерційне використання та клонування. Таке закріплення у ЦК захистить ембріон від кваліфікації як «товару», але надасть йому чітке місце серед об'єктів права.

Відсутність чітких норм у ЦК стосовно новітніх викликів біомедичних технологій призводить до того, що суди змушені використовувати аналогію права, системні прогалини чинного цивільного законодавства щодо визначення правового статусу репродуктивного матеріалу та ембріонів проявляються у двох гострих ситуаціях:

1. Розлучення подружжя зі спірною долею ембріонів *in vitro*: без визнання ембріона «річчю» або особливим благом, суди стикаються з правовим вакуумом. Стаття 200-4 Модельних правил, визначаючи ембріон як матеріальне немайнове благо, дозволяє вирішувати такий спір через призму особистих прав донорів, а не за механізмами поділу майна, одночасно легітимізуючи укладення договорів щодо розпорядження ними.

2. Спадкування репродуктивного матеріалу загиблого військовослужбовця: чинне законодавство України часто перешкоджає реалізації права дружини загиблого воїна на використання його кріоконсервованої сперми, оскільки репродуктивний матеріал не є об'єктом спадкування. Частина 1 статті 200-2 Модельних правил допускає перехід анатомічних матеріалів у порядку спадкування, якщо це не заборонено законом, що створює законну підставу для реалізації останньої волі померлого та дозволяє вирішувати ці питання, що стали особливо актуальними в умовах воєнного стану.

Важливо підкреслити, що імплементація норм Модельних правил до Цивільного кодексу України жодним чином не означає

легалізацію ринку органів чи дегуманізацію цивільних відносин. Навпаки, стаття 200-5 Модельних правил встановлює чітке правове розмежування стосовно поділу між неприпустимою комерціалізацією та правомірною компенсацією. Зокрема, під суворою заборонаю залишаються будь-які правочини, що мають на меті отримання прямої майнової вигоди від відчуження анатомічних матеріалів. Водночас законним визнається механізм компенсації, що передбачає виключно відшкодування виправданих витрат донора (втраченого заробітку, витрат на медичне обслуговування, реабілітацію та транспортування). Таке розмежування остаточно обґрунтовує унікальну специфіку анатомічних матеріалів як об'єктів із спеціальним правовим режимом. У цій площині класичне право власності перестає бути абсолютним і стає «обтяженим» пріоритетною соціальною та етичною функцією, що виключає можливість розгляду частин людського тіла як звичайного товару та гарантує дотримання принципу поваги до людської гідності в межах цивільного обороту.

Підсумовуючи викладене, слід зазначити, що імплементація Глави 15-1 Модельних правил у Цивільний кодекс України є безальтернативним кроком для правової держави 2026 року, що забезпечить належний захист генетичної інформації та прав особи на біологічні зразки, які є невід'ємною частиною сучасної концепції прав людини. Це дозволить забезпечити права громадян на розпорядження власним біологічним матеріалом, подолати правову невизначеність у сфері біомедицини, захистити інвестиції у галузі біотехнологій та створити прозорі правила для медичних закладів та кріобанків. Анатомічні матеріали людини мають бути закріплені як особлива категорія об'єктів цивільних прав, що поєднують ознаки матеріального світу та особистісних благ. Запровадження категорій «матеріальне немайнове благо» та «річ» (для певних видів матеріалів) дозволить збалансувати приватні інтереси (розпорядження власним тілом) та публічний порядок (заборона торгівлі органами). Визнання певних біоматеріалів «речами» дозволить легалізувати та впорядкувати існуючий цивільний обо-

рот, захистивши при цьому інтереси особи. І тим самим система речових прав має бути доповнена нормами про володіння та розпорядження анатомічними матеріалами, що базуються на принципі некомерційності (альтруїзму) та інформованої згоди.

Вовчок Руслан Володимирович

аспірант кафедри приватного права

Національного університету «Одеська юридична академія»

КІБЕРІНЦИДЕНТИ ЯК ОБСТАВИНИ НЕПЕРЕБОРНОЇ СИЛИ В ІТ-ДОГОВОРАХ

Кіберінцидент як підстава звільнення від відповідальності за порушення договірної зобов'язання є одним із найбільш дискусійних і методологічно не вирішених питань сучасного договірної права. Масштабні кібератаки – NotPetya (2017), атака на Colonial Pipeline (2021), інциденти з SolarWinds і Log4j, а також систематичні атаки на критичну інфраструктуру України після 24 лютого 2022 року – переконливо продемонстрували: кіберінцидент здатний паралізувати виконання договірних зобов'язань у спосіб, не менш руйнівний, ніж фізична катастрофа або збройний конфлікт [1, с. 117]. Однак, на відміну від повені, землетрусу або воєнних дій, кіберінцидент є явищем, чия правова кваліфікація як «обставини непереборної сили» у розумінні статті 617 ЦК України і відповідних договірних застережень залишається предметом гострої доктринальної дискусії і непослідовної судової практики. Центральна проблема полягає у принциповій відмінності кіберінциденту від класичних форс-мажорних обставин: він може бути прогнозованим, може бути наслідком недостатньої технічної захищеності сторони-порушника, може бути організований конкурентом або третьою особою – і у кожному з цих випадків відповідь на питання «чи є кіберінцидент форс-мажором?» має бути принципово різною.

Доктрина форс-мажору – непереборної сили як підстави звільнення від відповідальності за порушення зобов'язання – є однією з найбільш стійких конструкцій цивільного права, що бере

початок ще від римського принципу «*casus a nullo praestantur*». Стаття 617 ЦК України відтворює класичні ознаки непереборної сили: надзвичайність (виняткова, непередбачувана подія), невідворотність (неможливість запобігти наслідкам за будь-яких умов) і об'єктивність (незалежність від волі сторони-боржника). Торгово-промислова палата України уповноважена засвідчувати обставини форс-мажору, що надає процесуального значення факту настання таких обставин у договірних спорах.

Проте класична доктрина формувалась для природних і соціальних катастроф, де всі три ознаки є самоочевидними: землетрус є надзвичайним, невідворотним і об'єктивним явищем за визначенням. Кіберінцидент порушує цю тріаду в усіх трьох вимірах одночасно: він може бути частково передбачуваним через оцінку вразливостей; його наслідки можуть бути мінімізовані або навіть відвернуті належними заходами кіберзахисту; і він нерідко є продуктом дій людини – хакера, конкурента або іноземної спецслужби, – що розмиває «об'єктивність» події. Саме ця тріада методологічних проблем робить правову кваліфікацію кіберінцидентів нетривіальним завданням.

Методологічно вирішальним кроком у правовій кваліфікації кіберінцидентів як форс-мажору є побудова диференційованої класифікації за сукупністю критеріїв, що визначають юридичну природу конкретного інциденту. Доречним є, на нашу думку, запропонувати чотири категорії кіберінцидентів за критерієм форс-мажорності. По-перше, масштабні атаки державного або квазідержавного рівня (*nation-state attacks*) – на зразок NotPetya або атак на КІАС у 2022 році, – що мають ознаки воєнної операції і завдають шкоди незалежно від рівня захищеності жертви: такі інциденти найбільш відповідають критеріям форс-мажору і мають кваліфікуватись як такі за наявності зв'язку між загальним геополітичним контекстом і конкретним порушенням зобов'язання. По-друге, масові автоматизовані атаки (*ransomware*, *DDoS*-кампанії), що вражають тисячі суб'єктів одночасно незалежно від їхнього рівня захисту: їх кваліфікація як форс-мажору є обґрунтованою

лише за умови, що сторона-боржник вжила розумних заходів кіберзахисту відповідно до галузевих стандартів. По-третє, цільові атаки на конкретну організацію (targeted attacks, АРТ): їх форс-мажорна кваліфікація є найбільш сумнівною, оскільки адресний характер атаки свідчить про наявність конкретного ризику, управління яким є прямим обов'язком суб'єкта. По-четверте, не можуть визнаватися форс-мажорними обставинами інциденти, що стали наслідком експлуатації відомих вразливостей програмного забезпечення, якщо відповідна сторона мала можливість своєчасно усунути такі вразливості або вжити необхідних заходів захисту, але не зробила цього.

Центральним правовим питанням при оцінці кіберінциденту як форс-мажорної обставини є встановлення того, чи вжила сторона-боржник усіх розумно очікуваних заходів для запобігання інциденту або мінімізації його наслідків. За своєю суттю цей критерій є функціональним аналогом стандарту належної обачності, традиційно застосовуваного у цивільному праві, однак у сфері цифрових відносин він потребує конкретизації з урахуванням сучасних технічних та організаційних вимог кібербезпеки.

Правова наука і судова практика починають формувати контури цього стандарту: він включає відповідність кращим галузевим практикам кіберзахисту (ISO/IEC 27001, NIST Cybersecurity Framework, відповідні стандарти SOC 2), наявність і реалізацію плану реагування на інциденти (Incident Response Plan), регулярне оновлення програмного забезпечення і усунення відомих вразливостей, а також сегментацію мережі і резервне копіювання критичних даних. Відсутність будь-якого з цих елементів є підставою для висновку про те, що сторона не вжила розумних заходів і тому не може посилатись на форс-мажорний характер інциденту [2, с.276]. Практично важливим є питання про те, чи має цей стандарт бути закріплений у самому ІТ-договорі через спеціальне кіберзастереження, чи він застосовується незалежно від договірної регулювання як об'єктивний правовий критерій: порівняльний аналіз свідчить на користь гібридного підходу – стандарт існує

об'єктивно, але договірне кіберзастереження може конкретизувати і підвищити його рівень для конкретних відносин [3].

Практика розгляду спорів, пов'язаних із кіберінцидентами як підставою форс-мажору, є поки що обмеженою, але надзвичайно показовою. Найрезонанснішим і доктринально значущим є судовий процес у справі *Merck & Co. v. Ace American Insurance Co.* (Верховний суд Нью-Джерсі, 2023) у зв'язку з атакою NotPetya: страховик спочатку відмовив у відшкодуванні збитків на суму 1,4 млрд доларів, посилаючись на застереження про «воєнні дії» у страховому полісі, однак суд вирішив спір на користь позивача, вказавши, що застереження про воєнні дії вимагає оголошеного чи формально визнаного збройного конфлікту і не охоплює автоматично кібератаки державного рівня [4]. В Україні ТПП видавала сертифікати форс-мажору у зв'язку із кібератаками на державні інформаційні системи і критичну інфраструктуру після 24 лютого 2022 року, однак критерії, за якими конкретний кіберінцидент визнається форс-мажором, залишаються непублічними і непрозорими. Вітчизняна судова практика у цій сфері є мінімальною і непослідовною, що у поєднанні із зростаючою кількістю ІТ-договорів і кіберінцидентів утворює системну прогалину правозастосування.

У відсутність достатньої законодавчої і судової визначеності щодо правового режиму кіберінцидентів у ІТ-договорах центральним інструментом управління цим правовим ризиком є спеціальне договірне кіберзастереження (*cyber force majeure clause*) – нормативна конструкція, що конкретизує умови, за яких кіберінцидент звільняє сторону від відповідальності або змінює умови виконання договору. Оптимально сконструйоване кіберзастереження має вирішувати п'ять ключових питань:

1. визначення кіберінцидентів, що охоплюються застереженням, – через таксономію видів атак із прямим посиланням на галузеві класифікатори;
2. встановлення стандарту кіберзахисту, дотримання якого є умовою застосування застереження;
3. процедура повідомлення контрагента про настання інциденту і строки такого повідомлення;

4. правові наслідки кіберінциденту – повне звільнення, часткове звільнення, призупинення виконання або зміна умов договору;

5. розподіл ризиків між сторонами у разі, коли кіберінцидент стосується субпідрядника або постачальника хмарних послуг, а не безпосередньо сторони договору.

Відсутність чіткого кіберзастереження у IT-договорі є не нейтральним упущенням, а принциповим вибором на користь невизначеності, що у разі виникнення спору перекладає вирішення всіх цих питань на суд, який, як правило, не має ані спеціальних технічних знань, ані усталеного правового стандарту для їх вирішення.

Особливою і вкрай практично гострою різновидністю проблеми є так звані ланцюгові кіберінциденти – ситуації, коли виконавець IT-договору не зазнає безпосередньої кібератаки, але виявляється нездатним виконати зобов'язання внаслідок компрометації його підрядника, постачальника хмарних послуг або розробника програмного компонента. Атака на SolarWinds (2020), що скомпрометувала тисячі організацій через оновлення ПЗ, яке вони отримали від надійного постачальника, є найбільш показовим прикладом: жертви атаки не мали жодної можливості запобігти їй у власних системах, але зазнали повного порушення функціональності критичних сервісів [6].

З позиції договірної права виникає принципова колізія: виконавець IT-договору, що не виконав зобов'язання через компрометацію свого постачальника, посилається на форс-мажор – але замовник справедливо вказує, що вибір і моніторинг субпідрядників є прямим обов'язком виконавця. Ця колізія відображає ширшу доктринальну проблему – питання про те, чи поширюється форс-мажорний захист на обставини, що знаходяться у «сфері ризику» боржника навіть без його прямої вини. УНІДРУА, Принципи PECL і DCFR у цьому питанні солідарні: форс-мажор не охоплює обставини, що знаходяться у контролі боржника або його

субпідрядників – і ланцюгові кіберінциденти через ненадійного постачальника є саме такими.

Кіберінциденти як обставини непереборної сили в ІТ-договорах є тією сферою, де відсутність системної правової доктрини є не академічною проблемою, а джерелом реальних і масштабних правових конфліктів у найближчі роки – особливо в умовах триваючого збройного конфлікту, що перетворює Україну на один із найбільш кіберактивних середовищ у світі.

Отже, як висновок можна зазначити, що кваліфікація кіберінциденту як форс-мажорної обставини не може ґрунтуватися виключно на факті його настання. Вирішальне значення має оцінка поведінки сторони-боржника, зокрема того, чи були нею вжиті всі розумно необхідні технічні та організаційні заходи для запобігання інциденту або мінімізації його наслідків. Саме тому критерій належної обачності набуває у сфері цифрових відносин спеціалізованого змісту та повинен визначатися з урахуванням сучасних вимог кібербезпеки, галузевих стандартів і кращих практик управління інформаційними ризиками.

ЛІТЕРАТУРА:

1. Черняшук Н., Клещевник К. Аналіз кібератак останніх років: уроки для захисту. *Міжнародна науково-практична конференція «Проблеми комп'ютерних наук, програмного моделювання та безпеки цифрових систем»*. 2025, С. 116–118.

2. Маріц Д.О., Пазюк М.В., Уваров І.А. Проблеми доведення форс-мажорних обставин у договірних зобов'язаннях під час дії воєнного стану в Україні. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. Випуск № 03, 2025, частина 1. С. 272-278.

3. Юридичні договори у сфері кібербезпеки: як захистити дані та конфіденційність. URL: <https://www.bca.education/dogovory-kiberbezpeky/>

4. Merck & C., Inc., et al. vs. Ace American Insurance Company, et al. 2023. URL: <https://law.justia.com/cases/new-jersey/appellate-division-published/2023/a-1879-21.html>

5. Sunburst (кібератака). Вікіпедія – вільна енциклопедія. URL: [https://uk.wikipedia.org/wiki/Sunburst_\(кібератака\)](https://uk.wikipedia.org/wiki/Sunburst_(кібератака))

Галупова Лариса Ігорівна,
кандидатка юридичних наук, доцентка, доцентка кафедри права
інтелектуальної власності та патентної юстиції
Національного університету «Одеська юридична академія»

Мартинюк Іван Вікторович,
кандидат юридичних наук, доцент кафедри права інтелектуальної
власності та патентної юстиції Національного університету
«Одеська юридична академія»

НАВЧАЛЬНІ ДАТАСЕТИ У СИСТЕМАХ ШТУЧНОГО ІНТЕЛЕКТУ ЯК ОБ'ЄКТИ АВТОРСЬКО-ПРАВОВОЇ ОХОРОНИ

Стрімкий розвиток штучного інтелекту зумовлює активне використання значних масивів даних для навчання моделей, серед яких вагоме місце займають об'єкти, що охороняються авторським правом. Формування навчальних датасетів відбувається шляхом відбору, структурування та обробки контенту, який часто включає тексти, зображення, аудіовізуальні матеріали та інші результати інтелектуальної, творчої діяльності. У таких умовах постає питання правової природи самих датасетів, їх співвідношення з об'єктами авторського права, а також допустимості використання охоронюваних творів у процесі машинного навчання. Водночас чинні правові підходи, сформовані в епоху традиційного використання творів, не повною мірою враховують специфіку автоматизованої обробки інформації та створення нових цифрових продуктів на її основі.

Навчальний датасет (англ. training dataset) є структурованою або неструктурованою сукупністю даних, яка використовується для побудови та вдосконалення моделей машинного навчання. З точки зору права, датасет потенційно охоплює кілька самостійних режимів правової охорони: авторське право, право *sui generis* на бази даних, а також режим комерційної таємниці. У системах штучного інтелекту, де якість тренувального набору безпосередньо детермінує якість генеративних виходів, вирішення питання про правовий статус датасету набуває стратегічного значення для регулювання ринку ШІ-технологій.

Класична доктрина авторського права пов'язує охорону з наявністю творчого елемента. Застосовуючи цей критерій до датасетів, слід розрізнити два аспекти: по-перше, творчий характер самих вхідних даних (наприклад, літературні тексти, картини), котрі є самостійними об'єктами авторського права; по-друге, творчий характер процесу відбору, верифікації, анотування та структурування цих даних укладачами датасету. Рішення Верховного суду США у справі *Feist Publications v. Rural Telephone Service* (1991)[1] встановило, що для надання правової охорони необхідна наявність творчої діяльності та оригінальності твору. Звичайна компіляція без творчого елементу не є об'єктом авторсько-правової охорони. Відтак формально механічне відтворення загальнодоступних даних без ознак творчого упорядкування залишається поза сферою охорони авторського права, хоча може підпадати під режим *sui generis*.

Директива ЄС 96/9/ЄС про правову охорону баз даних запровадила паралельну систему захисту, що не вимагає творчого елемента, але передбачає суттєві якісні або кількісні вклади в отримання, верифікацію або представлення змісту [2]. Навчальний датасет для великої мовної моделі (LLM), формування якого потребує витрат обчислювальних ресурсів та значних інтелектуальних, творчих зусиль з боку людини на анотування, апріорі відповідає цьому критерію. Право виробника бази даних, будучи майновим і передаваним, забороняє вилучення або повторне використання суттєвої частини бази без згоди правовласника строком на 15 років. Це право є предметом обговорення в контексті застосування положень Акту ЄС про штучний інтелект (EU AI Act, 2024) [3] та Регламенту ЄС про дані (Data Act, 2023) [4].

Центральним дискусійним питанням є допустимість масового сканування та індексування охоронюваних творів без дозволу правовласників у процесі підготовки тренувальних матеріалів. У праві США питання використання навчальних даних у системах штучного інтелекту вирішується через доктрину добросовісного використання (*fair use*), закріплену у § 107 Закону про авторське

право 1976 року [5]. Зокрема, у справі *Authors Guild v. Google, Inc.* (2015) суд визнав масову оцифровку книжок таким використанням, що має трансформативний характер, тобто створює нову цінність і не замінює оригінал [6]. Водночас щодо генеративних систем штучного інтелекту цей підхід не є однозначним, оскільки такі системи можуть відтворювати значні фрагменти навчальних даних, що ставить під сумнів правомірність їх використання. У праві Європейського Союзу ключове значення має Директива 2019/790/ЄС, яка передбачає винятки для текстового та дата-майнінгу (text and data mining), але водночас дозволяє правовласникам забороняти використання своїх творів у комерційних цілях шляхом спеціального застереження (opt-out) [7].

Формування великих навчальних датасетів із відкритих інтернет-джерел створює проблему так званих «сирітських творів» – матеріалів, для яких неможливо знайти або встановити правовласника. Наприклад, у практиці *Common Crawl*¹ використовуються мільярди вебсторінок, але правовий статус такого контенту часто є невизначеним або різним. Більшість країн не мають чітких механізмів, як отримати дозволи на використання таких матеріалів у великому масштабі для навчання штучного інтелекту. Через це розробники моделей опиняються у ситуації правової невизначеності та ризику значної відповідальності, яка теоретично може перевищувати їхні фінансові можливості.

Використання у навчальному датасеті матеріалів, захищених авторським правом, без дозволу може призвести до відповідальності: безпосередньої – за копіювання під час завантаження і зберігання даних, а також опосередкованої – якщо система штучного інтелекту відтворює результати, подібні до оригінальних творів. У справах *Andersen v. Stability AI Ltd* [8]. та *The New York Times Co. v. Microsoft Corp.* [9] позивачі стверджують, що їхні твори були використані без дозволу і що такі системи створюють конкурен-

¹ **Common Crawl** – це неприбуткова організація, яка створює й відкрито надає масштабні набори даних веб-сканувань. Вона надає дослідникам, розробникам і компаніям безкоштовний доступ до репрезентативної вибірки світового вебу, що використовується для аналізу, навчання моделей ШІ та цифрових досліджень.

цію їхньому контенту, що має значення для оцінки добросовісного використання (fair use). Характер відповідальності залежить від юрисдикції та особливостей використання об'єктів авторського права тієї чи іншої моделі ІІІ.

EU AI Act (Регламент ЄС 2024/1689) у ст. 53 зобов'язує постачальників моделей загального призначення оприлюднювати детальне резюме щодо контенту, використаного для навчання, з достатньою деталізацією для уможливлення дотримання авторського права. Це вимога прозорості датасетів є інструментом *ex ante* (до виникнення правопорушення чи наслідків) регулювання, що дозволяє правовласникам ідентифікувати потенційні порушення та реалізовувати механізм *opt-out* (згода вважається наданою за замовчуванням, але особа має право відмовитися (вийти) з такого режиму) до або під час навчання. Водночас вимога прозорості вступає в колізію з правом на комерційну таємницю щодо методології формування датасету, що вимагає пошуку балансу між конкурентними правовими цінностями.

Якщо навчальний датасет визнається оригінальним, виникає питання, кому саме належать авторські права. Зазвичай авторами вважаються конкретні люди – ті, хто створює, відбирає або структурує дані, але майнові права зазвичай переходять до компанії чи замовника за договором. Складність з'являється тоді, коли датасет формується за участю великої кількості людей через платформи на кшталт Amazon Mechanical Turk чи Scale AI: у такому разі внесок кожного є невеликим, і це може призводити до «розпорошеного» співавторства, яке важко узгодити з класичними правилами авторського права. У деяких країнах, наприклад у Великій Британії, існують спеціальні норми для творів, створених комп'ютером, де автором визнається особа, яка організувала процес створення, що потенційно може застосовуватись і до автоматично сформованих датасетів [10].

У відповідь на правову невизначеність у сфері навчання штучного інтелекту формується ринок легально ліцензованих датасетів. Такі платформи, як Shutterstock, Getty Images та Adobe

Stock, укладають угоди з ШІ-компаніями (наприклад, OpenAI чи Google), дозволяючи використовувати контент для навчання моделей в обмін на винагороду і виплати авторам [11]. Паралельно поширюються відкриті ліцензії, такі як Creative Commons CC0, Creative Commons Attribution та Open RAIL, які дозволяють більш гнучке використання даних для ШІ. Водночас великі відкриті датасети, зокрема LAION-5B, фактично використовуються як відкриті, хоча правовий статус окремих матеріалів у їх складі часто залишається невизначеним, що демонструє розрив між реальними технологічними практиками та чинним правовим регулюванням.

Правова природа датасетів залишається однією з найбільш дискусійних проблем на перетині права інтелектуальної власності та розвитку технологій ШІ. Ефективна реформа потребує щонайменше трьох кроків: законодавчого уточнення критеріїв охороноздатності датасетів; запровадження обов'язкових механізмів ліцензування щодо навчальних матеріалів, які охороняються правом інтелектуальної власності; запровадження принципу прозорості щодо матеріалів, які використовувались для навчання ШІ. Такий підхід дозволить забезпечити баланс між стимулюванням ШІ-інновацій та захистом прав авторів та прав власників.

ЛІТЕРАТУРА:

1. Feist Publications, Inc. v. Rural Telephone Service Company : U.S. Supreme Court of Jan. 9 1991 in Case (499 U.S. 340). URL: <https://supreme.justia.com/cases/federal/us/499/340/>
2. Директива 96/9/ЄС Європейського Парламенту та Ради «Про правовий захист баз даних» від 11 березня 1996 року. URL: https://zakon.rada.gov.ua/laws/show/994_241#Text
3. 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>
4. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828

(Data Act) (Text with EEA relevance). URL: <https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng>

5. 17 U.S. Code § 107 – Limitations on exclusive rights: Fair use. URL: <https://www.law.cornell.edu/uscode/text/17/107>

6. Authors Guild v. Google, Inc., No. 13-4829 (2d Cir. 2015). URL: <https://law.justia.com/cases/federal/appellate-courts/ca2/13-4829/13-4829-2015-10-16.html>

7. Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance.). URL: <https://eur-lex.europa.eu/eli/dir/2019/790/oj>

8. Andersen et al v. Stability AI Ltd. et al, No. 3:2023cv00201 – Document 223 (N.D. Cal. 2024). URL: <https://law.justia.com/cases/federal/district-courts/california/candce/3:2023cv00201/407208/223/>

9. The New York Times Co. v. Microsoft Corp. URL: <https://picker.uchicago.edu/Copyright/Set3.pdf>

10. The Impact of Generative AI on UK Copyright Law. URL: <https://carson-mcdowell.com/news-insights/insights/the-impact-of-generative-ai-on-uk-copyright-law>

11. Opderbeck D. W. Copyright in AI Training Data: A Human-Centered Approach // Oklahoma Law Review. 2024. URL: <https://digitalcommons.law.ou.edu/cgi/viewcontent.cgi?article=2305&context=olr>

Глиняна Катерина Михайлівна

кандидатка юридичних наук, доцентка,

доцентка кафедри приватного права

Національного університету “Одеська юридична академія”

ЦИФРОВА ІДЕНТИЧНІСТЬ БАТЬКІВ І ДІТЕЙ ЯК ОБ’ЄКТ ЦИВІЛЬНО-ПРАВОВОЇ ОХОРОНИ

У сучасних умовах цифрової трансформації приватноправових відносин категорія цифрової ідентичності набуває самостійного значення не лише як технічний або соціальний феномен, а і як складний юридичний конструкт, що дедалі виразніше виявляє ознаки об’єкта цивільно-правової охорони. Особливої актуальності це питання набуває у сфері правового статусу батьків і дітей, оскільки саме у сімейних правовідносинах цифрова присутність особи формується, супроводжується, контролюється та, нерідко, комерціалізується вже з раннього віку. Якщо раніше індивідуалі-

зація особи у праві пов'язувалася переважно з її іменем, честю, гідністю, діловою репутацією, зображенням, таємницею особистого життя і персональними даними, то нині до цього комплексу дедалі частіше додається цифрова ідентичність як сукупність відомостей, цифрових маркерів, електронних профілів, поведінкових характеристик, візуальних та текстових слідів, які репрезентують особу в цифровому середовищі, забезпечують її впізнаваність та дозволяють третім особам ідентифікувати, відтворювати, оцінювати або прогнозувати її поведінку.

Цифрову ідентичність батьків і дітей доцільно розуміти як комплекс персоналізованих цифрових даних і цифрових проявів особи, що створюють її стійкий або динамічний образ у мережевому просторі та мають юридичне значення для реалізації, охорони і захисту її прав та інтересів. У цьому визначенні принципово важливо наголосити на кількох аспектах. По-перше, цифрова ідентичність не зводиться лише до технічного облікового запису чи профілю в соціальній мережі, оскільки включає ширшу систему інформаційних елементів, пов'язаних із конкретною особою. По-друге, вона має не лише зовнішній, комунікативний вимір, а й внутрішній юридичний зміст, оскільки може впливати на обсяг приватності, автономії, репутаційної цілісності, сімейної автономії та інтересів дитини. По-третє, у випадку батьків і дітей цифрова ідентичність нерідко формується не автономно, а через взаємодію та навіть залежність одних суб'єктів від інших, насамперед коли йдеться про малолітніх дітей, щодо яких ініціаторами цифрової присутності виступають батьки.

Структура цифрової ідентичності батьків і дітей є багатокомпонентною. Вона охоплює, передусім, ідентифікаційні дані, до яких належать ім'я, фотографії, відеозаписи, голос, дата народження, відомості про місце проживання, навчання, родинний статус, коло сімейних зв'язків. Водночас цим її зміст не вичерпується. До цифрової ідентичності входять також поведінкові дані, зокрема історія онлайн-активності, стиль комунікації, уподобання, пошукові запити, цифрові звички, маршрути взаємодії з платформами. Окреме місце займає репутаційний компонент, який формується

через коментарі, відгуки, публікації, теги, реакції інших осіб, а також алгоритмічно згенеровані оцінки та рекомендації. У сучасному цифровому середовищі дедалі більшого значення набуває і профілювальний компонент, пов'язаний із тим, що цифрові платформи та алгоритмічні системи не лише фіксують наявні ознаки особи, а й формують її цифрову модель через автоматизовану обробку даних. Саме тому цифрова ідентичність уже не є суто результатом волевиявлення самої особи: вона дедалі більше постає як поєднання самопрезентації, зовнішнього конструювання та алгоритмічного моделювання.

У сімейному контексті правова специфіка цифрової ідентичності особливо відчутна у відносинах між батьками та дітьми. Батьки нерідко створюють цифровий образ дитини задовго до того, як вона набуває фактичної здатності усвідомлено погоджуватися на це або заперечувати проти такого формування. Публікація фотографій дитини, медичних даних, інформації про її розвиток, особливості поведінки, місце перебування, успіхи чи проблеми у навчанні поступово створює цифровий профіль, який може мати довготривалі правові та соціальні наслідки. У науковому дискурсі це часто розглядається як прояв «успадкованої» або «сконструйованої іншими» цифрової ідентичності дитини. Відповідно, дитина у цифровому середовищі може виступати не лише суб'єктом прав, а й об'єктом чужих цифрових практик, що зумовлює підвищену потребу у цивільно-правовій охороні її особистої сфери. У свою чергу, цифрова ідентичність батьків також має сімейно-правове значення, оскільки через неї можуть розкриватися дані про дітей, сімейні стосунки, батьківські підходи до виховання, приватне листування та інші чутливі аспекти сімейного життя.

З позицій цивільного права принциповим є питання про співвідношення цифрової ідентичності з особистими немайновими правами. Видається, що цифрова ідентичність не може бути зведена до одного окремого права, оскільки вона є складним об'єктом, у межах якого перетинаються і взаємодіють декілька особистих немайнових благ і правомочностей. Йдеться, зокрема, про право на ім'я, право на індивідуальність, право на зображення, право на

повагу до честі, гідності та ділової репутації, право на недоторканість приватного життя, право на таємницю особистого і сімейного життя, а також право на захист персональних даних. Цифрова ідентичність фактично виступає новою формою зовнішнього існування цих прав у цифровому середовищі, а отже, не заперечує класичної системи особистих немайнових прав, а радше виявляє її новий вимір. Саме тому правова охорона цифрової ідентичності має спиратися не на створення повністю відокремленої категорії поза межами цивільного права, а на розвиток вже існуючих інститутів особистих немайнових прав із урахуванням цифрової специфіки їх реалізації та порушення.

Разом із тим цифрова ідентичність має і певні особливості, які не дозволяють повністю розчинити її у традиційній конструкції особистих немайнових прав. По-перше, вона є технічно відтворюваною, копійованою, масштабованою та алгоритмічно оброблюваною, що істотно посилює ризики втручання у сферу особистої автономії. По-друге, вона є кумулятивною, тобто накопичується протягом часу та нерідко зберігається навіть незалежно від волі особи. По-третє, вона може існувати у змішаному режимі, поєднуючи особисті немайнові та майнові інтереси. Наприклад, популярний акаунт одного з батьків може бути одночасно простором приватного самовираження, каналом сімейної комунікації і джерелом монетизації, а цифровий образ дитини може використовуватися як елемент публічного контенту, що приносить прибуток. У таких випадках цифрова ідентичність набуває подвійної природи, що ускладнює визначення меж допустимого розпорядження нею та посилює значення цивільно-правових механізмів охорони.

Особливої уваги потребує також питання суб'єктного контролю над цифровою ідентичністю дитини. Цивільно-правова модель має виходити з того, що батьківські права щодо участі у формуванні та адмініструванні цифрової присутності дитини не є абсолютними, а обмежуються найкращими інтересами дитини, її правом на приватність, майбутню автономію та захист від надмірної цифрової експозиції. Отже, цифрова ідентичність дитини не може розглядатися як «цифрове продовження» батьківського

статусу або як об'єкт вільного сімейного розпорядження. Навпаки, вона має визнаватися самостійно значущою сферою особистих немайнових благ дитини, яка потребує особливо делікатного режиму правової охорони. Це положення має особливе значення і для подальшого аналізу постмортального захисту, оскільки після смерті одного з батьків або дитини постає питання про межі доступу до такої цифрової ідентичності, можливість її збереження, видалення, меморіалізації або обмеження стороннього втручання.

Отже, теоретико-правова характеристика цифрової ідентичності батьків і дітей дозволяє дійти висновку, що вона є складним, багаторівневим і динамічним об'єктом цивільно-правової охорони, який формується на перетині інформаційних технологій, сімейних зв'язків та особистих немайнових прав. Її правова природа не може бути адекватно пояснена винятково через класичні категорії персональних даних або окремих особистих немайнових благ, оскільки цифрова ідентичність інтегрує ці елементи в єдину систему цифрового представлення особи. Саме тому сучасна цивілістика потребує вироблення більш чутливої та технологічно адаптованої моделі правового розуміння цифрової ідентичності, особливо коли йдеться про батьків і дітей як суб'єктів підвищеної приватноправової значущості у сфері сімейного життя, пам'яті, репутації та міжпоколінньої цифрової присутності.

Голубєва Неллі Юріївна

*докторка юридичних наук, професорка,
завідувачка кафедри цивільного, нотаріального
та виконавчого процесу, професор кафедри приватного права
Національного університету «Одеська юридична академія»,
член-кореспондентка НАПрН України,
заслужена юристка України, адвокатка*

ПРОБЛЕМИ АВТОМАТИЗОВАНОГО УКЛАДАННЯ ДОГОВОРІВ

Технології з великою швидкістю створюють нові можливості, але й нові ризики. Як у 1990-х роках, після об'єднання інтернет-технологій з технологіями мобільних телефонів, швидко роз-

винувся інтернет, так сьогодні розвиток ІІІ впливає майже на всі інновації. Розвиток е-комерції останніми роками характеризується все більшою автоматизацією у сфері договорів, які укладаються і виконуються електронними агентами, що актуалізує питання розподілу ризиків технічних помилок та недобросовісної поведінки третіх осіб чи агентів. З кожною новою технологічною хвилею у цих процесах все менше бере участь людина, що в свою чергу ставить питання про дійсність договорів, укладених і виконаних з використанням автоматизованих систем, застосування до цих відносин норм договірних права.

Автоматизовані системи широко використовуються для операцій як за участю людини (наприклад, коли фізична особа взаємодіє з автоматизованою системою через веб-сайт або платформу електронної торгівлі), так і без неї. ІІІ трансформує торгівлю не тільки з погляду нових товарів і послуг, що продаються, але і з точки зору підвищення ефективності таких пов'язаних з торгівлею дій, як управління виробничо-збутовими ланцюгами, маркетинг товарів та послуг (у тому числі через онлайн-платформи), а також укладання та виконання договорів [1].

Автоматизоване укладання договорів передбачає експлуатацію автоматизованих систем, що генерують та обробляють повідомлення даних, включаючи такі, які являють собою оферту та її акцептування, або дії щодо виконання договору [2].

На сьогодні поняття «автоматизованого укладання договору» вже давно є ширшим, ніж «розумні контракти», популярні для дослідження 10 років тому. Частіше дослідники пишуть про смарт-контракти, але у міжнародних документах, відповідно до принципу технологічної нейтральності, цей термін не використовується. Вони виникли у зв'язку із технологією розподілених реєстрів (системи розподілених реєстрів є способом запису даних). Одним із видів даних, що записуються у розподіленому реєстрі, є дані, що мають форму комп'ютерного коду, який виконується вузлами в мережі, та який може бути запрограмований на ініціювання події чи ініціювання події поза цією системою, прикладом

такої програми є смарт-контракт. Смарт-контракт – це програма, яка використовується для автоматизованого виконання договору (чи відслідковування його виконання), а не окремий вид договору, тобто це не «смарт» і не контракт. Щодо наслідків його невиконання – можливо застосувати тільки передбачені контрактом наслідки (вони мають умовний характер виконання: «якщо-то»), наприклад, блокування оплати за товар, а не передбачені ЦК (при застосуванні ЦК наслідки будуть наставати поза блокчейном, тобто традиційним шляхом). Застосування їх в економіці поки доволі низьке, якщо говорити про реальні операції, в основному вони застосовуються при ISO. З точки зору договірного права воля сторони виражена у коді, контрагент погоджується з умовами договору приєднання, тому договір є укладеним і юридично дійсним.

До появи смарт-контрактів успішно здійснювались правочини, які виконуються за допомогою автоматизованого виконання, наприклад платіжні термінали, вендингові машини, поштомати, ігрові автомати. В смарт-контрактах особливістю є сфера функціонування – системи розподілених реєстрів, тобто не підпадає під традиційні способи автоматизації, але це не створює новий вид договорів.

Не зупиняючись тут окремо, зазначимо, що на сьогодні вже є багато міжнародних актів, які направлені на розвиток е-комерції, особливо плідно працює UNCITRAL, а останній в цій сфері акт, Типовий закон ЮНСІТРАЛ про автоматизоване укладання договорів (2024) (далі – Типовий закон), встановлює додаткові правила юридичного визнання, які спеціально адаптовані для автоматизованого заключення договорів.

Приклади автоматизованого укладання договорів включають: 1) договори на постачання, що укладаються шляхом обміну електронними повідомленнями, які передаються між комп'ютерами в результаті електронного обміну даними; 2) договори купівлі-продажу, укладені фізичною особою, яка розміщує замовлення через веб-сайт (взаємодіючи з автоматизованою системою, що «підтримує» веб-сайт); 3) договори, що укладаються за допо-

могою «розумних» пристроїв, що розміщують замовлення через підключені онлайн-платформи; 4) договори, що укладаються інтернет-ботами, які взаємодіють з веб-сайтами. У зв'язку з використанням автоматизованих систем для укладання договору зазвичай виникає кілька питань, пов'язаних, зокрема, з юридичною силою такого договору; ідентифікацією сторін договору, визначенням наміру сторін бути пов'язаними зобов'язаннями та визначенням умов договору [1].

Перші два пункти вже є практично традиційними способами укладення договорів – електронна взаємодія контрагентів дозволяє наблизити фізично віддалених осіб за допомогою електронної передачі даних з частковою автоматизацією електронного укладання договору, то 3 – частково, а 4 – передбачають взагалі відсутність людини, що і викликає питання про дійсність дій, що вживаються для узгодження, укладання та виконання договорів.

Так, IoT-пристрої (Alexa, Google Home) автоматично формують замовлення на платформах. Пристрій сканує запаси, інтегрується з платформою та замовляє продукти через голосову команду. Підтвердження згоди в договорі з голосовим асистентом відбувається конклюдентними діями – активними жестами чи словами, що фіксують акцепт оферти. Акцепт відбувається: 1) голосовою командою («Окей, Google, купи ...» після попереднього інформування «Підтвердити? Так/Ні?»); 2) PIN-кодом (асистент каже «Введи PIN 0000», користувач промовляє, платформа фіксує); 3) жестом (пристрій запитує «Підтвердити покупку?», а людина торкається екрану смартфона); 4) попереднім налаштуванням (у додатку асистента вмикається «Автозамовлення» з лімітом та здійснюється згода на серію правочинів). Платформа записує аудіо/відео, лог дій та надсилає email/SMS-підтвердження.

Договори, що укладаються інтернет-ботами, що взаємодіють з веб-сайтами – приклад повної автоматизації. Наприклад, «боти для веб-скрейпінгу» – це «збирачі даних» (так би мовити «шпигуни»): сканують сайти, отримують інформацію (ціни, відгуки, контакти) і зберігають у таблиці/файл, наприклад, для моніторингу

цін конкурентів на Rozetka чи Amazon, збір оголошень з OLX для аналітики ринку. Боти для покупок – це «автопокупці»: самі знаходять товар, додають у кошик, оплачують (оскільки вони швидші, ніж будь-яка людина, їх використовують на онлайн-аукціонах).

Згідно ст. 7 Типового закону у відносинах між сторонами договору атрибуція операції, виконаної автоматизованою системою, провадиться у порядку, узгодженому сторонами. Якщо не узгоджено – операція, виконана автоматизованою системою, присвоюється особі, яка використовує систему для цієї мети. І головне, «в атрибуції операції, виконаної автоматизованою системою, не може бути відмовлено на тій лише підставі, що вона призвела до несподіваного результату». Автоматизовані системи є інструментами, що не мають незалежної волі чи правосуб'єктності, результати роботи автоматизованих систем мають приписуватися певним особам, а не самій системі. Важливо і те, що вимоги щодо несподіваних результатів підлягають врегулюванню не на основі правил про атрибуцію, а скоріше відповідно до інших норм договірної права, які визначають правові наслідки ненавмисних подій, таких як норми про розірвання договору у разі помилки або про виправдання невиконання [3].

Оскільки у повністю автоматизованому укладанні договору людина участі не бере (мається на увазі не юридично, а фактично – договір вчиняється між собою двома комп'ютерними алгоритмами), є проблема у визначенні суб'єкта відповідальності, якщо одним з агентів допущена помилка.

Згадаємо відому справу Quoine Pte Ltd проти B2C2 Ltd. Суд в Сінгапурі розглядав спір між криптобіржею і криптотрейдером, який торгував криптовалютою. При цьому і трейдер використовував комп'ютерний алгоритм (який автоматично здійснює правочини за цінами, які алгоритм визнає прийнятними з урахуванням інформації про інші операції, що здійснюються на біржі), і біржа використовувала комп'ютерний алгоритм (який автоматично встановлює котирування криптовалют, виходячи з інформації про курси, що переважають на інших біржах). Через недогляд Quoine

щодо внесення певних необхідних змін до критичних операційних систем (технічну помилку) біржовий робот почав працювати некоректно, а робот трейдера закупив партію криптовалюти за ціною в 250 разів нижчою від ринкової. Оператори криптобіржі скасували операцію. B2C2 розпочав судовий процес, стверджуючи, що скасування угод порушувало договір з користувачем платформи, а скасування розрахункових транзакцій було порушенням довіри. Суддя першої інстанції виніс рішення на користь B2C2 Ltd з обох питань. В апеляційному порядку Апеляційний суд одноголосно відхилив позов про порушення довіри. Щодо другої вимоги, суд постановив, що одностороннє скасування Quoine спірних угод було порушенням договору, зокрема пункту, який передбачав, що після виконання замовлення трейдер повідомляється через Платформу, і така дія є незворотною. Суд не визнав, що в договорі були явні або неявні умови, які дозволяли Quoine скасувати спірні угоди, пункт, який нібито дозволяв Quoine скасувати транзакцію, якщо вона відбулася «за відхиленням від норми», не був включений до Угоди [4, 5]. Рішення цікаве тим, що суд, вирішуючи питання недійсності правочинів через суттєву помилку однієї зі сторін та застосування доктрини односторонньої помилки у загальному праві та праві справедливості, аналізував їх саме у правочинах, вчинених між собою двома комп'ютерними алгоритмами.

Фактично суворо дотримуючись відповідних доктрин та умов договорів між платформою та клієнтом, суд дав змогу скористатися помилкою програмістів. Тільки один суддя, лорд Манс, не погодився та вважав, що угоди могли бути визнані недійсними через односторонню помилку. Вважаємо, що окрема думка судді була більш справедливою, яку можна коротко передати словами: фундаментальний збій комп'ютерної системи, як причину транзакцій, чесний та розсудливий трейдер одразу зрозумів би та не покладався на можливість отримати аномальне збагачення.

На подібні випадки передбачено норму ст. 8 Типового закону «Несподівані операції, які виконуються автоматизованими системами»: «Якщо сторони не домовилися про інше, у випадку якщо

операція, виконана автоматизованою системою, присвоюється одній із сторін договору, інша сторона договору не має права посилатися на цю операцію, якщо з урахуванням усіх обставин: а) сторона, якій присвоюється ця операція, не могла розумно очікувати на її виконання; б) інша сторона знала або могла знати, виходячи з розумних очікувань, що сторона, якій присвоюється операція, не очікувала на її виконання» [3]. Думається, це правило дуже спростило б вирішення проблем із аномальними операціями при укладанні автоматизованих контрактів. Зазначений вище кейс міг би бути вирішений зовсім інакше. Хоча треба відмітити, що ст. 8 Типового закону передбачена у якості факультативної пропозиції, яку мають оцінити країни, які будуть імплементувати відповідні норми.

Згідно ч. 4 ст. 736 Проекту Цивільного кодексу України (Кодексу права приватного) волевиявлення сторони можуть здійснювати з використанням інформаційних систем, у тому числі в автоматизованому порядку. Повідомлення або інші дані, сформовані інформаційною системою відповідно до таких умов, прирівнюються до дій сторони, яка її застосувала, і є підставою для виникнення у неї цивільних прав та обов'язків. Також згадується про «автоматизовану» оферту та виконання у ст. 738, 785 [6]. Наслідки технічних сбоїв передбачені тільки для грошових зобов'язань (ст. 810), але в цілому не передбачено специфічних норм як у Типовому законі ЮНСІТРАЛ про автоматизоване укладання договорів. Тобто виниклі проблеми будуть вирішуватися відповідно до інших норм приватного права, наприклад, про недійсність договору у разі помилки або форс-мажор.

ЛІТЕРАТУРА:

1. Юридична таксономія з питань, що стосуються цифрової економіки, 2023. URL: <https://uncitral.un.org/sites/default/files/media-documents/EN/Texts/UNCITRAL/2516855e-ebook-accessible.pdf>
2. Положення текстів ЮНСІТРАЛ, які застосовуються до автоматизованого укладання договорів Записка Секретаріату. Комісія Організації Об'єднаних Націй з права міжнародної торгівлі. Робоча група IV

(Електронна торгівля), 31 жовтня – 4 листопада 2022 року. URL: <https://docs.un.org/ru/A/CN.9/WG.IV/WP.176>

3. Model Law on Automated Contracting (UNCITRAL, 2024) . URL: <https://uncitral.un.org/sites/default/files/2424674e-mlautomatedcontracting-rev1-ebook.pdf>

4. Technology and the Law The Dover House Lecture 2020, London Lord Hodge, Deputy President of The Supreme. URL: https://supremecourt.uk/uploads/speech_200310_78771609b3.pdf

5. Singapore, Quoine Pte. Ltd. v. B2B2 Ltd. URL: https://www.elitigation.sg/gd/s/2020_SGCAI_2

6. Проект Цивільного кодексу України (Кодексу права приватного) . URL: [blob:https://itd.rada.gov.ua/9ce5f60f-95f0-4b69-b39c-868b1af45199](https://itd.rada.gov.ua/9ce5f60f-95f0-4b69-b39c-868b1af45199)

Давидова Ірина Віталівна

*докторка юридичних наук, професорка,
професорка кафедри приватного права*

Національного університету «Одеська юридична академія»

РОЛЬ ЦИФРОВІЗАЦІЇ ПРАЦІ ПІД ЧАС ЗАХИСТУ МАЙНОВИХ І НЕМАЙНОВИХ ПРАВ НЕПОВНОЛІТНІХ

Активний розвиток цифрових технологій у сфері праці, зокрема розширення дистанційної роботи, платформенної (гіг-) зайнятості, застосування електронних комунікацій та автоматизованих систем управління персоналом, суттєво змінює зміст і характер традиційних трудових правовідносин. За таких умов однією з найбільш уразливих категорій на ринку праці залишаються неповнолітні працівники, чий правовий статус потребує особливого державного захисту відповідно до норм національного законодавства та міжнародних стандартів у сфері праці й захисту прав дитини.

Неповнолітні працівники є особливою соціально-демографічною групою учасників трудових правовідносин, яка має низку специфічних ознак порівняно з іншими категоріями найманих працівників. Хоча трудове законодавство загалом гарантує їм рівний із повнолітніми обсяг трудових прав, організація праці неповнолітніх повинна враховувати вікові, фізіологічні та психоемо-

ційні особливості розвитку молоді. Саме тому законодавче регулювання у цій сфері передбачає посилені вимоги щодо тривалості робочого часу, забезпечення безпечних і належних умов праці, а також здійснення контролю за станом здоров'я неповнолітніх працівників. Водночас вони виступають самостійними суб'єктами трудових правовідносин, для яких законодавством встановлено спеціальний механізм реалізації та захисту трудових прав.

Згідно зі статтею 188 КЗпП, загальним правилом є можливість укладення трудового договору з особами, які досягли шістнадцятирічного віку. Разом із тим як виняток дозволяється прийняття на роботу осіб, яким виповнилося п'ятнадцять років, за наявності письмової згоди одного з батьків або особи, яка їх замінює. Також законодавством передбачено можливість залучення до праці осіб із чотирнадцятирічного віку за умови, що неповнолітній продовжує навчання, виконує легку роботу, яка не завдає шкоди здоров'ю та не перешкоджає навчанню, а трудова діяльність здійснюється у вільний від навчання час і за згодою одного з батьків або законного представника.

Неповнолітні особи у сфері трудових правовідносин мають такі самі права, як і повнолітні працівники. Водночас щодо охорони праці, тривалості робочого часу, надання відпусток та інших умов праці законодавством України для них встановлено спеціальні гарантії та пільги.

Цифровізація праці полягає у використанні інформаційно-комунікаційних технологій під час укладення, виконання та контролю трудових і пов'язаних із ними цивільно-правових договорів. Для неповнолітніх такі процеси мають подвійний характер: з одного боку, вони розширюють можливості доступу до ринку праці, а з іншого – посилюють ризики зловживань з боку роботодавців або цифрових платформ.

У приватно-правовій сфері неповнолітній працівник може бути стороною як трудового договору, так і цивільно-правових договорів (зокрема договору про надання послуг, авторського договору тощо), укладених у цифровій формі. За таких умов осо-

бливого значення набуває дотримання вимог щодо дієздатності, усвідомленості волевиявлення та забезпечення захисту інтересів дитини, що впливає з норм цивільного законодавства та міжнародних стандартів у сфері захисту прав дитини.

У контексті дослідження цифровізації праці особливо актуальною є проблема автоматизації управлінських процесів, спрямованої на оптимізацію витрат часу та ресурсів як працівників, так і роботодавців, а також на зменшення надмірних бюрократичних процедур. Водночас запровадження цифрових технологій у трудовій сфері підвищує прозорість трудових відносин, що сприяє мінімізації корупційних ризиків та забезпечує більш ефективний і чіткий контроль за дотриманням трудових прав.

До основних майнових прав неповнолітніх працівників належать право на оплату праці, право на справедливую винагороду за виконану роботу, а також право на відшкодування матеріальної шкоди. В умовах цифровізації порушення цих прав часто пов'язане з невивплатою або зниженням винагороди, непрозорістю алгоритмів нарахування оплати, а також одностороннім блокуванням акаунтів на цифрових платформах.

Неповнолітні особи в Україні мають часткову цивільну дієздатність, що безпосередньо впливає на можливість самостійного набуття та реалізації майнових прав. У цифровому середовищі це проявляється, зокрема, під час укладення електронних трудових договорів, цивільно-правових договорів (договорів про надання послуг, авторських договорів), а також користувацьких угод із цифровими платформами.

Особливість полягає в тому, що цифрові платформи нерідко не пристосовують свої умови до участі неповнолітніх осіб, унаслідок чого фактично обмежується реалізація їхніх майнових прав або ж відповідальність покладається на законних представників без належного правового врегулювання.

Право неповнолітніх працівників на оплату праці в умовах цифрового середовища супроводжується низкою проблем, серед яких: неформалізований характер зайнятості, коли робота вико-

нується через цифрові платформи без чіткого правового статусу; здійснення виплат через електронні платіжні системи, доступ до яких може бути обмежений через вік; а також відсутність ефективних механізмів контролю за повнотою та справедливістю оплати праці.

Отже, у сукупності це свідчить про наявність ризиків порушення принципу рівності в оплаті праці та можливих зловживань з боку роботодавців або цифрових платформ.

Окрему категорію майнових прав неповнолітніх працівників становлять права на результати інтелектуальної діяльності, створені у цифровому середовищі. Йдеться, зокрема, про відео- та аудіоматеріали, графічні роботи, програмні продукти, цифрові тексти та інші об'єкти авторського права.

Проблемним залишається питання належності майнових прав, оскільки у багатьох випадках цифрові платформи передбачають автоматичну передачу таких прав або встановлюють їх обмеження, що може суперечити інтересам неповнолітнього автора та принципу належного захисту його майнових прав.

Цивільно-правовий механізм захисту майнових прав передбачає можливість звернення з вимогами про стягнення заборгованості, неустойки та відшкодування збитків. Особливістю таких спорів за участю неповнолітніх є необхідність врахування їх обмеженої цивільної дієздатності та участі законних представників, що має забезпечуватися як на етапі укладення договору, так і під час захисту порушених прав.

Захист майнових прав неповнолітніх працівників має здійснюватися за допомогою превентивних механізмів, зокрема спеціальних умов договорів, вікових обмежень та участі законних представників, а також юрисдикційних засобів захисту, серед яких судовий захист і відшкодування шкоди. Важливе значення мають і компенсаційні механізми, зокрема відшкодування матеріальної та моральної шкоди у разі порушення прав.

Водночас чинне національне законодавство поки що недостатньо враховує специфіку цифрової праці неповнолітніх, що зумовлює потребу його подальшого вдосконалення.

Немайнові права неповнолітніх працівників в умовах цифровізації також стикаються з низкою специфічних викликів. Передусім це стосується права на повагу до честі, гідності та ділової репутації, права на приватне життя і захист персональних даних, а також права на психологічну безпеку.

Використання цифрових засобів контролю, систем відеоспостереження, моніторингу онлайн-активності, а також публічних рейтингів і відгуків може негативно позначатися на психоемоційному стані неповнолітніх осіб. У цивільно-правовому аспекті такі дії можуть розглядатися як посягання на особисті немайнові права, що створює підстави для застосування способів захисту, передбачених цивільним законодавством.

Відшкодування шкоди виступає одним із ключових інструментів цивільно-правового захисту прав неповнолітніх працівників. Матеріальна шкода може бути наслідком незаконного позбавлення доходу, пошкодження майна або витрат, пов'язаних із відновленням порушених прав.

Особливо складним є питання компенсації моральної шкоди, заподіяної неповнолітньому працівникові у цифровому середовищі. Під час визначення розміру такої шкоди необхідно враховувати вік потерпілого, характер правопорушення, тривалість негативно-го впливу та психологічні наслідки. Цифрові форми праці можуть посилювати моральні страждання через публічний характер порушення та тривале збереження відповідної інформації у мережі.

З огляду на це доцільним є вироблення спеціальних підходів у судовій практиці щодо визначення розміру моральної шкоди, завданої неповнолітнім у сфері цифрової праці, з урахуванням принципів справедливості та пріоритетності інтересів дитини.

Отже, цифровізація праці є одним із ключових чинників трансформації сучасних трудових відносин, що суттєво впливає на реалізацію та захист майнових і немайнових прав неповнолітніх працівників. Використання цифрових платформ, дистанційних форм зайнятості, електронного документообігу та алгоритмічного управління працею, з одного боку, розширює можливості

доступу неповнолітніх до ринку праці, сприяє розвитку їх професійних навичок і творчого потенціалу, а з іншого – створює нові ризики порушення їхніх прав та законних інтересів.

Майнові права неповнолітніх працівників у цифровому середовищі найчастіше порушуються через неформалізований характер платформенної зайнятості, непрозорість механізмів нарахування винагороди, відсутність належного контролю за оплатою праці, а також обмеження доступу до електронних платіжних систем. Особливого значення набуває проблема захисту прав на результати інтелектуальної діяльності, створені неповнолітніми у цифровому просторі, оскільки умови користування платформами нерідко передбачають автоматичне обмеження або передачу майнових прав на такі об'єкти.

Водночас немайнові права неповнолітніх працівників зазнають нових викликів у зв'язку з використанням цифрових засобів контролю, моніторингу онлайн-активності, алгоритмічного оцінювання праці та поширенням кібербулінгу. Це створює загрозу порушення права на приватність, повагу до честі та гідності, психологічну безпеку й захист персональних даних. У таких умовах особливого значення набувають цивільно-правові механізми захисту, зокрема відшкодування матеріальної та моральної шкоди, а також ефективна участь законних представників у захисті прав неповнолітніх.

Чинне законодавство України недостатньо враховує специфіку цифрової праці неповнолітніх, оскільки переважно орієнтоване на традиційні форми трудових правовідносин. Це зумовлює необхідність удосконалення нормативно-правового регулювання шляхом запровадження спеціальних гарантій для неповнолітніх у сфері дистанційної та платформенної зайнятості, посилення вимог щодо захисту персональних даних, обмеження алгоритмічного контролю та визначення особливостей цивільно-правової відповідальності цифрових платформ.

Тож, ефективний захист майнових і немайнових прав неповнолітніх працівників в умовах цифровізації праці потребує комп-

лексного підходу, що поєднує вдосконалення трудового, цивільного та інформаційного законодавства, розвиток судової практики та врахування міжнародних стандартів у сфері прав дитини. Пріоритетом подальшого розвитку правового регулювання має стати забезпечення балансу між інноваційним розвитком цифрового ринку праці та принципом найкращих інтересів дитини.

Жорнокуй Юрій Михайлович

доктор юридичних наук, професор,

завідувач кафедри цивільного права та процесу

Харківського національного університету внутрішніх справ

ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА ПРАВА ЛЮДИНИ: ПРОБЛЕМНІ ПИТАННЯ

Штучний інтелект (далі - ШІ) є новою сферою, що змінює світ і саму будову громадянського суспільства. На сьогодні законодавство не дає відповіді на питання інтеграції або хоча б встановлення меж і обмежень щодо впливу ШІ на функціонування соціальної та політичної сфер. Оскільки ШІ має величезний потенціал для підвищення людських можливостей і покращення процесів ухвалення рішень, що пов'язано з його можливою упередженістю і підзвітністю, а також конфіденційністю використання ним інформації, виникає кілька етичних і правових наслідків, які необхідно враховувати. Ці проблеми необхідно вирішити, забезпечивши етичне використання ШІ та пом'якшення його негативного впливу на права людини.

Дискусії щодо впливу ШІ на права людини тривають уже довгий час. Попри спроби визначити роль ШІ в дотриманні прав людини, все ще не напрацьовані нормативні документи, які б регулювали можливість його впливу на здійснення та дотримання прав людини та межі такого впливу. У контексті викладеного актуалізуються питання, пов'язані з етичним аспектом впливу ШІ на здійснення прав людини, а також можливі шляхи охорони та захисту таких прав.

Питання схильності технологій ІІІ до втручання у права людини поступово набуває гостроти. Звичайно, проблеми порушення прав людини не є новими для суспільства. Однак через втручання ІІІ їхня кількість істотно збільшується з перспективою впливу та поширення на реальне життя [1]. Отже, виникає проблема етичного впливу ІІІ на права людини, що пов'язано з алгоритмічним вибором. У зв'язку із цим постають питання: хто використовує етичні засади та вирішує розбіжності між етичними і правовими аспектами, до якої межі етика може інтегруватися в законодавство. Зазначається, що «етичні оцінки потрібні, коли використання ІІІ відповідає вимогам права та перетинає етико-соціальні цінності суспільства» [2].

Права людини часто характеризуються як невід'ємні, невідчужувані, взаємопов'язані, неподільні, взаємозалежні й універсальні. Вони розглядаються як такі, що мають однакову важливість і буття, відповідно важливо у рівному ступені поважати гідність і цінність кожної людини [3, р. 95]. Коли йдеться про зв'язок між правами людини та ІІІ, найчастіше постає питання про те, як ІІІ впливає на такі права. Фактично, існує певна група прав людини, яку постійно згадують як найбільш вразливу до цих впливів і захист якої в управлінні та регулюванні ІІІ вважається пріоритетною проблемою. Це стосується конфіденційності та захисту даних, свободи вираження поглядів і доступу до інформації, рівності та недискримінації. Отже, чи є потреба у використанні ІІІ для реалізації деяких або всіх прав людини?

У сфері прав людини те, що може викликати у нас занепокоєння щодо будь-якої технології, не тільки ІІІ, це, з одного боку, процес створення і проєктування технології, а з іншого – використання, застосування, ефекти або результати технологій, які виключають, обмежують, дискримінують, зводять нанівець, погіршують, перешкоджають або зменшують визнання, або здійснення прав людини та основних свобод на рівних умовах [4, рр. 116–117]. У цьому контексті варто мати на увазі права людини у сфері ІІІ, так само як ми не повинні забувати і про ІІІ у сфері прав людини, оскільки вплив існує в обох напрямках, хоча не всі вони завжди є

негативними. Наприклад, чи потрібен нам ШІ, щоб здійснювати і гарантувати право на житло, або право на свободу пересування, або право на доступ до правосуддя?

Використання технологій ШІ створює значні проблеми з конфіденційністю. Із величезною кількістю особистих даних, які збираються та аналізуються, люди часто опиняються в ненадійному становищі, коли відомості про них можуть використовуватися без їхньої згоди. Враховуючи ці складнощі, важливо встановити етичні принципи і межі, які регулюють розроблення та впровадження технологій ШІ. Первинні дослідження в цій галузі наголосили на потребі в міждисциплінарній співпраці із залученням фахівців з етики, технологів, політиків і громадськості для забезпечення того, щоб ШІ розроблявся відповідально та справедливо [5, pp. 1–2].

Хоча цифрові комунікації, з одного боку, зробили революцію у світі праці та міжособистісних стосунків, з іншого – вони зробили нашу конфіденційність більш крихкою, більш уразливою для порушень. Зі збільшенням використання ШІ в системах спостереження конфіденційність людей може бути серйозно порушеною. Крім того, чат-боти та голосові помічники на основі ШІ можуть збирати й обробляти персональні дані, що викликає занепокоєння щодо конфіденційності та безпеки даних. Праву на приватність також загрожує масштабний збір даних, нові методи стеження та поліцейські дії [3, р. 98]. Втручання в наше право на приватність може включати порушення інших прав, таких як свобода вираження поглядів, саме через взаємозалежність і взаємозв'язок прав людини, бо порушення одного права загрожує всім іншим. Свобода вираження поглядів через інтернет може бути обмежена тільки законом і тільки, якщо обмеження є необхідним і пропорційним законній меті (наприклад, захист національних інтересів) [2].

Щоб визначити, чи потрібен нам ШІ для здійснення, гарантій та захисту конкретного права чи свободи, ми маємо поставити як мінімум такі питання: 1) що привносить ШІ в конкретне право, яке виходить за межі його здійснення, гарантій або захисту в аналоговій реальності; 2) який рівень ефективного доступу до пев-

ного права існує в цей час в аналоговій реальності; 3) чи покращує використання ШІ доступ до здійснення цього права та чи не утверджує воно наявні (не створює нові) винятки; 4) чи може ШІ гарантувати всі елементи і характеристики, які містить конкретне право у стандартах, щодо здійснення прав людини; 5) який рівень ухвалення рішень буде делеговано ШІ для здійснення, забезпечення чи захисту цього права і, як результат, який рівень ухвалення рішень буде в людей.

Сьогодні науковці, які працюють у сфері ШІ, проявляють мало інтересу до прав людини і вважають за краще звертатися до етики, коли їх запитують про можливий негативний вплив ШІ на життя людей та їхні права. Зв'язок між ШІ та правами людини все ще перебуває у стадії формування, попри його величезну важливість: практично в кожній сфері, де впроваджується ШІ, є право людини, яке безпосередньо чи опосередковано з ним пов'язане.

Хоча ШІ має потенціал для підвищення людських можливостей і покращення процесів ухвалення рішень, він викликає стурбованість його негативним впливом на права людини. Однією з основних етичних проблем ШІ є його потенціал закріплювати наявні суспільні стереотипи та дискримінацію. Використання технології ШІ для розпізнавання облич, наприклад під час найму та підбору персоналу, й алгоритми машинного навчання можуть призвести до серйозних порушень прав людини, включаючи права на рівність, конфіденційність і недискримінацію. Крім того, викликає занепокоєння прозорість, підзвітність і зрозумілість рішень, ухвалених ШІ. У майбутньому важливо забезпечити розвиток ШІ відповідно до реалізації принципів прав людини. Подальша робота має бути зосереджена на розробленні етичного зрізу систем ШІ, які надають пріоритет прозорості, справедливості й підзвітності, мінімізуючи потенційний негативний вплив на права людини.

ЛІТЕРАТУРА:

1. Chatterjee S. A critical study of creative problem solving on level, style and complexity. *International Journal of Science, Technology & Management*. 2015. Vol. 4, Iss. 1. Pp. 705–713.

2. Cataleta M. S. The Fragility of Human Rights Facing AI. 2021 // HAL : сайт. URL: <https://hal.science/hal-03289002v1/file/Paper%20No%202%20East-West%20Center.pdf>

3. Homam el T., Polok B., Ahmed Rana A. Balancing Potential and Peril: The Ethical Implications of Artificial Intelligence on Human Rights. *Multicultural Education*. 2023. Vol. 9, No. 6. Pp. 94–101.

4. Donahoe E., MacDuffee M. Metzger. Artificial Intelligence and Human Rights. *Journal of Democracy*. 2019. Vol. 30, Iss. 2. Pp. 115–126.

5. Sai Teja B. Ethical implications of artificial intelligence: a review of early research and perspectives. *International Engineering Journal for Research & Development*. 2022. Vol. 7, Iss. 1. Pp. 1–8.

Журило Сергій Сергійович

кандидат юридичних наук, доцент,
доцент кафедри економіки, права та управління бізнесом
Одеського національного економічного університету

ДО ПИТАННЯ ПРО ЕФЕКТИВНІСТЬ АНТИКОРУПЦІЙНОЇ ПОЛІТИКИ В СФЕРІ ПУБЛІЧНОГО УПРАВЛІННЯ

Корупція у сфері публічного управління є однією з ключових проблем сучасної держави, що негативно впливає на ефективність функціонування органів влади, економічний розвиток країни та рівень довіри громадян до державних інституцій. Її поширення призводить до порушення принципів законності, справедливості та прозорості діяльності органів державної влади й місцевого самоврядування. Саме тому формування ефективної антикорупційної політики є одним із пріоритетних напрямів державного управління в Україні.

Антикорупційна політика у сфері публічного управління передбачає комплекс правових, організаційних та інституційних заходів, спрямованих на запобігання корупційним проявам, виявлення правопорушень та притягнення винних осіб до відповідальності. Її ефективність значною мірою залежить від належного законодавчого забезпечення, функціонування спеціалізованих антикорупційних органів, а також від рівня координації між державними інституціями.

Законодавчою основою антикорупційної політики в Україні є Конституція України, Закони України «Про запобігання корупції», «Про Національне антикорупційне бюро України», «Про Вищий антикорупційний суд», а також інші нормативно-правові акти, що регулюють питання боротьби з корупцією. Важливе значення має Антикорупційна стратегія на 2021–2025 роки, затверджена Законом України «Про засади державної антикорупційної політики на 2021–2025 роки». Основною метою цієї стратегії є забезпечення системності та узгодженості антикорупційних заходів, удосконалення механізмів запобігання корупції та підвищення рівня доброчесності у діяльності органів публічної влади.

Протягом останніх років в Україні було проведено масштабне реформування антикорупційної системи. Зокрема, у процесі реалізації Антикорупційної стратегії на 2014–2017 роки було створено спеціалізовані антикорупційні органи: Національне агентство з питань запобігання корупції (НАЗК), Національне антикорупційне бюро України (НАБУ), Спеціалізовану антикорупційну прокуратуру (САП), Національне агентство з розшуку та управління активами (АРМА), а також Вищий антикорупційний суд (ВАКС). Створення зазначених органів стало важливим етапом у формуванні сучасної антикорупційної інфраструктури держави.

Особливе місце у системі антикорупційних органів займає Національне агентство з питань запобігання корупції. НАЗК є центральним органом виконавчої влади зі спеціальним статусом, основним завданням якого є формування та реалізація державної антикорупційної політики. До його повноважень належать розроблення антикорупційної стратегії та державної програми її виконання, проведення антикорупційної експертизи нормативно-правових актів, контроль за дотриманням вимог фінансового контролю, перевірка декларацій посадових осіб, моніторинг способу життя суб'єктів декларування, виявлення та врегулювання конфлікту інтересів, а також координація міжнародного співробітництва у сфері боротьби з корупцією.

Попри значний прогрес у створенні антикорупційної системи, проблема ефективності її функціонування залишається акту-

альною. Однією з ключових проблем є відсутність територіальних органів НАЗК. Закон України «Про запобігання корупції» передбачає можливість створення таких органів, однак на практиці вони досі не функціонують. У результаті значна частина повноважень щодо запобігання корупції на місцевому рівні покладається на уповноважених осіб у державних органах та органи Національної поліції.

Разом із тим діяльність поліції у сфері складання адміністративних протоколів за корупційні правопорушення не є основною та профільною. Це створює ризики недостатнього контролю та неповного охоплення всіх корупційних правопорушень. Йдеться, зокрема, про порушення вимог фінансового контролю, недотримання обмежень щодо отримання подарунків, конфлікту інтересів, сумісництва та інших обмежень, передбачених антикорупційним законодавством.

У зв'язку з цим важливим напрямом удосконалення антикорупційної політики є створення територіальних підрозділів НАЗК. У 2023 році це питання вже аналізувалося НАЗК у межах реалізації Державної антикорупційної програми на 2023–2025 роки. Було запропоновано декілька моделей організації територіальних підрозділів: зі статусом юридичної особи, із централізованим управлінням адміністративними функціями або без статусу юридичної особи як структурних підрозділів центрального апарату.

Серед основних переваг створення територіальних органів НАЗК визначено розширення представництва агентства в регіонах, збільшення охоплення суб'єктів контролю, підвищення оперативності виявлення корупційних порушень та покращення взаємодії з місцевими громадами. Наявність регіональних підрозділів дозволила б ефективніше здійснювати моніторинг діяльності органів місцевого самоврядування та державних адміністрацій, своєчасно реагувати на корупційні ризики та забезпечувати належну превентивну роботу.

Водночас НАЗК звернуло увагу і на певні недоліки створення територіальних органів. Серед них – необхідність значних фі-

нансових витрат на утримання персоналу, матеріально-технічне забезпечення, ризик дублювання функцій центрального апарату, а також складність реалізації такої реформи в умовах воєнного стану. Крім того, наголошувалося на обмеженому обсязі повноважень, які можуть бути передані на регіональний рівень.

Однак зазначені аргументи не можна вважати беззаперечними. Саме в умовах воєнного стану проблема ефективного контролю за використанням бюджетних коштів, гуманітарної допомоги та ресурсів держави набуває особливої актуальності. Відсутність територіальних підрозділів НАЗК суттєво ускладнює оперативне реагування на корупційні правопорушення в регіонах та обмежує можливості здійснення превентивних заходів.

Крім того, кожен регіон України має власну специфіку корупційних ризиків. Централізована система управління не завжди дозволяє врахувати місцеві особливості, своєчасно реагувати на порушення та забезпечувати ефективну взаємодію з громадськістю й антикорупційними активістами. Створення територіальних органів сприяло б посиленню комунікації з населенням, проведенню роз'яснювальної та просвітницької роботи, а також підвищенню рівня правової культури у сфері запобігання корупції.

Не менш важливим є питання оперативності реагування. Наявність територіальних підрозділів дозволила б швидше виявляти факти порушень антикорупційного законодавства, проводити перевірки, здійснювати моніторинг діяльності посадових осіб та забезпечувати належне документування правопорушень. Це, у свою чергу, позитивно вплинуло б на ефективність реалізації державної антикорупційної політики загалом.

Ураховуючи викладене, доцільним є повернення до питання створення територіальних підрозділів НАЗК та розроблення поетапного механізму їх впровадження. Оптимальним варіантом може стати реалізація пілотних проєктів у найбільш стратегічно важливих регіонах із подальшим поширенням позитивного досвіду на всю територію України. Такий підхід дозволить оцінити ефективність функціонування регіональних підрозді-

лів, визначити оптимальну модель їх організації та мінімізувати можливі ризики.

Отже, антикорупційна політика у сфері публічного управління є складним та багатогранним процесом, який потребує постійного вдосконалення. Незважаючи на створення сучасної системи антикорупційних органів, ефективність їх діяльності значною мірою залежить від рівня організаційного забезпечення, координації та наближеності до регіонального рівня. Створення територіальних підрозділів НАЗК може стати важливим кроком до посилення контролю за дотриманням антикорупційного законодавства, підвищення прозорості діяльності органів влади та зміцнення довіри суспільства до державних інституцій. Реалізація таких змін сприятиме підвищенню ефективності антикорупційної політики та забезпеченню сталого розвитку України.

Зубар Володимир Михайлович

кандидат юридичних наук, професор,

професор кафедри приватного права

Національного університету «Одеська юридична академія»

БЛОКЧЕЙН ТА ЙОГО РОЛЬ У ТРАНСФОРМАЦІЇ КОРПОРАТИВНИХ ПРАВОВІДНОСИН

Цифровізація економіки та стрімкий розвиток інформаційних технологій суттєво впливають на механізми регулювання суспільних відносин, у тому числі й корпоративних. Однією з найбільш перспективних технологій сучасності є блокчейн (blockchain) – технологія розподіленого реєстру, яка забезпечує безпечне, прозоре та незмінне зберігання інформації. Саме блокчейн став технологічною основою для розвитку багатьох цифрових інструментів, серед яких особливе місце займають смарт-контракти. У сучасних умовах блокчейн розглядається не лише як технологічне нововведення, а й як важливий інструмент модернізації корпоративного управління та правового регулювання корпоративних відносин.

Актуальність дослідження ролі блокчейну у корпоративній сфері обумовлена необхідністю підвищення ефективності корпо-

ративного управління, забезпечення прозорості діяльності юридичних осіб, зниження ризиків шахрайства та скорочення витрат на здійснення корпоративних процедур. Особливого значення це питання набуває в умовах цифрової трансформації економіки України та процесів гармонізації національного законодавства із правом Європейського Союзу.

Блокчейн являє собою децентралізовану систему зберігання даних, у якій інформація фіксується у вигляді послідовних блоків, пов'язаних між собою криптографічними методами. Однією з ключових особливостей цієї технології є неможливість несанкціонованої зміни вже внесених даних. Завдяки цьому блокчейн забезпечує високий рівень довіри між учасниками правовідносин без необхідності залучення додаткових посередників.

У корпоративній сфері блокчейн може застосовуватися для вирішення широкого кола завдань. Насамперед технологія здатна забезпечити надійне ведення реєстрів учасників товариств та акціонерів. Традиційні централізовані реєстри можуть бути вразливими до технічних збоїв, втручання третіх осіб або помилок адміністраторів. Натомість використання блокчейну дозволяє створити єдину систему обліку корпоративних прав, доступну всім уповноваженим учасникам та захищену від несанкціонованих змін.

Одним із найбільш перспективних напрямів використання блокчейну є автоматизація корпоративних процедур. Завдяки поєднанню технології блокчейн та смарт-контрактів можливим стає автоматичне виконання рішень органів управління юридичної особи, розподіл дивідендів між учасниками, реалізація корпоративних договорів, а також контроль за виконанням певних умов корпоративного управління. У таких випадках блокчейн виступає не лише середовищем для зберігання інформації, а й платформою для реалізації програмного коду, який забезпечує виконання визначених дій.

Важливе значення технологія має і для організації корпоративного голосування. Традиційні механізми проведення загальних зборів часто пов'язані з необхідністю перевірки повноважень учас-

ників, підрахунком голосів та фіксацією результатів. Блокчейн дозволяє створити систему електронного голосування, у якій кожен голос буде зафіксований у реєстрі та не може бути змінений після його внесення. Це сприяє підвищенню прозорості корпоративного управління та зміцненню довіри між учасниками товариства.

Ще одним перспективним напрямом є токенизація корпоративних прав. Завдяки блокчейну права на частки у статутному капіталі або акції можуть бути представлені у вигляді цифрових токенів. Такий підхід спрощує обіг корпоративних прав, підвищує ліквідність активів та створює нові можливості для залучення інвестицій. У світовій практиці вже активно розвиваються механізми випуску так званих security tokens, які підтверджують майнові права власників та можуть використовуватися як цифровий аналог традиційних цінних паперів.

Суттєвою перевагою блокчейну є зниження транзакційних витрат. Використання технології дозволяє скоротити потребу у залученні посередників, таких як реєстратори, депозитарії чи інші суб'єкти, що здійснюють облік та підтвердження корпоративних прав. Крім того, автоматизація процесів сприяє зменшенню кількості помилок, пов'язаних із людським фактором.

Попри значні переваги, впровадження блокчейн-технологій у корпоративні правовідносини супроводжується низкою проблем. Насамперед це стосується відсутності комплексного правового регулювання. Чинне законодавство України поки що не містить достатньо чітких положень щодо використання блокчейну в корпоративному управлінні, правового статусу цифрових активів та порядку здійснення корпоративних процедур у децентралізованих системах.

Існують також технічні ризики, пов'язані з можливими помилками програмного забезпечення, вразливістю систем безпеки та кіберзагрозами. Незважаючи на високий рівень захищеності блокчейну, помилки у програмному коді можуть призвести до негативних наслідків для учасників корпоративних відносин. Крім того, незмінність інформації, яка є перевагою технології, водночас

може створювати труднощі у випадках необхідності виправлення помилок або зміни умов правовідносин.

Окрему проблему становлять питання доказування та правозастосування. Для належної оцінки інформації, що міститься у блокчейні, суди та інші органи повинні володіти спеціальними знаннями у сфері інформаційних технологій. Це зумовлює необхідність формування нових підходів до використання цифрових доказів та залучення технічних експертів.

Перспективи розвитку блокчейн-технологій у корпоративному праві пов'язані з подальшою цифровізацією корпоративного управління, розвитком цифрових активів, інтеграцією корпоративних реєстрів із державними електронними сервісами та створенням нових організаційно-правових форм ведення бізнесу. Особливий інтерес викликає концепція децентралізованих автономних організацій (DAO), діяльність яких ґрунтується на використанні блокчейну та смарт-контрактів для прийняття управлінських рішень без централізованого керівного органу.

Для ефективного впровадження блокчейну в корпоративні правовідносини необхідно забезпечити комплексний підхід, який включатиме вдосконалення законодавства, розробку технічних стандартів, розвиток судової практики та підготовку фахівців, здатних працювати на перетині права й інформаційних технологій. Важливим завданням також є гармонізація національного регулювання із міжнародними та європейськими стандартами цифрової економіки.

Отже, блокчейн є однією з ключових технологій, здатних суттєво змінити сучасні корпоративні правовідносини. Його використання сприяє підвищенню прозорості, безпеки та ефективності корпоративного управління, створює передумови для автоматизації корпоративних процедур та розвитку нових форм здійснення господарської діяльності. Водночас успішна інтеграція блокчейн-технологій у корпоративне право потребує належного нормативного забезпечення, технічної стандартизації та адаптації правозастосовної практики до викликів цифрової епохи.

Калітенко Оксана Михайлівна
кандидатка юридичних наук, доцентка,
професорка кафедри приватного права
Національного університету “Одеська юридична академія”

ВРАЗЛИВІСТЬ ПРИВАТНОЇ ОСОБИ ПЕРЕД ЦИФРОВИМИ ЗАГРОЗАМИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ: ДО ФОРМУВАННЯ СУЧАСНОЇ ЦИВІЛІСТИЧНОЇ ДОКТРИНИ

Сучасний етап розвитку приватного права характеризується глибокими трансформаціями, зумовленими стрімкою цифровізацією суспільних відносин, що особливо загострюються в умовах гібридної війни. Цифровий простір, який донедавна розглядався переважно як середовище комунікації та економічної взаємодії, нині набуває ознак повноцінного простору конфлікту, де поєднуються інформаційні операції, кібератаки, маніпулятивні технології та використання систем штучного інтелекту. У цьому контексті приватна особа дедалі частіше опиняється у стані підвищеної вразливості, що обумовлює необхідність переосмислення традиційних цивілістичних підходів до захисту її прав та інтересів.

Цифровізація соціальних зв'язків істотно змінює характер загроз, які виникають для приватної особи в сучасному світі. Якщо в класичній цивілістиці домінували ризики, пов'язані з майновими посяганнями або порушенням особистих немайнових прав у фізичному середовищі, то в цифрову добу ці ризики трансформуються у складні, багаторівневі та часто латентні форми. Йдеться, зокрема, про незаконне збирання та обробку персональних даних, цифрову ідентифікацію без належної згоди, втручання у приватне життя через цифрові платформи, а також про вплив алгоритмічних рішень, здатних визначати доступ особи до ресурсів, послуг або соціальних можливостей. Умови гібридної війни лише посилюють ці процеси, оскільки цифрові технології використовуються не лише для економічних чи соціальних цілей, але й як інструменти цілеспрямованого впливу на населення.

У таких умовах особливої актуальності набуває необхідність формування категорії «вразливість приватної особи» як самостійного приватно-правового (цивілістичного) концепту. На відміну від традиційного розуміння вразливості, яке пов'язувалося переважно з фізичним станом особи, віком або соціальним статусом, сучасна вразливість має значно ширший, динамічний характер. Вона обумовлюється не лише індивідуальними характеристиками особи, але й її включеністю у цифрове середовище, рівнем цифрової грамотності, доступом до технологій, а також ступенем залежності від цифрових сервісів. Відтак доцільно визначати вразливість приватної особи як об'єктивно зумовлений стан підвищеної чутливості до правопорушень у цифровому середовищі, що виникає внаслідок поєднання технологічних, соціальних та правових факторів і потребує спеціальних цивільно-правових механізмів захисту.

Розвиток категорії вразливості приватної особи у цивілістичній доктрині має еволюційний характер і відображає загальні тенденції трансформації приватного права від формально рівного до матеріально орієнтованого на захист слабшої сторони. Традиційно вразливість розглядалася через призму окремих, чітко визначених правових статусів – малолітніх, неповнолітніх, осіб із обмеженою дієздатністю, споживачів, а також інших суб'єктів, які потребують підвищеного рівня правового захисту. У цих випадках вразливість визнавалася як виняткова характеристика, що обґрунтовувала відступ від принципу юридичної рівності сторін та застосування спеціальних правових гарантій.

Подальший розвиток приватного права, особливо під впливом європейських підходів, сприяв поступовому розширенню розуміння вразливості. Вона почала розглядатися не лише як статичний статус, а як функціональна категорія, що залежить від конкретних обставин правовідносин, рівня поінформованості сторін, їх економічної спроможності та здатності впливати на зміст правочину. Такий підхід особливо проявився у сфері договірної

права, де концепція слабшої сторони стала одним із ключових інструментів забезпечення справедливого балансу інтересів.

У сучасних умовах цифровізації суспільства та гібридних загроз відбувається подальша трансформація цієї категорії. Вразливість приватної особи набуває нової якості, оскільки вона більше не обмежується ані традиційними соціальними групами, ані класичними видами правовідносин. Цифрове середовище створює ситуації, в яких навіть формально рівні учасники можуть перебувати у нерівному становищі через різний рівень доступу до інформації, технологій та механізмів впливу на процес прийняття рішень. У цьому сенсі вразливість стає універсальною характеристикою цифрових правовідносин, що проявляється залежно від контексту, а не лише від правового статусу особи.

Особливого значення ця трансформація набуває в умовах гібридної війни, коли цифрові технології використовуються як інструмент цілеспрямованого впливу на поведінку, свідомість і правове становище особи. Вразливість у таких умовах посилюється не лише технологічними факторами, але й інформаційним тиском, маніпулятивними практиками та підвищеним рівнем невизначеності. Це зумовлює необхідність переходу від фрагментарного нормативного закріплення окремих випадків вразливості до формування цілісної цивілістичної доктрини, здатної враховувати динамічний характер сучасних загроз.

Таким чином, розвиток категорії вразливості приватної особи демонструє поступовий перехід від вузького, статусного розуміння до широкого, контекстуального та динамічного підходу, який відповідає реаліям цифрового суспільства. У цьому процесі ключовим завданням цивілістичної науки стає не лише опис нових проявів вразливості, але й формування таких правових конструкцій, які забезпечуватимуть ефективний захист прав особи в умовах постійно змінюваного цифрового середовища.

Категорія «вразливості» (vulnerability) у сучасному праві вже набула нормативного закріплення в низці правопорядків, однак її використання має фрагментарний, галузевий характер і поки що

не сформувалося як універсальна приватно-правова конструкція. Водночас аналіз зарубіжного законодавства дозволяє констатувати стійку тенденцію до інституціоналізації вразливості як юридично значущої категорії, насамперед у сферах захисту прав людини, споживчого права, міграційного права та цифрового регулювання.

У межах європейського правового простору найбільш послідовно категорія вразливості розробляється на рівні права Європейського Союзу. Зокрема, у споживчому праві ЄС активно використовується концепція «вразливого споживача» (*vulnerable consumer*). Вона закріплена, зокрема, у Directive 2005/29/EC, де вразливими визнаються особи, які через вік, фізичні чи психічні особливості або довірливість є особливо сприйнятливими до недобросовісних комерційних практик. Ця конструкція фактично вводить критерій підвищеного рівня правового захисту, що прямо корелює з ідеєю матеріальної, а не формальної рівності сторін.

Подальший розвиток цієї категорії простежується у новітніх актах ЄС, пов'язаних із цифровим середовищем. Так, Digital Services Act передбачає спеціальні гарантії для вразливих користувачів цифрових платформ, зокрема дітей, а також встановлює підвищені вимоги до прозорості алгоритмів і захисту прав користувачів. Аналогічні підходи містяться і в AI Act, де прямо враховується ризик експлуатації вразливих груп при використанні систем штучного інтелекту, що свідчить про поступове перенесення концепції вразливості у сферу технологічного регулювання.

Цифрові загрози у період гібридної війни виступають одним із ключових факторів формування такої вразливості. Вони характеризуються масштабністю, швидкістю поширення та складністю виявлення, що істотно ускладнює можливість ефективного захисту прав приватної особи традиційними юридичними засобами. Зокрема, кібератаки можуть призводити до втрати доступу до цифрових активів або персональних даних, інформаційні операції – до порушення права на честь, гідність та ділову репутацію, а використання штучного інтелекту – до прийняття рішень, які

впливають на правове становище особи без належної прозорості та підконтрольності. У сукупності ці фактори формують нову якість правової реальності, у якій приватна особа стає значно менш захищеною порівняно з класичними правовими моделями.

Цивільно-правові механізми захисту, сформовані у межах традиційної доктрини, виявляються частково недостатніми для ефективного реагування на такі виклики. Вони орієнтовані переважно на індивідуальні правопорушення, тоді як цифрові загрози часто мають масовий, системний або транскордонний характер. У зв'язку з цим постає необхідність їх переосмислення та адаптації до нових умов. Йдеться про розширення підходів до відшкодування шкоди, завданої у цифровому середовищі, удосконалення механізмів захисту персональних даних, розвиток інструментів превентивного захисту, а також запровадження підвищених стандартів відповідальності для суб'єктів, що здійснюють обробку інформації або використовують системи штучного інтелекту.

Водночас вирішення зазначених проблем неможливе без формування сучасної цивілістичної доктрини вразливості приватної особи. Така доктрина має стати теоретичною основою для розробки нових підходів до правового регулювання цифрових відносин, у яких ключовим орієнтиром виступатиме не лише формальна рівність сторін, але й фактичний баланс їхніх можливостей у цифровому середовищі. Це передбачає визнання вразливості як юридично значущої категорії, що впливає на обсяг правового захисту, характер правових засобів та рівень відповідальності інших учасників правовідносин.

У цьому контексті доцільно запропонувати розгорнуте визначення досліджуваної категорії, яке відображало б її багатовимірний характер та відповідало сучасним умовам цифровізації й гібридних загроз. Тож вразливість приватної особи в сучасному цифровому світі доцільно розуміти як об'єктивно зумовлений і динамічний правовий стан особи, що виникає внаслідок її включеності у цифрове середовище та характеризується підвищеною чутливістю до порушень її майнових і особистих немайнових прав через

асиметрію інформаційних, технологічних і організаційних можливостей учасників правовідносин, складність або непрозорість цифрових процесів, а також обмежену здатність особи ефективно контролювати використання власних даних, цифрових ідентифікаторів і результатів алгоритмічних рішень.

Кармолін Лев Маркович

*магістр права Національного університету
«Одеська юридична академія»*

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПІД ЧАС ЗДІЙСНЕННЯ ПРАВОСУДДЯ

Сучасний етап розвитку інформаційного суспільства характеризується активною цифровою трансформацією державного управління та правової системи. Відтак, впровадження технологій штучного інтелекту у сферу правосуддя розглядається як один із ключових напрямів модернізації судової влади та підвищення ефективності правозастосовної діяльності.

Здатність алгоритмічних систем обробляти значні обсяги інформації, аналізувати складні закономірності та здійснювати прогнозування правових результатів створює нові можливості для оптимізації функціонування судових органів.

У науковій літературі штучний інтелект у сфері правосуддя визначається як сукупність технологічних рішень, що використовують методи машинного навчання, аналізу великих даних та автоматизованого прийняття рішень для підтримки юридичної діяльності [1, с. 21-38].

Основними напрямками застосування таких технологій є аналіз судової практики, автоматизація документообігу, систематизація правових позицій та прогнозування можливих результатів судового розгляду.

Вищевказане свідчить про те, що використання відповідних систем дозволяє значно скоротити час, необхідний для пошуку правової інформації, а також сприяє підвищенню узгодженості судової практики.

Важливим елементом цифрової трансформації правосуддя є впровадження електронних судових систем, зокрема в Україні таким інструментом стала підсистема «Електронний суд», яка забезпечує електронний документообіг між судом і учасниками процесу, дистанційне подання процесуальних документів та онлайн-доступ до матеріалів справи тощо.

Використання цифрових технологій у судовій діяльності сприяє підвищенню прозорості правосуддя, оптимізації адміністративних процедур та забезпеченню доступності судового захисту [2].

Разом із тим застосування штучного інтелекту у сфері правосуддя пов'язане з низкою правових та етичних викликів, зокрема з ключових проблем є забезпечення прозорості алгоритмів та можливості пояснення рішень, прийнятих із використанням систем машинного навчання.

Функціонування таких систем за принципом «чорної скриньки» ускладнює перевірку логіки прийняття рішень, що може створювати ризики порушення права на справедливий суд.

Особливу увагу в міжнародній практиці приділяють проблемі алгоритмічної упередженості, адже системи штучного інтелекту можуть відтворювати існуючі соціальні або правові дисбаланси, що зумовлює необхідність формування етичних стандартів їх застосування.

Важливим міжнародним документом у цій сфері є Європейська етична хартія щодо використання штучного інтелекту в судових системах та оточуючих їх реаліях, прийнята Радою Європи 3 грудня 2018 року. У ній визначено основні принципи застосування штучного інтелекту: повага до прав людини, недискримінація, забезпечення якості та безпеки даних, прозорість і підзвітність, а також контроль з боку людини [3].

У вітчизняній правовій доктрині також приділяється увага етичним аспектам використання цифрових технологій. Зокрема, Ульянова Галина Олексіївна наголошує на необхідності дотримання принципів академічної доброчесності та недопущення зловживань цифровими інструментами, що є релевантним і у контексті застосування штучного інтелекту в судовій діяльності [4].

Значним кроком у розвитку міжнародного правового регулювання стало ухвалення 13 березня 2024 року Регламенту Європейського Союзу про штучний інтелект (Artificial Intelligence Act), який запровадив ризико-орієнтований підхід до класифікації систем штучного інтелекту.

Системи, що застосовуються у сфері правосуддя, віднесені до категорії високого ризику, що передбачає підвищені вимоги до прозорості, контролю з боку людини та захисту фундаментальних прав [5].

Таким чином, використання штучного інтелекту у сфері правосуддя має значний потенціал для підвищення ефективності судової системи, проте його впровадження повинно здійснюватися з дотриманням принципів верховенства права, забезпечення прозорості алгоритмічних рішень, недопущення дискримінації та збереження визначальної ролі судді у процесі здійснення правосуддя тощо.

ЛІТЕРАТУРА:

1. Баранов О.А. Правові аспекти національних стратегій розвитку штучного інтелекту. *Юридична Україна*. 2019. № 7. С. 21-38.
2. Офіційний портал судової влади України. Електронний суд. URL: <https://court.gov.ua>.
3. European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems. Council of Europe, 2018. URL: <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>.
4. Ульянова Г. О. Порушення академічної доброчесності відповідно до проекту закону про академічну доброчесність. *Європейські орієнтири розвитку України: нові виміри у воєнний час* : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 16 трав. 2025 р.) : у 2 т. Одеса : Фенікс, 2025. Т. 2. С. 207-210. URL: <https://dspace.onua.edu.ua/items/2a6395c8-6599-4c0c-b513-606feec1dad>.
5. Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. 2024. URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>.

Кірсанов Олексій Володимирович,
*аспірант кафедри цивільно-правових дисциплін
Одеського державного університету внутрішніх справ*

Берназ-Лукавецька Олена Михайлівна
*кандидатка юридичних наук, доцентка,
доцентка кафедри приватного права
Національного університету «Одеська юридична академія»*

ОКРЕМІ НЕСПРАВЕДЛИВІ УМОВИ КРЕДИТНОГО ДОГОВОРУ

Актуальність аналізу несправедливих умов кредитного договору в сучасній доктрині цивільного права зумовлена низкою правових, економічних і соціальних чинників, які безпосередньо впливають як на стабільність цивільного обороту, так і на ефективність захисту прав приватних осіб.

У сучасних реаліях більшість кредитних договорів оформлюється у формі договорів приєднання, де умови повністю визначає банк або інша фінансова установа. Це створює постійну небезпеку зловживань з боку сильнішої сторони (кредитора), яка за допомогою складних юридичних формулювань та прихованих застережень перекладає основний тягар майнових ризиків на позичальника. Вивчення правових механізмів виявлення та усунення таких несправедливих умов має ключове значення для забезпечення фундаментальних принципів справедливості, добросовісності та розумності.

У зв'язку з продовженням дії правового режиму воєнного стану в Україні, запроваджені державою тимчасові пільги та мораторії на нарахування штрафів та пені стимулюють певних кредиторів шукати обхідні правові механізми для збереження своїх надприбутків. Зокрема, це стосується впровадження прихованих щоденних комісій, механізмів квазі-пронлонгацій та капіталізації відсотків. Аналіз подібних практик з точки зору доктрини *fraus legis* (дій в обхід закону) є вкрай актуальним. Це необхідно як для захисту майнових прав громадян, так і для запобігання соціальному напруженню, пов'язаному з надмірною закредитованістю населення.

Також, ми бачимо, що гармонізація українського законодавства зі стандартами Європейського Союзу, зокрема щодо імпле-

ментації положень Директиви ЄС 93/13/ЕЕС про недобросовісні умови в договорах зі споживачами, вимагає створення чітких юридичних критеріїв для формування так званих «чорних» і «сірих» списків договірних положень.

Наразі вітчизняна судова практика, включаючи висновки Великої Палати Верховного Суду, перебуває на етапі активного розвитку, що потребує ґрунтовного теоретичного осмислення. Це важливо для впровадження принципу *contra proferentem*, який передбачає тлумачення неоднозначних умов на користь споживача, на системному рівні.

Розглянемо основні з таких несправедливих умов кредитного договору.

Так, однією з таких умов є спроба замаскувати заборонену під час дії воєнного стану неустойку (штрафи та пені) під інші правові механізми. Діюче законодавство однозначно забороняє нараховувати штрафні санкції за прострочення кредитних платежів у цей період, однак окремі кредитори обходять цю норму, вводячи умови на кшталт «автоматичної зміни тарифікації» чи «плати за сервісне обслуговування у випадку невиходу на зв'язок». Наприклад, у договорах може бути прописано, що у разі несвоєчасного платежу базова процентна ставка, обмежена законом, автоматично змінюється на підвищену «щоденну ставку за користування коштами після строку».

Другою категорією несправедливих умов можна вважати нав'язування «штучно» створених супутніх послуг – часом їх вартість навіть перевищує розмір самого кредиту. Яскравий приклад такого підходу – це обов'язкове страхування (життя, здоров'я або майна від воєнних ризиків), що здійснюється виключно у страховій компанії, обраній самим кредитором [1].

При цьому оплата страхового полісу відбувається не рівномірно протягом усього строку кредитування, а разово, одразу при видачі позики, і зазвичай утримується безпосередньо з суми кредиту. Також нерідко трапляються умови про обов'язкову оплату таких послуг, як «юридичний супровід кредитної справи», «смс-інформування за завищеною вартістю» або «видача довідок

про стан рахунку». Так, наприклад, Ощадбанк підняв оплату за цю послугу до 480 гривень на рік [2]. У більшості випадків вони не дають реальної цінності для споживача, оскільки є звичайними елементами операційної діяльності банку.

На практиці ми також стикаємося з тим, що у договорах онлайн-кредитування часто зустрічається положення, за яким у разі неможливості своєчасного погашення боргу система автоматично стягує з картки позичальника кошти, оформлені як «плата за пролонгацію» на новий термін. При цьому сплачені кошти йдуть виключно на покриття відсотків, залишаючи суму основного боргу незмінною. Такий підхід створює умови для затягування людини у безкінечну боргову спіраль.

Усі зазначені умови разом призводять до серйозного правового та майнового дисбалансу, за якого банк або інша фінансова установа повністю захищає себе від макроекономічних ризиків, тоді як позичальник залишається наодинці з надмірним фінансовим тягарем. Це повністю порушує принципи добросовісності та розумності у договірних відносинах.

ЛІТЕРАТУРА:

1. Страхування від військових ризиків. URL: <https://taslife.com.ua/lifemarket/strahuvannya-vid-vijskovykh-ryzykiv>
2. Платні SMS стають розкішшю: «Ощадбанк» підняв тарифи на сповіщення до 480 гривень на рік. URL: https://expert.in.ua/groshi/platni-sms-stayut-rozkishshyu-oshhadbank-pidnyav-taryfy-na-spovishhennya-do-480-gryven-na-rik/#google_vignette
3. Берназ-Лукавецька О.М. Кредитні канкули : досвід зарубіжних країн. Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів ХХІ століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 17 черв. 2022 р.) за заг. ред. С. В. Ківалова. Одеса : Гельветика, 2022. Т. 2. С. 624-625.
4. Кірсанов О.В., Берназ-Лукавецька О.М. Визнання кредитного договору недійсним як спосіб захисту цивільних прав. *Правнича мова в галузі приватного права* : матер. кругл. столу 29 березня 2024 р., С. 13-15.
5. Кірсанов О.В., Берназ-Лукавецька О.М., Онлайн кредитування в умовах воєнного стану. *Римське право і сучасність : реалізація і захист речових прав в умовах воєнного стану* : матер. Всеукр. конфер. Одеса, 2024 (25 травня). С. 16-18.

Кривенко Юлія Василівна
*кандидатка юридичних наук, доцентка,
доцентка кафедри приватного права
Національного університету «Одеська юридична академія»*

DEEPFAKE ЯК ПІДСТАВА ЦИВІЛЬНО-ПРАВОВОЇ ВІДПОВІДАЛЬНОСТІ: ВИКЛИКИ ГІБРИДНОЇ ВІЙНИ

Сучасне суспільство характеризується стрімким розвитком цифрових технологій не лише у сфері глобальних економічних процесів, а й у сфері моделей соціальних та суспільних взаємодій на різних рівнях. Вдосконаленню deepfake-технологій сприяє процес швидкої модернізації програмного забезпечення та консолідації професійної спільноти програмістів.

Нові технологічні можливості, пов'язані з дипфейком, несуть серйозні ризики. Перелік загроз починається з окремої особи або групи користувачів і сягає рівня державних інтересів.

Упродовж останніх років технологія дипфейку набула широкого поширення серед користувачів. Більшість із них сприймають дипфейк як нову форму онлайн-гумору та розваг, а не як інструмент обману чи шантажу. З кожним роком технологія дипфейку вдосконалюється, і відрізнити справжні відеоматеріали від підроблених стає дедалі складніше. Потерпають не лише знаменитості та публічні особи, а й пересічні користувачі. Кар'єра та репутація людини можуть бути скомпрометовані й повністю зруйновані, а підроблені відеоматеріали зі світовими лідерами здатні спричинити дипломатичні конфлікти та навіть збройні зіткнення. На законодавчому рівні вкрай складно врахувати всі аспекти розвитку та застосування сучасних технологій, тому соціальні мережі намагаються самостійно впроваджувати інструменти, що обмежуватимуть використання технології дипфейку.

Слід врахувати, що технологія дипфейк набула широкого поширення в умовах відсутності нормативного регулювання. Таким чином вона підриває засади демократії, дестабілізує довіру громадян до органів державної влади та правових інститутів, вводить виборців в оману, а також становить загрозу громадській безпе-

ці та загострює соціальні суперечності в сучасних умовах російсько-української війни.

Наприклад, 16.03.2022 мережею почав ширитися дипфейк з Президентом України В. Зеленським. У відео він нібито звернувся до народу України із закликом скласти зброю. Проте творці дипфейку не змогли правильно синтезувати голос президента, колір обличчя відрізнявся від кольору тіла, саме тіло було занадто статичне, міміка обмежена. Пізніше фейкове відео видалили зі своїх платформ Facebook та Instagram.

Російські пропагандисти поширюють у тіктоці відео зі згенерованими штучним інтелектом військовими, які, нібито перебуваючи на різних ділянках фронту, розповідають про «обвал оборони» та «проникнення російських військ у фланги». [1]

Голова Донецької облдержадміністрації, начальник обласної військової адміністрації Вадим Філашкін повідомив, що в мережі поширюється дипфейкове відео з начебто його коментарем про ситуацію в Покровській громаді.

У сфальшованому відео йдеться про те, що начебто місцеві жителі організовують мітинги проти ЗСУ, конфліктують з військовими, а тому в громаді буде проведена примусова евакуація населення. Ця інформація не відповідає дійсності.

«Голос на відео не належить мені, а озвучена інформація повторює російські пропагандистські наративи та покликана спричинити напруження в суспільстві», — заявив Вадим Філашкін і закликав усіх уважно ставитись до інформації в інтернеті та довіряти тільки офіційним джерелам. [2]

Потік дезінформації набув такого масштабу, що чимало соціальних мереж взяли за протидію дипфейкам. Facebook і Twitter запроваджують автоматичне виявлення та видалення підроблених відео. Великі технологічні корпорації — зокрема Microsoft і Amazon — вкладають кошти в розробку програмного забезпечення для розпізнавання фейкових матеріалів. Над вирішенням цієї проблеми працює й наукова спільнота.

Цивільно-правова відповідальність за створення та поширення дипфейк-контенту має ґрунтуватися на загальній конструк-

ції цивільного правопорушення, передбаченій ЦК України, однак кожен із чотирьох елементів складу набуває специфічного змісту в умовах цифрового середовища.

Коло потенційних відповідачів у дипфейк-спорах не обмежується безпосереднім автором синтетичного контенту. Залежно від обставин справи, до нього можуть належати такі суб'єкти як: автор дипфейку, замовник або особа, яка профінансувала створення дипфейку, платформа або соціальна мережа, поширювач контенту, засіб масової інформації.

Окрему категорію становлять дипфейки, що створюються та поширюються державними структурами держави-агресора як інструмент інформаційної війни. У такому разі відповідальність виходить за межі класичного цивільно-правового делікту і підлягає розгляду в контексті міжнародно-правової відповідальності та репараційних механізмів, що наразі формуються в рамках реакції міжнародної спільноти на збройну агресію проти України.

Отже, ефективний цивільно-правовий захист від дипфейку потребує не лише застосування наявних загальних норм ЦК України, а й запровадження спеціального регулювання, яке б визначило порядок сповіщення платформ, строки реагування, розподіл тягара доказування та механізми забезпечення позову щодо цифрового контенту.

ЛІТЕРАТУРА:

1. Горон Д. В тіктоці поширюють ШІ-дипфейки з військовими, які розповідають про «обвал української оборони», ЦПД. URL: <https://detector.media/infospace/article/246425/2025-12-18-v-tiktotsi-poshyryuyut-shi-dypfeyky-z-viyskovymy-yaki-rozpovidayut-pro-obval-ukrainskoi-oborony-tspd/>
2. Голос на відео не належить мені: ворог запустив «дипфейк» про ситуацію в Покровську. URL: <https://armyinform.com.ua/2024/09/28/golos-na-video-ne-nalezhyt-meni-vorog-zapustyv-dipfejk-pro-sytuacziyu-v-pokrovsku/>
3. Цивільний кодекс України : Кодекс України; Закон, Кодекс від 16.01.2003 № 435-IV. URL: <https://zakon.rada.gov.ua/go/435-15>

Ларіонов Владислав Сергійович
аспірант кафедри права інтелектуальної власності
та патентної юстиції
Національного університету
«Одеська юридична академія»

ПРАВОВА ПРИРОДА ТА КЛАСИФІКАЦІЯ ЦИФРОВИХ РЕЧЕЙ У КОНТЕКСТІ ОНОВЛЕННЯ ЦИВІЛЬНОГО ЗАКОНОДАВСТВА УКРАЇНИ

Цивільне законодавство багатьох країн світу зараз переживає часи значних змін. Необхідність адаптації до нової реальності, що стрімко стала частиною повсякденного життя за останні декілька років, зумовлює появу законодавчих ініціатив, що спрямовані на врегулювання суспільних відносин в епоху цифрової економіки.

Класичне розуміння «речі» як фізичного об'єкта все більше розмивається. У цифровій економіці на перший план виходять цифрові речі, серед яких віртуальні активи, NFT, криптогаманці, цифровий контент.

Закон України від 10.08.2023 № 3320-IX «Про внесення змін до Цивільного кодексу України щодо розширення кола об'єктів цивільних прав» доповнив Цивільний кодекс новими об'єктами цивільних прав. Так, ст. 177 ЦК України закріпила такі види об'єктів цивільних прав: речі, гроші, цінні папери, цифрові речі, майнові права, роботи та послуги, результати інтелектуальної, творчої діяльності, інформація, а також інші матеріальні та нематеріальні блага. Об'єкти цивільних прав можуть існувати у матеріальному світі та/або цифровому середовищі, що обумовлює форму об'єктів, особливості набуття, здійснення та припинення цивільних прав і обов'язків щодо них.

Новації, закріплені у ст. 177 ЦК України, відображають фундаментальний перехід від традиційного «права речей» до права «цифрових активів». Вперше у переліку об'єктів цивільних прав поряд із традиційними речами, грошима та цінними паперами з'являються цифрові речі. Це означає визнання їхньої самостійної майнової цінності.

Фізична присутність у матеріальному світі більше не є необхідною для того, щоб володіти річчю, розпоряджатися нею, а також захищати свої права і законні інтереси щодо таких речей.

Також Закон України № 3320-IX у ст. 179-1 закріпив у цивільному законодавстві поняття цифрової речі. Відповідно до ст. 179-1 ЦК України цифровою річчю є благо, що створюється та існує виключно у цифровому середовищі та має майнову цінність. Цифровою річчю є віртуальні активи, цифровий контент та інші блага, щодо яких застосовуються положення частини першої цієї статті.

За визначенням цифрова річ – це перш за все благо, тобто об’єкт, що може задовольнити певну потребу власника або користувача цього об’єкта. Перелік цифрових речей у Цивільному кодексі не є вичерпним. Серед цифрових речей законодавець виділив віртуальні активи та цифровий контент.

У випадку із цифровим контентом законодавча згадка обумовлена необхідністю імплементації норм законодавства Європейського Союзу та гармонізації українського законодавства із Директивою Європейського Парламенту і Ради (ЄС) від 20 травня 2019 року № 2019/770 про деякі аспекти, що стосуються договорів про постачання цифрового контенту та цифрових послуг.

2 березня 2024 року набрав чинності Закон України «Про цифровий контент та цифрові послуги», який закріпив, зокрема, такі поняття як цифровий контент і цифрова послуга. Відповідно до цього Закону, цифровий контент – це дані, які створюються і надаються в цифровій формі. До цифрового контенту належать, зокрема, комп’ютерні програми, застосунки, відеофайли, аудіофайли, музичні файли, цифрові ігри та електронні книги.

Як видно із визначення, цифровий контент – це перш за все товари із цифровим елементом, які створюються авторами цього контенту і потім комерціалізуються через введення у цивільний обіг.

Також цим Законом введено поняття цифрової послуги як послуги, що надає можливість споживачу створювати, обробля-

ти, зберігати та поширювати дані у цифровій формі або отримувати доступ до таких даних, а також здійснювати будь-які інші дії з даними у цифровій формі, що були створені чи завантажені споживачем або іншими користувачами такої послуги. До цифрових послуг належать, зокрема такі, що дають змогу створювати, обробляти, отримувати доступ або зберігати дані в цифровій формі, включаючи хостинг файлів, обробку текстів або гри, які пропонуються в середовищі хмарних обчислень і соціальних мережах.

Разом із цифровим контентом, цифрові послуги формують значну частину ринку електронної комерції. Закріплення їхніх визначень, а також чітке нормативне регулювання їхнього розповсюдження, створюють підґрунтя для цивілізованого комерційного обігу та можливості для споживачів отримати якісні товари та послуги у цифровому середовищі і за необхідності захистити свої права як покупця цифрового контенту або цифрової послуги.

Окремим видом цифрових речей, що отримали пряме законодавче закріплення, є віртуальні активи. Потреба у їхній нормативній фіксації зумовлена стрімким розвитком технологій розподіленого реєстру, масовим обігом криптовалют та NFT, а також стратегічним завданням держави щодо інтеграції цих активів у легальний економічний простір та встановлення механізмів їхнього прозорого оподаткування.

Законодавче визначення віртуальних активів як різновиду цифрових речей є відповіддю на виклики цифрової економіки. Це дозволяє трансформувати фактичні відносини щодо криптовалют та токенизованих активів у юридично значущі цивільні правовідносини, забезпечуючи правовий інструментарій для їхнього захисту, відчуження та фіскального регулювання.

Закон України «Про віртуальні активи» від 17.02.2022 № 2074-IX, який набере чинності з дня набрання чинності законом України про внесення змін до Податкового кодексу України щодо особливостей оподаткування операцій з віртуальними активами,

визначає віртуальний актив як нематеріальне благо, що є об'єктом цивільних прав, має вартість та виражене сукупністю даних в електронній формі. Існування та оборотоздатність віртуального активу забезпечується системою забезпечення обороту віртуальних активів. Віртуальний актив може посвідчувати майнові права, зокрема права вимоги на інші об'єкти цивільних прав.

Отже, віртуальний актив – це певна логічна послідовність цифрових даних, яка ідентифікується в мережі Інтернет. Іншою важливою ознакою віртуального активу є наявність вартості. Це може дозволити використовувати віртуальні активи як об'єкти застави, включати до статутного капіталу юридичних осіб, фіксувати збитки у разі викрадення або блокування активу, бути об'єктом спадкуваннятощо.

Контроль над віртуальним активом здійснюється не через фізичне володіння, а через технічну можливість розпоряджатися даними в межах певної системи, що забезпечує його оборот. Якщо система припиняє існування, юридично актив може бути визнаний таким, що втратив оборотоздатність.

Також варто відзначити, що сучасне цивільне законодавство України перебуває у фазі фундаментальної трансформації, центром якої є переосмислення правової природи цифрових об'єктів. Опублікований у січні 2026 року Проект Цивільного кодексу України (Кодексу права приватного) репрезентує амбітну стратегію рекодифікації, спрямовану на створення адаптивного та ефективного регуляторного інструментарію. Нова архітектура Кодексу покликана забезпечити правову визначеність у динамічному цифровому середовищі, відповідаючи актуальним викликам технологічного прогресу.

Проект Цивільного кодексу виділяє цифрові речі серед об'єктів приватних відносин. Проект визначає цифрову річ як благо, що створене та наявне лише в цифровому середовищі і має майнову цінність.

Згідно з Проектом до цифрових речей належать: віртуальні активи; цифровий контент, бази даних, зображення, зокрема 3D-моделі; доменні імена та облікові записи в цифрових системах; інші об'єкти.

Така розширена класифікація цифрових речей є досить прогресивною новелою Проекту Цивільного кодексу України. На відміну від попередніх законодавчих змін, Проект не обмежується виключно віртуальними активами, а включає до правового регулювання доменні імена, облікові записи в цифрових системах, 3D-моделі.

Таким чином, цифрові речі можна буде вважати виокремленими у самостійну категорію об'єктів приватних відносин. Визначення цифрової речі як блага, що існує виключно у цифровому середовищі та має майнову цінність, дозволяє остаточно подолати доктринальну невизначеність щодо статусу нематеріальних активів та створити надійний фундамент для застосування до цифрових об'єктів класичних інститутів права: власності, спадкування, застави та судового захисту.

ЛІТЕРАТУРА:

1. Про внесення змін до Цивільного кодексу України щодо розширення кола об'єктів цивільних прав: Закон України від 10 серпня 2023 року № 3320-IX. URL: <https://zakon.rada.gov.ua/laws/show/3320-20>.
2. Цивільний кодекс України від 16 січня 2003 № 435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15>.
3. Про цифровий контент та цифрові послуги: Закон України від 10 серпня 2023 року № 3321-IX. URL: <https://zakon.rada.gov.ua/laws/show/3321-20>.
4. Про віртуальні активи: Закон України від 17 лютого 2022 року № 2074-IX. URL: <https://zakon.rada.gov.ua/laws/show/2074-20>.
5. Проект Цивільного кодексу України (Кодексу права приватного) від 22 січня 2026 № 14394. URL: <https://itd.rada.gov.ua/billinfo/Bills/Card/69528>

Маковій Віктор Петрович
кандидат юридичних наук, професор
завідувач кафедри цивільно-правових дисциплін інституту права та
безпеки
Одеського державного університету внутрішніх справ

ТРАНСФОРМАЦІЯ ПРАВОВОГО РЕГУЛЮВАННЯ ЦИФРОВОГО СЕРЕДОВИЩА З ОГЛЯДУ НА ПРОЄКТ КОДЕКСУ ПРАВА ПРИВАТНОГО

Умови сьогодення характеризуються поєднанням низки факторів, які справляють доленосний вплив на формування та розвиток приватних відносин, покликаних забезпечити реалізацію кола приватних прав та інтересів особи у поєднанні із охороною публічних інтересів суспільства. Серед таких: екзистенціальні загрози національним інтересам у розрізі положень Закону України «Про національну безпеку», глобалізаційні тенденції розвитку людства, інтеграція українського суспільства до європейської спільноти, транзитивний розвиток національних та світової економік, багаторівневе та прогресуюче втілення цифровізації у всіх сферах суспільного буття посередництвом соціально-економічних, технічних, організаційно-правових інструментів. Вказані фактори мають низку спільнокоренових процесів, пріоритетне місце в числі яких варто надати невід’ємному атрибуту інформаційного суспільства процесу створення, поширення та використання інформації та її різноманітних втілень з використанням цифрових обчислювальних машин. Безумовно, суспільні відносини, в межах яких відбуваються вказані явища, за допомогою яких забезпечується реалізація приватних прав та інтересів осіб, безпосередньо являються предметом правового регулювання цивільного права, визначальною формою якого є Цивільний кодекс України.

Вказані вище процеси в питомій вазі послуговували передумовою до проєктування змін у цивільно-правовому регулюванні суспільних відносин в умовах сьогодення, що виразилося у розробці та впровадженні моделі рекодифікації (оновлення) Цивільного кодексу України, відображеній у відповідній Концепції оновлення Цивільного кодексу України (надалі – Концепція) [1]. Наслідком

реалізації Концепції стало напрацювання проєкту Цивільного кодексу України (Кодексу права приватного) (надалі – Проєкт) з відповідними положеннями [2]. Як Концепція, так і Проєкт містять положення, присвячені питанням трансформації приватноправового регулювання суспільних відносин з огляду на цифровізацію всіх сфер суспільного буття, що може бути охарактеризовано наступним чином.

По-перше, реалізація змісту таких спеціальних законодавчих актів як Закон України «Про стимулювання розвитку цифрової економіки в Україні», Закон України «Про електронну комерцію», Закон України «Про електронні комунікації», Закон України «Про електронну ідентифікацію та електронні довірчі послуги», Закон України «Про цифровий контент та цифрові послуги», Закон України «Про віртуальні активи» потребує релевантного приватноправового нормативного матеріалу у Цивільному кодексі України (надалі – ЦК України).

По-друге, структура та зміст ЦК України має відображати основні тенденції інформаційного суспільства, серед яких визначальною є саме діджиталізація всіх галузей економіки.

По-третє, серед прав людини як основного примату цивілізованого суспільства особливе місце займають цифрові права, виникнення, здійснення, трансформація та припинення яких пов'язане з процесом відповідної обробки, кодування інформації з використанням цифрових обчислювальних машин.

По-четверте, укладення тенденцій цифровізації суспільного буття у формулу співіснування західної моделі інформаційного суспільства «інформаційне суспільство = громадянське суспільство» [3, с. 596-597], де ЦК України виділена основоположна роль.

По-п'яте, імплементація до ЦК України міжнародних стандартів у даній сфері, відтворених зокрема у Європейській декларації про цифрові права та принципи, Декларації про свободу спілкування в Інтернеті, Декларації про майбутнє Інтернету, Рекомендаціях ЮНЕСКО щодо етики штучного інтелекту, Директиві ЄС «Про певні аспекти стосовно договорів поставки цифрового контенту та надання цифрових послуг» тощо.

Необхідно зважити на поступальність дій розробників Концепції щодо впровадження закладених у ній ідей у зміст Проєкту, у тому числі й в розрізі приватноправового регулювання цифрового середовища. Проєктом передбачено відображення цифрової форми у структурі цивільних правовідносин з огляду на ознаку ідентифікації осіб як їх учасників, спеціальний правовий режим об'єктів, а також особливості здійснення їх змісту (природи та відрізняльних рис цифрових прав, вчинення цифрових правочинів та контрактів тощо). Розробниками Концепції у контексті наведеного виокремленні питання щодо запровадження цифрової форми правочину задля забезпечення функціонування електронної комерції, старт-контрактів, веб-банкінгу та інших інструментів цифрової економіки, розвитку положень про цифрові права особи, прояву спеціальних правових модусів, у тому числі цифрової (електронної) особи, розширення кола переліку об'єктів цивільних прав цифровими благами, захисту персональних даних та посилення права на приватність у цифровому середовищі.

Аналіз Проєкту свідчить про відтворення особливостей правового регулювання приватних відносин у контексті: ідентифікації особи через відповідні цифрові інструменти, визначення правового режиму цифрових речей, окреслення кола немайнових прав особи, вчинення (укладення) правочину (договору) у цифровому середовищі, правового режиму речових прав щодо цифрової речі та права інтелектуальної власності стосовно цифрових об'єктів, реалізації зобов'язальних відносин у цифровому середовищі, а також здійснення спадкових прав щодо цифрових об'єктів.

Разом з тим, з огляду на висловлене наявні певні неузгодженості нормативних приписів Проєкту у розрізі предмету даного дослідження, що в певній мірі релевантне відтвореним протиріччям суджень та умовиводів авторів Концепції. Так, спірним є питання визначення правової природи цифрових речей як визначального терміну, пов'язаного з діджиталізацією приватних відносин. Так, ст. 199 Проєкту визначає річчю предмет матеріального світу, щодо якого можуть виникати цивільні права та

обов'язки. Ст. 202 Проекту визначає цифрову річ як благо, що створене та наявне лише в цифровому середовищі. Притому, що деталізація правового режиму цифрових речей має визначати закон, під яким вочевидь розуміється низка законодавчих актів, як-то Закон України «Про віртуальні активи», де віртуальним активом є нематеріальне благо, Закон України «Про цифровий контент та цифрові послуги», в якому детермінується поняття «цифровий контент» як сукупність даних, які створюються і надаються в цифровій формі, та «цифрове середовище», в якому забезпечується доступ до цифрового контенту та/або цифрової послуги й можливість їх використання. З іншого боку маємо у ст. 593 Проекту норму, за якою визначається правовий режим права інтелектуальної власності та права власності на матеріальний чи електронний (цифровий) об'єкт, в якому втілено об'єкт права інтелектуальної власності.

Наведений підхід фактично з одного боку повторює модель цифрової речі, яка міститься у положеннях чинного ЦК України. Однак, частиною 2 ст. 177 ЦК України здійснена диференціація об'єктів як таких, що можуть існувати у матеріальному світі та (або) цифровому середовищі. Подібний підхід створює передумови до формування декількох термінологічних підходів до формування підмножин у системі об'єктів цивільних прав: матеріальних та нематеріальних, цифрових та нецифрових. При цьому слушним буде буквальне сприйняття змісту наведеної норми ЦК України, де мова йде про форму відображення того чи іншого об'єкта з огляду на використану логічну операцію, що пов'язує відповідні предикативні конструкції (кон'юнкція чи дез'юнкція): у цифровому середовищі або матеріальному світі, у цифровому середовищі та матеріальному світі одночасно.

У наукових дослідженнях цивільно-правової природи цифрових об'єктів наявні міркування, що диференціюють цифровий контент на матеріальний (ототожнюється з правовим режимом речей) та нематеріальний, який охоплює майнові та особисті немайнові права автора. При цьому висловлюється думка, згідно якої

цифровий контент асоціюється із природою інформаційного блага та є комплексним інститутом, що охоплюється не тільки нормами права інтелектуальної власності [4, с. 46].

Розробники концепту оновлення ЦК України теж у цьому питанні висловлюють суперечливі міркування, які з одного боку свідчать про відмову від теорії «безтілесних речей», пояснюючи це недопустимістю спрощення правової регламентації цифрових об'єктів до правового режиму речей (майна) [5, с. 132-136], а з іншого – запровадження пропрієтарної моделі сприйняття віртуальних активів з відповідними наслідками [5, с. 269-274], що відображене у згаданих положеннях проєкту.

Безумовно, наведені суперечності та прогалини Проєкту є питанням складності визначення правової природи вказаних правових явищ, а тому стануть предметом подальших розробок поряд з унормуванням правового регулювання суспільних відносин щодо штучного інтелекту, трансформації у цифровому середовищі інших приватноправових конструкцій.

ЛІТЕРАТУРА:

1. Концепція оновлення Цивільного кодексу України. URL: <https://www.rada.gov.ua/uploads/documents/76363.pdf>.
2. Проєкт Цивільного кодексу України (Кодексу права приватного) від 22.01.2026 № 14394. URL: <https://itd.rada.gov.ua/billinfo/Bills/Card/69528>.
3. Харитонов Є.О., Харитонova О.І. Приватне право як концепт. Том III. Концепт приватного права і рекодифікації цивільного законодавства в Україні: рефлексії фронтиру: монографія. Одеса: Фенікс, 2019. 752 с.
4. Трофименко Д.С., Федоренко Д.О. Проблемні аспекти розуміння правової природи цифрового контенту. *Juris Europensis Scientia*. 2022. №1. С. 43-47.
5. Рекодифікація цивільного законодавства України: виклики часу: монографія / за заг. ред. Н. С. Кузнєцової. Одеса: Вид. дім «Гельветика», 2021. 690 с.

Майданик Роман Андрійович

*доктор юридичних наук, професор, професор Київського
національного університету імені Тараса Шевченка,
головний науковий співробітник Науково-дослідного інституту
приватного права та підприємництва імені Ф. Г. Бурчака
Національної академії правових наук України*

ШТУЧНИЙ ІНТЕЛЕКТ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я: АКТУАЛЬНІ ПИТАННЯ ПРАВА

Штучний інтелект має значний вплив на всіх учасників відносин у сфері охорони здоров'я, що може сприяти значному підвищенню ефективності та доступності медичних послуг.

Застосування штучного інтелекту трансформує сферу охорони здоров'я, завдяки якій пацієнти отримують нову надію. Від діагностики до лікування на основі штучного інтелекту – ці досягнення здатні рятувати життя, подовжувати тривалість життя та покращувати його якість.

Однак їхнє впровадження також породжує важливі етичні та правові виклики, зокрема необхідність забезпечити передбачуваність і доступність цих технологій для всіх зберігаються значні нерівності і правова невизначеність.

Це дослідження містить огляд окремих актуальних питань права, що виникають внаслідок використання штучного інтелекту в сфері охорони здоров'я з урахуванням кращої світової практики.

Основною метою цього дослідження є проведення загальної характеристики правових та етичних концепцій, сучасних тенденцій і практичного застосування штучного інтелекту в сфері охорони здоров'я.

У дослідженні висвітлюються такі питання: стан використання ШІ на ринку медицини (1), загальні принципи використання ШІ (2), ШІ як інноваційна технологія у сфері охорони здоров'я (3), тенденції та приклади використання ШІ, які впливають на взаємовідносини «пацієнт-лікар» (4), виклики ШІ у відносинах «пацієнт-лікар» (5), ШІ у відносинах «пацієнт-лікар» та основоположні права людини (6).

1. Стан використання ШІ на ринку медицини

Еволюція розвитку штучного інтелекту має циклічний характер: періоди великого інтересу та інвестицій змінювалися розчаруванням і критикою (так звані «зими штучного інтелекту»). Ми щойно пережили довге і спекотне літо штучного інтелекту в медицині [1].

Зростання ринку зумовлене потребою у більш ефективній діагностиці, персоналізованому лікуванні та оптимізації роботи медичних закладів охорони здоров'я. Старіння населення, поширення хронічних захворювань та збільшення обсягу медичних даних створюють умови для широкого впровадження ШІ у медичну практику.

Основні сфери застосування ШІ в медицині включають: автоматизоване тлумачення медичних зображень; підтримку клінічних рішень; роботизовані операції; персоналізовану медицину; управління адміністративними процесами.

Ключові гравці ринку активно розробляють нові продукти та розширюють співпрацю з медичними закладами.

Експерти прогнозують, що впровадження ШІ у сфері охорони здоров'я продовжить зростати, змінюючи підходи до діагностики, лікування та управління медичними процесами.

2. Загальні принципи використання ШІ

Активне використання ШІ, зокрема в сфері охорони здоров'я, має врегулюватися правовими нормами і правилами професійної етики. Право має визначати визначальні положення (принципи) створення, встановлення та використання заснованих на штучному інтелекті автоматизованих систем, у поєднанні з демократичними цінностями та захистом прав, свобод та приватності.

Учасники правовідносин із використанням штучного інтелекту повинні бути захищені від небезпечних та неефективних систем, розроблятися та використовуватися на засадах:

- повідомлення та пояснення про використання щодо особи систем ШІ,
- недискримінації та справедливості,
- бути захищеними від практик зловживання даними через впроваджені способи захисту та

- нагляд особи за тим, як використовуються її дані,
- особа має знати як автоматизована система використовується та розуміти як та хто впливає на результат, який має відношення до особи, дані якої використовуються або іншим чином впливає на її права, свободи та інтереси,
- особа повинна мати однакові можливості доступу до критично важливих матеріальних й інших соціальних благ,
- особа має бути здатною відмовитися, у допустимих випадках, та мати допуск до особи, яка може швидко розглянути та забезпечити захист прав, свобод та інтересів, якого потребує особа.

3. ШІ як інноваційна технологія у сфері охорони здоров'я

Сучасна сфера охорони здоров'я використовує широке коло інноваційного лікування та технологій у медицині, до яких зазвичай відносять персоналізовану або точну медицину, репродуктивну медицину, генне редагування, імунотерапією, наномедицину, нейрохірургію, цифрову терапію, діагностику на місці надання медичної допомоги (Point-of-care, POC), телемедицину, робототехніку, технології 3D-друку та штучний інтелект (ШІ). Ці технології можуть бути або безпосередньо інтегровані в терапевтичні процедури, або використовуватися як самостійні методи лікування [2].

ШІ є інформаційною системою, яка демонструє властиву людині «розумну» поведінку за допомогою аналізу навколишнього середовища та вжиття заходів для досягнення конкретних цілей. «Розумна» поведінка ШІ базується на машинному навчанні та алгоритмах прогнозування, що дають можливість навчатися на досвіді та автоматично покращувати свою ефективність за рахунок засвоювання представлення даних із різними рівнями абстракції з метою поступового підвищення точності прогнозів.

4. Тенденції та приклади використання ШІ, які впливають на взаємовідносини «пацієнт-лікар»

ШІ використовується для автоматизації лікарняних процесів, дистанційного моніторингу пацієнтів, у машинному зорі, вбу-

дованому в хірургію з використанням роботів, для прискорення розробки лікарських препаратів, у взаємодії з пацієнтами за допомогою чат-ботів, у персоналізації планів лікування, а також у прогностичних алгоритмах на основі самонавчання для допомоги в інтерпретації медичних зображень та прогнозуванні клінічних результатів [2].

ШІ має потенціал для значного перетворення взаємовідносин «пацієнт-лікар», хоча наслідки їхнього впровадження для цих відносин ще невідомі.

5. Виклики ШІ у відносинах «пацієнт-лікар»

Використання ШІ ускладнює для регуляторних органів, закладів охорони здоров'я та медичних працівників оцінювання безпеки та ефективності медичних послуг при визначенні того, чи пропонують ці інновації поліпшення порівняно з існуючими стандартами медичної допомоги, зокрема внаслідок динамічного характеру та невизначеності щодо безпеки та ефективності цих інноваційних технологій.

Інноваційні методи лікування часто стикаються з труднощами при узагальненні результатів досліджень на різноманітні групи пацієнтів, оскільки ранні клінічні випробування зазвичай проводяться в контрольованих умовах і зосереджуються на вузькоспецифічних групах пацієнтів. У цих випробуваннях часто відсутня достатня репрезентативність ключових демографічних груп, таких як жінки, люди похилого віку, етнічні меншини або пацієнти з рідкісними захворюваннями чи супутніми захворюваннями, що призводить до нерівномірних результатів лікування при застосуванні в реальних клінічних умовах.

ШІ, що використовується в медицині, має потенціал значно покращити процес прийняття клінічних рішень, але він також несе ризик алгоритмічної упередженості, особливо коли ці технології ґрунтуються на незбалансованих або неповних базах даних.

Для зменшення алгоритмічної упередженості необхідні постійні зусилля для забезпечення того, щоб бази даних, які використовують для навчання ШІ, були інклюзивними та репрезентативними для різноманітних груп населення, а також, щоб системи

ШІ оцінювалися та контролювалися на предмет упередженості їхніх результатів за допомогою систем порівняльного аналізу упередженості та різноманітних команд, що оцінюють якість даних [3].

Впровадження ШІ в охороні здоров'я створює унікальні виклики, насамперед через брак прозорості, пояснюваності та відтворюваності. Моделі ШІ, що функціонують як «чорні скриньки», можуть надавати високоточні результати, але роблять майже неможливим для медичних працівників зрозуміти логіку їхніх рішень, що погіршує здатність оцінювати доцільність рекомендацій щодо лікування, згенерованих ШІ, та виявляти потенційні помилки й упередження. Як наслідок, медичні працівники можуть або надто покладатися на ШІ, або взагалі відкидати його, і те, і інше може негативно вплинути на догляд за пацієнтами.

Медичні працівники можуть надмірно покладатися на рекомендації ШІ, не розуміючи повністю медичного обґрунтування, що з часом може призвести до зниження критичного мислення та діагностичних навичок.

Для зменшення цих ризиків надзвичайно важливо ретельно керувати переходом до медичного обслуговування на основі ШІ. Слід встановити чіткі керівні принципи та правила щодо розробки та використання систем ШІ, гарантуючи, що ці системи проходять ретельну валідацію через клінічні випробування та підлягають регуляторним стандартам для забезпечення їхньої безпеки та надійності. Також важливо підтримувати та надавати можливості медичним працівникам під час цього переходу, просувати мінімальні стандарти щодо інформації та пояснюваності в системах ШІ, а також гарантувати, що ШІ в сфері охорони здоров'я перебуває під значущим людським контролем.

6. ШІ у відносинах «пацієнт-лікар» та основоположні права людини

Застосування ШІ у відносинах «пацієнт-лікар» має відповідати основоположним правам людини як пацієнта, зокрема щодо автономії (стаття 5, Конвенції Ов'єдо), професійних стандартів (стаття 4 Конвенції Ов'єдо), самовизначення щодо медичних пер-

сональних даних (стаття 10 Конвенції Ов'єдо) та справедливого доступу до медичної допомоги (стаття 3 Конвенції Ов'єдо, права на однаковий і справедливий доступ до медичної допомоги (стаття 3 Конвенції Ов'єдо).

Розробка, розвиток та застосування ІІІ в медицині повинні здійснюватися таким чином, щоб «інтереси та благополуччя людини превалювали над виключними інтересами усього суспільства або науки» (Див.: Стаття 2 Конвенції Про захист прав і гідності людини щодо застосування біології та медицини: Конвенція про права людини та біомедицину, Ов'єдо, 4 квітня 1997 року.).

Цим зумовлена необхідність взаємного доповнення прогресу та заходів захисту, що забезпечуються системами ІІІ [4].

Для збереження юридично та етично правильних відносин «пацієнт–лікар» із використанням ІІІ необхідно передбачати спільне прийняття рішень, звернення за інформацією та поясненнями (до медичних працівників, постачальників ІІІ, технічних співробітників) щодо того, як і кому системи ІІІ дають певні результати, щоб забезпечити дотримання професійних стандартів та автономії пацієнта. З цією метою пацієнт і медичні працівники повинні мати право вимагати надання інформації про логіку, сферу застосування та наслідки рекомендацій, наданих ІІІ.

Своєчасний доступ до належної медичної допомоги – а отже, і доступ до інноваційних методів лікування та технологій – є не привілеєм, а питанням прав людини. У цьому контексті рівний доступ до ІІІ у сфері охорони здоров'я означає лікування й інші медичні послуги, які адаптовані до індивідуальних медичних потреб та враховує існуючі нерівності, з метою забезпечення того, щоб кожен міг ефективно отримати належний рівень медичної допомоги.

Будь-яке втручання у сфері охорони здоров'я, включаючи наукові дослідження, має здійснюватися відповідно до відповідних професійних обов'язків та стандартів.

Надання медичних послуг відповідно до професійних обов'язків і стандартів передбачає обов'язок лікарів піклуватися про пацієнтів та визначати належне лікування в межах спільного

прийняття рішень разом із пацієнтом. Вжиті заходи ґрунтуються на компетентності, наукових знаннях та клінічному досвіді, що включає оцінку ризиків (систем ШІ, наприклад, Закон ЄС про ШІ та Конвенція Ради ЄС про ШІ, права людини, демократію та верховенство права).

Висновки. 1. На сучасному етапі спостерігається значне зростання використання ШІ у сфері охорони здоров'я, що зумовлено потребою у більш ефективній діагностиці, персоналізованому лікуванні та оптимізації роботи медичних закладів охорони здоров'я.

2. Активне використання ШІ, зокрема в медицині, повинно бути врегульованим у праві та правилах професійної етики. Право має визначати визначальні положення (принципи) створення, встановлення та використання заснованих на штучному інтелекті автоматизованих систем, у поєднанні з демократичними цінностями та захистом прав, свобод та приватності.

3. ШІ є інформаційною системою, яка демонструє властиву людині «розумну» поведінку за допомогою аналізу навколишнього середовища та вжиття заходів для досягнення конкретних цілей.

4. Виклики використання ШІ у відносинах «пацієнт – лікар» пов'язані з оцінкою якості лікування, проблемами щодо можливості узагальнення результатів досліджень, алгоритмічною упевненістю, складнощами у визначенні професійних стандартів.

5. Розробка, розвиток та застосування ШІ в медицині повинні здійснюватися таким чином, щоб «інтереси та благополуччя людини превалювали над виключними інтересами усього суспільства або науки». Цим зумовлена необхідність взаємного доповнення прогресу та заходів захисту, що забезпечуються системами ШІ.

6. Для збереження юридично та етично правильних відносин «пацієнт–лікар» із використанням ШІ необхідно передбачати спільне прийняття рішень, звернення за інформацією та поясненнями щодо того, як і кому системи ШІ дають певні ре-

зультати, щоб забезпечити дотримання професійних стандартів та автономії пацієнта.

7. Доступ до ШІ у сфері охорони здоров'я повинен ґрунтуватися на правах людини, а рівність має бути його керівним принципом.

ЛІТЕРАТУРА:

1. Ethical, safe, lawful A toolkit for artificial intelligence projects. Linklaters. 2024. URL: https://edge.sitecorecloud.io/linklaterslbf57-linklatersx7ccc-linklatersxf9f5-394d/media/digital-marketing-image-library/files/06_ckp/2024/june/74194_001-linklaters-ai-digital-handbook-a4-l_4.pdf

2. WHITE PAPER Equitable and timely access to appropriate innovative treatments and technologies in healthcare Steering Committee for Human Rights in the fields of Biomedicine and Health (CDBIO). September 2025. Council of Europe. Pp. 14–16. URL: <https://rm.coe.int/white-paper-equitable-and-timely-access-to-appropriate-innovative-trea/488028aae7>

3. Пояснювальна доповідь до Конвенції про захист прав людини та гідності людини в контексті застосування біології та медицини: Конвенція щодо прав людини та біомедицини, параграф 24. URL: <https://rm.coe.int/16800ccde5>

4. REPORT ON THE APPLICATION OF ARTIFICIAL INTELLIGENCE IN HEALTHCARE AND ITS IMPACT ON THE ‘PATIENT-DOCTOR’ RELATIONSHIP Steering Committee for Human Rights in the fields of Biomedicine and Health (CDBIO). Council of Europe. September 2024. P. 6. URL: <https://rm.coe.int/cdbio-2023-7-rev3-ai-report-web-e/1680b17b35>

Матійко Микола Володимирович

кандидат юридичних наук, доцент,

доцент кафедри приватного права

Національного університету «Одеська юридична академія»

ЩОДО ОКРЕМИХ АСПЕКТІВ РЕГУЛЯТИВНОГО ФУНКЦІОНУВАННЯ ЦИВІЛЬНОГО ПРАВА В СФЕРІ НАДАННЯ ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ ПОСЛУГ КІНЦЕВОМУ КОРИСТУВАЧУ

Електронні комунікації є дуже важливою технічною складовою інформаційної сфери. Особливої важливості останнім часом набули розвиток ринків доступу до електронних комунікаційних мереж та ринків електронних комунікаційних послуг, на якому

має базуватися розгортання та використання електронних комунікаційних мереж високої та надвисокої пропускнуї здатності, розвиток конкуренції, сумісність електронних комунікаційних послуг, отримання більш якісних послуг для кінцевих користувачів.

Під комунікацією розуміються «шляхи сполучення, лінії зв'язку тощо»[1, С. 245], під електронним – «пов'язаний із застосуванням властивостей електрона, заснований на їх використанні»[2, С. 471]. Відповідно до статті 2 Закону України «Про електронні комунікації» електронна комунікація (телекомунікація, електрозв'язок) являє собою передавання та/або приймання інформації незалежно від її типу або виду у вигляді електромагнітних сигналів за допомогою технічних засобів електронних комунікацій. Відповідно до статті 2 Закону України «Про електронні комунікації» електронна комунікаційна послуга – це послуга, що полягає в прийманні та/або передачі інформації через електронні комунікаційні мережі, крім послуг з редакційним контролем змісту інформації, що передається за допомогою електронних комунікаційних мереж і послуг. При цьому під електронною комунікаційною мережею розуміється – комплекс технічних засобів електронних комунікацій та споруд, призначених для надання електронних комунікаційних послуг.

Варто зауважити, що «інформаційно-комунікаційна складова – один із базових елементів поняття електронної комерції»[3, С. 28], оскільки остання відповідно до п.1 ч.1 ст.3 Закону України «Про електронну комерцію» електронна комерція – відносини, спрямовані на отримання прибутку, що виникають під час вчинення правочинів щодо набуття, зміни або припинення цивільних прав та обов'язків, здійснені дистанційно з використанням інформаційно-комунікаційних систем, внаслідок чого в учасників таких відносин виникають права та обов'язки майнового характеру. Разом з цим відповідно до п. 13 ч.1 ст.3 Закону України «Про електронну комерцію» послуга проміжного характеру в інформаційній сфері – послуга з передачі та/або зберігання інформації та присвоєння мережевих ідентифікаторів. З огляду на зміст статті 6

цього закону учасниками відносин у сфері електронної комерції є суб'єкти електронної комерції, постачальники послуг проміжного характеру в інформаційній сфері, органи державної влади та органи місцевого самоврядування в частині виконання ними функцій держави або місцевого самоврядування. Постачальниками послуг проміжного характеру в інформаційній сфері є постачальники електронних комунікаційних послуг, оператори послуг платіжної інфраструктури, реєстратори (адміністратори), що присвоюють мережеві ідентифікатори, та інші суб'єкти, що забезпечують передачу та зберігання інформації з використанням інформаційно-комунікаційних систем.

При цьому «зобов'язання щодо надання послуг можуть виникати в різних сферах людської діяльності і опосередковуватися цивільно-правовими договорами. Вибір форми регулювання конкретного різновиду зобов'язальних відносин залежить від виду послуги і форми вираження її результату. Диференціація зобов'язань проводиться за характером діяльності виконавця послуги... Оскільки спектр послуг постійно розширюється, їх вичерпний перелік скласти неможливо. Саме на цій підставі законодавець пропонує договором про надання послуг охоплювати будь-які види послуг, що відповідають установленим цивільним законодавством критеріям»[4, С. 366]. Звертає на себе увагу думка, згідно якої «в економічній науці послуги розуміються і як вид діяльності, і як вид економічного блага. Виходячи з цього, можна припустити, що кожне з цих значень опосередковується адекватною правовою формою»[5, С. 563]. Разом з цим згідно статті 901 Цивільного кодексу України за договором про надання послуг одна сторона (виконавець) зобов'язується за завданням другої сторони (замовника) надати послугу, яка споживається в процесі вчинення певної дії або здійснення певної діяльності, а замовник зобов'язується оплатити виконавцеві зазначену послугу, якщо інше не встановлено договором. Положення глави 63 Цивільного кодексу України можуть застосовуватися до всіх договорів про надання послуг, якщо це не суперечить суті зобов'язання. Отже «положення ст. 901-907 ЦК

підлягають застосуванню до відносин, предметом яких є послуги, як вони визначаються в ч.1 ст. 901 ЦК» [6, С. 365].

Розділом XIV Закону України «Про електронні комунікації» встановлюються особливості надання електронних комунікаційних послуг кінцевим користувачам. При цьому кінцевий користувач послуг розуміється як користувач послуг, який не надає електронних комунікаційних послуг.

Постачальники електронних комунікаційних послуг не повинні застосовувати дискримінаційні умови надання електронних комунікаційних послуг для кінцевих користувачів з причин, пов'язаних з громадянством кінцевого користувача, місцем його проживання або місцем надання послуги, якщо такі відмінності (обмеження) не обумовлені технічними та економічними умовами надання електронних комунікаційних послуг чи іншими об'єктивними причинами відповідно до правил надання та отримання електронних комунікаційних послуг.

Умовами надання та отримання електронних комунікаційних послуг кінцевому користувачу є: укладення договору про надання електронних комунікаційних послуг відповідно до правил надання та отримання електронних комунікаційних послуг та інших актів законодавства; оплата замовленої кінцевим користувачем електронної комунікаційної послуги, якщо інше не передбачено Законом України «Про електронні комунікації» або договором про надання електронних комунікаційних послуг.

Законодавством серед інших виділяються послуги міжособистісної електронної комунікації. Під послугою міжособистісної електронної комунікації розуміється електронна комунікаційна послуга, що дає змогу здійснювати прямий міжособистісний та інтерактивний обмін інформацією через електронні комунікаційні мережі між обмеженою кількістю осіб, за якого особи, які ініціюють або беруть участь у комунікації, визначають одержувача (одержувачів) інформації (крім послуг, що дають змогу міжособистісного та інтерактивного спілкування лише як незначну допоміжну функцію, невід'ємно пов'язану з іншою послугою).

При цьому розрізняються послуга міжособистісної електронної комунікації без використання нумерації (послуга міжособистісної електронної комунікації, під час надання якої не використовується номер (номери) з національного чи міжнародних планів нумерації або не здійснюється зв'язок з номером (номерами) з національного чи міжнародних планів нумерації) та послуга міжособистісної електронної комунікації з використанням нумерації – послуга міжособистісної електронної комунікації, під час надання якої використовується номер (номери) з національного чи міжнародних планів нумерації або здійснюється зв'язок з номером (номерами) з національного чи міжнародних планів нумерації. Також при цьому постачальники послуг міжособистісних електронних комунікацій, за винятком послуг без використання нумерації, повинні забезпечувати відповідно до Законом України «Про електронні комунікації» та правил надання та отримання електронних комунікаційних послуг: сумісність електронних комунікаційних послуг, що надаються ними; можливість з'єднання кінцевих користувачів з номерами національного плану нумерації; дотримання вимог щодо захисту прав кінцевих користувачів електронних комунікаційних послуг.

Кінцевий користувач має право отримувати послугу знеособлено відповідно до правил надання та отримання електронних комунікаційних послуг та умов надання послуг, встановлених постачальником електронних комунікаційних послуг.

Кінцевий користувач, не ідентифікований постачальником електронних комунікаційних послуг, має право здійснити ідентифікацію в порядку, встановленому регуляторним органом, у тому числі дистанційну із застосуванням відповідно до законодавства у сферах електронної ідентифікації та електронних довірчих послуг будь-яких засобів електронної ідентифікації середнього та високого рівнів довіри, передбачених зазначеним порядком ідентифікації.

Постачальники електронних комунікаційних послуг повинні безоплатно надавати: послуги голосових електронних комуніка-

цій або послуги з передачі текстового повідомлення, якщо вони надаються абонентам для направлення (здійснення) ними благодійного електронно-комунікаційного повідомлення; послуги з перерахування коштів як благодійної пожертви на користь неприбуткової організації, у тому числі благодійної організації (крім політичних партій і кредитних спілок), або територіальної громади на виконання благодійного електронно-комунікаційного повідомлення, направленою (здійсненою) таким абонентом; послуги з публічного збору благодійних пожертв з використанням благодійного електронно-комунікаційного повідомлення згідно з договором, укладеним між постачальником електронних комунікаційних послуг та неприбутковою організацією, у тому числі благодійною організацією (крім політичних партій і кредитних спілок), або територіальною громадою. При цьому на суму коштів, перераховану постачальником електронних комунікаційних послуг на цілі благодійної діяльності, зібраних публічним збором благодійних пожертв з використанням благодійного електронно-комунікаційного повідомлення, зменшується аванс абонента за електронні комунікаційні послуги. Відповідна сума коштів списується з особового рахунку абонента.

Регулятивна функція цивільного права в сфері надання електронних комунікаційних послуг, що надаються кінцевому користувачу являє собою вплив цивільного права у регулятивному напрямку в сфері надання електронних комунікаційних послуг, що надаються кінцевому користувачу та регулятивне соціальне призначення цивільного права в сфері надання електронних комунікаційних послуг, що надаються кінцевому користувачу.

В регулятивній функції цивільного права в сфері надання електронних комунікаційних послуг кінцевому користувачу, можуть бути виділені нормативна та індивідуальна складові. Нормативна складова пов'язана із регулюванням відповідних суспільних відносин шляхом створення, зміни, доповнення або скасування норм цивільного права, тобто з правотворчою діяльністю в галузі цивільного права. Індивідуальна складова пов'язана з упоряд-

куванням на основі норм цивільного права суспільних відносин шляхом конкретизації масштабу поведінки їх суб'єктів після встановлення необхідних для цього фактів. Поряд із зазначеним з огляду на теоретичні розробки в регулятивній функції цивільного права в сфері надання електронних комунікаційних послуг кінцевому користувачу, може бути виділена складова саморегуляції (складова горизонтального регулювання). Прикладом тут може виступати договірне регулювання.

ЛІТЕРАТУРА:

1. Словник української мови. Білодід І.К. та ін. [В 11 т.] (1970-1980), Т. 4, 1973, 840 с.
2. Словник української мови. Білодід І.К. та ін. [В 11 т.] (1970-1980), Т. 2, 1971, 550 с.
3. Марченко В.Б. Правове забезпечення інформаційно-комунікаційної складової електронної комерції відповідно до Закону України «Про електронні комунікації». Науковий вісник Ужгородського Національного Університету, Серія ПРАВО. Вип. 75: Ч. 2. 2023., С.27-31.
4. Цивільне право України: Підручник У 3 кн. Кн.3. За ред. проф. Є.О. Харитонова. Одеса: Юридична література, 2006., 832 с.
5. Степанович Д. Г. Послуга як об'єкт цивільних прав. *Актуальні проблеми держави і права*. 2011. Вип. 59. , С.558-564.
6. Ярема А.Г., Карабань В.Я., Кривенко В.В., Ротань В.Г. Науково-практичний коментар до цивільного законодавства України: [В 4 т.] Т.3. К.: А.С.К.: Севастополь: Інститут юрид. дослідж., 2005, 928 с.

Менджул Марія Василівна

*докторка юридичних наук, професорка,
професорка кафедри цивільного права та процесу
ДВНЗ «Ужгородський національний університет»*

ЗАХИСТ ДІТЕЙ ВІД ЦИФРОВОГО НАСИЛЬСТВА ЯК ЕЛЕМЕНТ КІБЕРБЕЗПЕКИ

Захист дітей від цифрового насильства є важливою складовою кібербезпеки, потреба в якому обумовлена стрімким поширенням інформаційних технологій та активним використанням Інтернету, а також технології штучного інтелекту (далі – ШІ) неповнолітніми. Діти та підлітки в сучасному світі все частіше

стикаються з ризиками онлайн-середовища: кібербулінгом, шкідливим контентом, втручанням у приватне життя, неправомірним збором персональних даних та іншими формами цифрового насильства. Водночас, відсутність належної правової, освітньої та технічної захищеності створює потенційні загрози фізичному та психоемоційному здоров'ю неповнолітніх. Тому дослідження механізмів запобігання таким загрозам, розробка практичних рекомендацій для батьків, педагогів та органів публічної влади є важливим кроком для забезпечення безпечного використання цифрових ресурсів дітьми та підвищення загального рівня кібербезпеки в суспільстві.

На разі статистика доволі не втішна, за даними дослідження UNICEF 45 % дітей та підлітків в Україні страждали від кібербулінгу або онлайн-залякування [1]. Понад третина дітей в Україні стикалася хоча б з однією сексуальною загрозою в Інтернеті протягом останнього року. За результатами опитування, 33% дітей зазначили, що протягом року мали щонайменше один досвід небезпечної взаємодії он-лайн. Зокрема, 19,7% отримували запитання інтимного характеру, 13,2% – фото чи відео з оголеними тілами, а 12,6% стикалися з проханнями надіслати власні інтимні матеріали. Також 18,1% підлітків зустрічалися в реальному житті з людьми, з якими до того спілкувалися лише в Інтернеті. Ще 3,3% дітей повідомили, що проти них намагалися застосувати або вже використали сексуалізований контент, створений за допомогою штучного інтелекту. Водночас 59,6% дітей не повідомляли нікому про подібні випадки насильства або експлуатації в мережі [2].

В державах ЄС були проведені дослідження щодо випадків булінгу. У період 2021-2022 рр. рівень кібербулінгу щодо дітей, коливався від 7,5% в Іспанії до 27,1% у Литві, середній показник в Європі становив 15,5%. Поряд з Литвою, до країн з вищим рівнем кібербулінгу, ніж середній, належать Латвія, Польща, Англія, Угорщина, Естонія, Ірландія, Шотландія, Словенія, Швеція, Уельс, Фінляндія та Данія. Португалія, Греція та Франція також входять до числа країн з найнижчим рівнем кібербулінгу. У Ні-

меччині та Італії кібербулінг також був нижчим за середній показник по Європі [3].

Дослідження в ЄС у 2025 році, в якому взяли участь 6 343 дітей та підлітків віком від 12 до 17 років із усіх 27 країн Європейського Союзу. Серед учасників 57% становили дівчата, 40% – хлопці, 2% визначили себе як «інші» та ще 2% не надали інформації про стать. Результати показали, що майже чверть опитаних (24%) особисто зазнавали кібербулінгу, а 39% спостерігали подібні випадки у своїх знайомих. Ще половина респондентів знали когось, кого ображали в інтернеті, при цьому серед дівчат цей показник складав 52%, а серед хлопців – 40%. Діти також вважали, що найбільш уразливими до кібербулінгу є ті, хто відрізняється від інших, і що основними мотивами онлайн-знущань є «розвага та привернення уваги» (70%) та бажання «показати владу» (62%). Що стосується емоційного впливу кібербулінгу, то більшість дітей зазначали, що він викликає смуток (73%), психологічний біль (65%), почуття самотності чи ізоляції (62%), при цьому дівчата відчували це частіше, ніж хлопці (70% проти 52%). Також 59% відчували сором через ображення он-лайн. Щодо отримання підтримки, 62% дітей звернулися б до батьків або опікунів (67% дівчат, 56% хлопців), 41% – до друзів (46% серед 17-річних і 29% серед 12-річних), 25% – до вчителів чи шкільного персоналу (38% серед наймолодших і 19% серед старших), а 14% скористалися б гарячою лінією чи онлайн-платформою підтримки [4].

У відповідь на зростаючу загрозу та вимоги суспільства, Європейська Комісія розробила План дій проти кібербулінгу, що спрямовано на забезпечення дітей, батьків, опікунів та освітян необхідними інструментами для виявлення, повідомлення та боротьби з кібербулінгом. Під час підготовки плану було проведено широкі консультації за участю різних зацікавлених сторін, зокрема дітей, науковців, експертів та громадськості. План дій базується на трьох ключових напрямках: координована європейська політика захисту (План дій закликає держави-члени розробити національні політики протидії кібербулінгу, узгоджені на основі

спільного розуміння цього явища); профілактика та підвищення обізнаності (основною метою є формування у дітей з раннього віку здорових та відповідальних цифрових звичок і підвищення обізнаності щодо онлайн-ризиків. Для цього на рівні ЄС створюються різноманітні освітні інструменти та ресурси за участю дітей, батьків, освітян, експертів з психічного здоров'я, держав-членів та організацій, таких як Safer Internet Centres); механізми повідомлення та підтримки (План дій забезпечує чіткі та доступні шляхи повідомлення про кібербулінг для жертв, свідків, батьків та опікунів. Передбачено впровадження онлайн-додатку безпеки, який дозволяє дітям та підліткам швидко повідомляти про випадки кібербулінгу, збирати та надсилати докази, а також отримувати персоналізовану підтримку) [5].

В Україні прийнято Закон «Про основні засади забезпечення кібербезпеки України», в якому не враховано важливість захисту дітей від кібербулінгу, з огляду на це необхідно доповнити статтю 2 вказаного закону наступним принципом: «8) пріоритетного захисту дітей, згідно з яким усі рішення та заходи суб'єктів владних повноважень у сфері кібербезпеки повинні першочергово враховувати потребу захисту неповнолітніх осіб від кібербулінгу, онлайн-насилства та інших порушень у сфері використання інформаційно-комунікаційних систем, забезпечувати своєчасне попередження, реагування та захист для постраждалих у найкращих інтересах дитини».

ЛІТЕРАТУРА:

1. Nearly 95 per cent of children and young people actively check online sources. URL: <https://www.unicef.org/ukraine/en/press-releases/actively-check-online-sources>
2. Кожна третя дитина в Україні стикалася з сексуальними загрозами онлайн – дослідження. URL: <https://nus.org.ua/2026/03/06/kozhna-tretya-dytyna-v-ukrayini-stykalasya-z-seksualnymy-zagrozamy-onlajndoslidzhennya>
3. Cyberbullying among children rises in all European countries: Which are suffering the most? URL: <https://www.euronews.com/next/2025/12/08/>

cyberbullying-among-children-rises-in-all-european-countries-which-are-suffering-the-most

4. Children's Voices on Cyberbullying. URL: https://eu-for-children.europa.eu/cyberbullying_en

5. The Digital Services Act. URL: <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act>

Мусієнко Андрій Юрійович

аспірант кафедри приватного права

Національного університету «Одеська юридична академія»

ДО ПИТАННЯ ПРО РОЛЬ СУДОВОЇ ПРАКТИКИ В ПИТАННЯХ ЗАХИСТУ ПРАВ ВЛАСНИКІВ НЕЖИТЛОВИХ ПРИМІЩЕНЬ

У сучасних умовах розвитку цивільного обороту нерухомості в Україні особливого значення набуває проблема належного захисту прав власників нежитлових приміщень. Активне використання таких об'єктів у підприємницькій діяльності, зростання кількості комерційної нерухомості, реконструкцій, перепланувань та спорів щодо користування спільним майном багатоквартирних будинків зумовлюють збільшення кількості конфліктів у сфері реалізації та захисту права власності. Судова практика свідчить про наявність численних спорів щодо визначення правового режиму нежитлових приміщень, порядку їх використання, державної реєстрації речових прав, оскарження рішень органів місцевого самоврядування, витребування майна з чужого незаконного володіння, а також захисту прав добросовісного набувача.

Особливої актуальності ця проблематика набуває в контексті формування єдиної правозастосовної практики Верховного Суду щодо визначення належних способів захисту прав власників нежитлових приміщень, співвідношення приватних та публічних інтересів, а також розмежування допоміжних і нежитлових приміщень у багатоквартирних будинках. Водночас існуючі прогалини законодавчого регулювання та неоднозначність судових підходів ускладнюють ефективну реалізацію власниками своїх прав та потребують комплексного наукового осмислення.

Право власності є одним із фундаментальних приватних прав, гарантованих Конституцією України та цивільним законодавством. Особливе місце серед об'єктів цивільних прав займають нежитлові приміщення, які активно використовуються у сфері підприємницької, господарської, професійної та іншої діяльності. Розвиток ринку комерційної нерухомості, збільшення кількості об'єктів у багатоквартирних будинках, поширення практики реконструкції та перепланування приміщень обумовлюють зростання кількості судових спорів, пов'язаних із реалізацією та захистом прав власників нежитлових приміщень.

Відповідно до ст. 41 Конституції України кожен має право володіти, користуватися та розпоряджатися своєю власністю, а ніхто не може бути протиправно позбавлений права власності. Аналогічні положення закріплені у Цивільному кодексі України, який визначає право власності як право особи на річ, що здійснюється нею відповідно до закону за своєю волею та незалежно від волі інших осіб. При цьому власник має право вимагати усунення будь-яких порушень свого права, навіть якщо такі порушення не пов'язані з позбавленням володіння майном.

Особливістю правового режиму нежитлових приміщень є те, що вони можуть бути самостійними об'єктами нерухомості або складовими частинами багатоквартирного будинку. У зв'язку з цим у судовій практиці часто виникають спори щодо визначення правового статусу таких приміщень, розмежування нежитлових і допоміжних приміщень, а також обсягу прав власників щодо користування спільним майном будинку.

Однією з найбільш поширених категорій спорів є спори щодо визначення правового статусу приміщень у багатоквартирних будинках. Верховний Суд у своїй практиці неодноразово наголошував, що допоміжні приміщення призначені для забезпечення експлуатації будинку та побутового обслуговування мешканців, тоді як нежитлові приміщення є самостійними об'єктами цивільних прав і можуть використовуватися для здійснення підприємницької чи іншої діяльності. Неправильне визначення статусу

приміщення часто стає підставою для виникнення конфліктів між співвласниками будинку, органами місцевого самоврядування та власниками комерційних об'єктів.

Важливе значення у сфері захисту прав власників нежитлових приміщень мають спори, пов'язані з державною реєстрацією речових прав. На практиці нерідко виникають ситуації подвійної реєстрації прав на один і той самий об'єкт, незаконного внесення змін до реєстрів або реєстрації права власності на підставі документів, що не відповідають вимогам законодавства. У таких випадках власники змушені звертатися до суду з вимогами про скасування рішень державних реєстраторів, визнання недійсними правочинів або витребування майна з чужого незаконного володіння.

Судова практика свідчить про те, що ефективність захисту права власності значною мірою залежить від правильного вибору способу судового захисту. Зокрема, у випадках незаконного позбавлення володіння майном застосовується віндикаційний позов, а у разі створення перешкод у користуванні майном – негаторийний позов. Водночас власники нежитлових приміщень часто поєднують декілька способів захисту, наприклад вимоги про визнання права власності та скасування незаконної державної реєстрації.

Окрему категорію спорів становлять конфлікти, пов'язані з реконструкцією, переплануванням або самочинним будівництвом. На практиці власники нежитлових приміщень нерідко здійснюють переобладнання об'єктів без належних дозвільних документів або з порушенням будівельних норм. Це може призводити до порушення прав інших співвласників будинку, створення загроз безпечній експлуатації об'єкта чи обмеження доступу до спільного майна. У таких спорах суди, як правило, оцінюють не лише наявність правовстановлюючих документів, але й дотримання будівельного, містобудівного та житлового законодавства.

Не менш важливими є спори щодо користування спільним майном багатоквартирного будинку. Власники нежитлових приміщень мають право на користування спільним майном нарівні з

іншими співвласниками, однак на практиці виникають конфлікти щодо доступу до інженерних мереж, прибудинкової території, підвальних чи технічних приміщень. Судова практика свідчить про необхідність забезпечення балансу між інтересами власників житлових і нежитлових приміщень, а також недопущення дискримінаційних обмежень у реалізації права власності.

Аналіз судової практики дозволяє констатувати, що Верховний Суд поступово формує єдині підходи до вирішення спорів у сфері захисту прав власників нежитлових приміщень. Разом із тим залишається проблема неоднакового застосування норм права судами нижчих інстанцій, особливо у питаннях визначення правового статусу приміщень, співвідношення приватних та публічних інтересів, а також оцінки правомірності дій державних реєстраторів.

Суттєвим недоліком чинного законодавства є відсутність чіткого та системного визначення правового режиму нежитлових приміщень у багатоквартирних будинках. Нормативне регулювання міститься у різних актах цивільного, житлового, містобудівного та реєстраційного законодавства, що ускладнює їх практичне застосування. У зв'язку з цим доцільним є удосконалення законодавства шляхом конкретизації правового статусу нежитлових приміщень, порядку їх використання та меж здійснення прав власників.

Таким чином, захист прав власників нежитлових приміщень є складним комплексним інститутом, який поєднує норми цивільного, житлового, господарського та адміністративного права. Ефективність такого захисту залежить не лише від належного нормативного регулювання, але й від формування сталої та послідовної судової практики. Судова практика відіграє важливу роль у забезпеченні єдності правозастосування, конкретизації способів захисту порушених прав та забезпеченні балансу інтересів усіх учасників правовідносин у сфері використання нежитлових приміщень.

Орзiх Юрiй Геннадiйович

*кандидат юридичних наук, доцент, доцент кафедри приватного права Нацiонального унiверситету «Одеська юридична академiя»,
тaриший викладач в Унiверситетi Еребру (Швецiя)*

**КРИПТОАКТИВИ ЯК ЦИФРОВА ВЛАСНIСТЬ
В УМОВАХ ГIБРИДНОЇ ВIЙНИ: ПРАВО ВЛАСНОСТI,
ДОКАЗУВАННЯ КОНТРОЛЮ ТА AML/CFT-РИЗИКИ**

Проблема криптоактивiв в умовах гiбридної вiйни виходить за межi дискусiї про цифровi фiнансовi iнструменти. Криптоактиви можуть бути засобом швидкого транскордонного перемiщення вартостi, iнвестицiйним активом, об'єктом спадкування, дарування чи внеску до статутного капiталу, а також iнструментом приховування походження майна. Тому вони одночасно належать до площини приватного права, фiнансового монiторингу, кiбербезпеки та правозастосування. Для України, яка перебуває в умовах вiйни та гiбридних загроз, iх правовий режим має не лише ринковий, а й безпековий вимiр.

Європейський пiдхiд поступово формує двi взаємопов'язанi логiки: регулювання ринку криптоактивiв i запобiгання iх використанню для вiдмивання коштів та фiнансування тероризму. Вiдповiдно до MiCA, криптоактивом є цифрове представлення вартостi або права, яке може передаватися i зберiгатися електронно з використанням технологiї розподiленого реєстру або подiбної технологiї [1, ст. 3]. AMLR використовує близьку дефiнiцiйну логiку i поширює AML/CFT-вимоги на ширше коло постачальникiв послуг [2].

Однак для приватного права центральним є питання, чи може криптоактив бути об'єктом майнових прав, передаватися, бути предметом забезпечення, спадкування, дарування, подiлу майна або примусового виконання i сьогодні можна це питання вiдповiсти з позитивно. CNUE Guide розрiзняє криптовалюту, stablecoins, security tokens, utility tokens та NFTs, пiдкреслюючи, що такi криптоактиви є найбільш розповсюдженими i можуть виконувати платiжну, iнвестицiйну, посвiдчувальну або сервісну

функцію [3, с. 7]. Отже, цифрова власність не є однорідною категорією. Її правовий режим залежить від функції активу, способу набуття, форми зберігання та можливості встановити фактичний і правовий контроль.

Ключовим є розмежування між фактичним контролем і правом власності. Приватний ключ або доступ до wallet забезпечує можливість розпорядження активом, але сам по собі не завжди доводить законне набуття активу або виключне право особи на нього. Без врегульованого правом порядку обліку та реєстрації таких активів доказування права власності на нього у певної особи зводить до фактичного володіння активом, а інколи навіть і не самим активом і його носієм. CNUE Guide прямо вказує, що доступ до гаманця може демонструвати контроль, але не є абсолютним доказом права власності водночас підтверджуючи обов'язок нотаріуса перевіряти законність походження активу та право власності на актив у особи [3, с. 23-24]. Тому «контроль» є важливим доказовим індикатором, але не повним юридичним еквівалентом права власності.

Саме тут зростає роль нотаріуса. У традиційному цивільному обороті нотаріус виконує функцію гаранта правової визначеності, перевірки волевиявлення, дієздатності, повноважень, належності документів та законності правочину. Поява криптоактивів не усуває цієї функції, а підвищує її значення. Якщо криптоактив використовується у правочині з нерухомістю, при внеску до статутного капіталу, договорі позики, даруванні, поділі майна подружжя або спадкуванні, нотаріус має встановити юридичну підставу участі цифрового активу в правочині та оцінити ризики його незаконного походження.

CNUE Guide наголошує, що нотаріуси як суб'єкти, на яких поширюються AML/CFT-вимоги, відіграють істотну роль у моніторингу законності правочинів, а включення криптоактивів у юридичні операції створює нові ризики у сфері відмивання коштів і фінансування тероризму [3, с. 19]. В умовах гібридної війни це має особливе значення, адже приватно-правові конструкції

можуть використовуватися для легалізації активів, приховування зв'язку з підсанкційними особами або переміщення вартості поза банківським контролем.

Практична роль нотаріуса не повинна зводитися до технічного спостереження за доступом до гаманця. Нотаріальна перевірка має охоплювати встановлення особи та кінцевого бенефіціарного власника, з'ясування економічної мети правочину, перевірку джерела походження активів, аналіз зв'язку з регульованими або нерегульованими постачальниками послуг, оцінку підозрілих ознак транзакції, документування доказів контролю і передачі. Для hosted wallets можливими доказами можуть бути довідки від regulated exchangers чи wallet providers. Для self-hosted wallets можуть використовуватися digital signatures, screenshots with metadata, signed wallets, transaction history та дані blockchain explorers [3, с. 23-24].

Перевірка завершення передачі криптоактиву має окреме значення. Blockchain explorers дозволяють перевірити transaction ID або transaction hash, адреси учасників, суму, кількість підтверджень, дату, час і статус транзакції [3, с. 24]. У нотаріальному процесі це не перетворює блокчейн-дані на безспірний доказ права власності, але дає можливість фіксувати юридично значущі факти: наявність транзакції, її технічне завершення, відповідність заявлених адрес і часу, а також зв'язок між правочином і цифровим слідом. Окрім цього слід звернути увагу на необхідність приведення Закон України «Про нотаріат» у відповідність з потребами ринку криптоактивів.

Проблема примусового виконання щодо криптоактивів демонструє межі класичних правових інструментів. Якщо активи зберігаються у регульованого постачальника послуг, органи правозастосування можуть взаємодіяти з таким суб'єктом, отримувати інформацію, накладати обмеження або забезпечувати виконання рішення. Якщо активи зберігаються у self-hosted wallet, відсутній центральний адміністратор, який міг би виконати розпорядження державного органу. CNUE Guide зазначає, що в децентралізова-

них системах правоохоронним органам складно спрямувати дії на один центральний суб'єкт або місце для цілей розслідування чи арешту активів [3, с. 12].

AMLR виходить із того, що розвиток технологій створює нові продукти й системи обміну коштів або вартості, однак водночас породжує нові ризики ML/TF [2, п. 7 преамбули]. Для криптоактивів такими ризиками є псевдоанонімність, транскордонність, використання mixers, privacy coins, peer-to-peer transfers, self-hosted wallets та юрисдикцій зі слабким контролем. FATF також підкреслює необхідність risk-based approach, ліцензування або реєстрації VASPs, нагляду з боку компетентних органів та застосування до них релевантних AML/CFT-заходів [4].

У гібридній війні AML/CFT-ризики криптоактивів мають додатковий вимір: фінансування терористичної діяльності, обхід санкцій, приховування активів осіб, пов'язаних з агресором, кіберзлочини, ransomware-платежі, фінансування дезінформаційних або підривних мереж. Тому правове регулювання цифрової власності не може бути ізольованим від режимів фінансового моніторингу, санкційного контролю, кібербезпеки і доказового права. Нотаріус у такій моделі має виступати як gatekeeper правової довіри, який не допускає надання формальної легальності сумнівним цифровим активам через нотаріально посвідчений правочин.

Додатковою правовою невизначеності в українському контексті додає Закон України «Про віртуальні активи» від 17 лютого 2022 року № 2074-IX, який прийнятий, але офіційно не набрав чинності [5]. Водночас чинним залишається Закон України «Про запобігання та протидію легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» [6].

З огляду на актуальну ситуацію, доцільно розглядати криптоактиви не лише як об'єкти ринку, а як цифрові майнові об'єкти, які потребують особливого режиму доказування. Такий режим має включати: встановлення виду криптоактиву; перевірку способу набуття; доказування контролю над wallet/private key або

обліковим записом у постачальника послуг; перевірку законності походження джерела доходу; документування цифрового сліду транзакції. Для нотаріальної практики це означає потребу у стандартах обережності, які дозволяють відрізнити технічний доступ від права власності та фіксувати межі нотаріальної відповідальності.

Отже, криптоактиви в умовах гібридної війни мають розглядатися як складна форма цифрової власності, що поєднує приватно-правову, доказову, AML/CFT та кібербезпекову проблематику. Контроль над ключем не дорівнює автоматично праву власності; blockchain record не замінює правочин; нотаріальне посвідчення не повинно легалізувати сумнівне походження активу; AML/CFT-перевірка має враховувати технологічні особливості цифрової власності. Для українського правопорядку перспективною є інтегрована модель яка повинна надавати можливість нотаріусу виконати свої обов'язки суб'єкта первинного фінансового моніторингу та не допустити проведення незаконних правочинів.

ЛІТЕРАТУРА:

1. Regulation (EU) 2023/1114 of 31 May 2023 on markets in crypto-assets. OJ EU. 2023. L 150. P. 40-205. <https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng>
2. Regulation (EU) 2024/1624 of 31 May 2024 on the prevention of the use of the financial system for money laundering or terrorist financing. OJ EU. 2024.
3. CNUE. Crypto Assets: Characteristics, risks and best practices. Council of the Notariats of the European Union.
4. FATF. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris: FATF, 2021.
5. Про віртуальні активи: Закон України від 17.02.2022 № 2074-IX. <https://zakon.rada.gov.ua/laws/main/2074-20>
6. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення: Закон України від 06.12.2019 № 361-IX. <https://zakon.rada.gov.ua/laws/show/361-20#Text>

Рябченко Вікторія Олександрівна
аспірантка 3-го року навчання кафедри приватного права
Національного університету «Одеська юридична академія»

ВИКОРИСТАННЯ ОНЛАЙН ІГОР ТА МЕСЕНДЖЕРІВ ЯК ІНСТРУМЕНТУ ВЕРБУВАННЯ: ВИКЛИКИ ДЛЯ ІТ-ПРАВА

В умовах війни, коли соціальні та економічні структури дестабілізовані, кіберпростір остаточно став ще одним фронтом гібридної війни. Поряд із масовими кампаніями дезінформації та маніпуляціями зі сторони країни-агресора все частіше фіксуються випадки онлайн-вербування українських громадян за допомогою ігрових платформ, соціальних мереж та різних месенджерів з метою виконання розвідувальних, диверсійних чи пропагандистських завдань.

Вербувальники зазвичай діють за чітко відпрацьованою схемою. За останніми даними, представники російських спецслужб продовжують свою діяльність, вдаючись до дедалі більш цинічних і протиправних методів. Активно використовують месенджери та соціальні мережі, надсилаючи громадянам підроблені повістки, залякуючи неіснуючими справами [2]. У деяких випадках вони пропонують фіктивну допомогу у врегулюванні вигаданих проблем в обмін на виконання певних розвідувальних або підривних завдань стосовно військових об'єктів або об'єктів критичної інфраструктури. Російські спецслужби використовують сайти й сервіси онлайн-знайомств для вербування українців. Вони створюють фейкові жіночі акаунти, налагоджують спілкування з чоловіками та виманюють особисті дані. Після цього з жертвою зв'язується так званий «співробітник СБУ», який звинувачує її у контактах із представницею ворожих спецслужб. Під приводом уникнення відповідальності, шляхом шантажу, особі пропонують співпрацювати, змушуючи виконувати розвідувальні чи диверсійні завдання. Спецслужби країни-агресора використовують бот-мережі в соціальних мережах і месенджерах для вербування українців. Такі боти імітують живе спілкування, створюють довірливу атмосфе-

ру та поступово залучають користувача до спільних завдань чи закритих груп. Через них збирають персональні дані, відстежують емоційний стан людини та відбирають найбільш вразливих осіб для подальшої індивідуальної роботи з кураторами. Вербувальники також створюють оголошення про нібито високооплачувану роботу – часто з формулюваннями на кшталт «підробіток онлайн», «робота, можна без досвіду», «година часу і гроші твої». Такі повідомлення розміщуються у соціальних мережах, ігрових чатах, телеграм-каналах чи на платформах з пошуку роботи.

Організатори вербувальних схем постійно знаходять нові можливості для обходу державних обмежень, адаптуючи свої методи до розвитку цифрових технологій.

Одним із очевидних результатів цифровізації є створення криптовалюти. Біткоїн та інші криптовалюти змінили не тільки фінансову систему, а й способи та засоби протиправної діяльності. Цифрова інфраструктура створила сприятливе середовище для фінансування терористичних організацій [3, с. 72]. В реаліях сьогодення викликом стає використання внутрішньо-ігрових систем та цифрових активів, таких як віртуальні монети, токени, скіни чи предмети обміну, як інструменту для проведення нелегальних фінансових операцій, пов'язаних із вербуванням. Фіксується тенденція, коли організатори уникають традиційних фінансових каналів, переходячи до розрахунків усередині ігрових платформ або з використанням криптовалют. Такі транзакції значно ускладнюють відстеження руху коштів і створюють правові прогалини і у результаті віртуальні предмети стають «сірою зоною» фінансових взаєморозрахунків, де можливо здійснювати виплати за збір інформації, пропагандистську діяльність або виконання завдань розвідувального характеру.

Також проблемою залишається визначення меж відповідальності цифрових платформ за використання їхньої інфраструктури для сприяння злочинним діям. Хоча європейський законодавчий досвід, зокрема Digital Services Act (DSA), встановлює обов'язок провайдерів модерувати заборонений контент, цей механізм де-

монструє обмежену ефективність у зашифрованих месенджерах та ігрових чатах через пріоритетність таємниці приватного спілкування. У цьому контексті особливої ваги набуває Постанова Кабінету Міністрів України № 1533 від 26.11.2025 р. Вона пропонує змістити акцент із пасивного очікування скарг на активну координацію між державними органами та ІТ-сектором [1]. Відповідно до Постанови, дії, пов'язані з онлайн-вербуванням можуть бути кваліфіковані як соціально орієнтовані кіберінциденти, що дозволяє застосовувати технічні протоколи реагування, не порушуючи при цьому приватно-правову природу листування. Натомість, наприклад, діяти на рівні оперативного виявлення нетипової активності у поведінці автоматизованих систем (ботів), які використовуються для масових розсилок та пошуку потенційних жертв вербування.

Підсумовуючи, необхідно зазначити, що онлайн-вербування через ігрові платформи, сайти, месенджери демонструє прогалини правових інструментів для протидії гібридним загрозам у цифрову епоху. Використання нетрадиційних фінансових каналів, як ігрова валюта, токени чи криптовалюта, створює приховане середовище для розрахунків, що потребує адаптації норм ІТ-права. Крім того, важливим є законодавче визначення меж відповідальності цифрових платформ за безпеку їх систем та впровадження правових механізмів моніторингу обігу віртуальних грошових активів.

ЛІТЕРАТУРА:

1. Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози: Постанова Кабінету Міністрів України від 26.11.2025 р. № 1533. URL: <https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF#Text>
2. Російські спецслужби активізували вербування українців, видаючи себе за СБУ. *Армія FM*. URL: <https://www.armyfm.com.ua/rosiiskispetssluzhby-aktyvizuvaly-verbuvannia-ukraintsiv-vydaichy-sebe-za-sbu/>
3. Dyntu, V., & Dykyj, O. (2021). Cryptocurrency as an instrument of terrorist financing. *Baltic Journal of Economic Studies*, 7(5), 67-72. <https://doi.org/10.30525/2256-0742/2021-7-5-67-72>

Савенко Дмитро Олександрович
магістр, спеціальність «Системний аналіз»
Одеського державного університету внутрішніх справ

ВИКОРИСТАННЯ OSINT ІНСТРУМЕНТІВ ДЛЯ ВИЯВЛЕННЯ ФЕЙКОВИХ НОВИН ТА ДЕЗІНФОРМАЦІЇ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

OSINT (Open Source Intelligence) – це методологія збору, систематизації та аналізу інформації з відкритих джерел, таких як соціальні мережі, агрегатори новин, сервіси геолокації, відкриті державні реєстри та бази даних. На відміну від традиційних розвідувальних дисциплін, інструменти та засоби OSINT є юридично прозорими та забезпечують відтворюваність результатів, тому ця дисципліна також чудово підходить для перевірки інформації у публічному просторі та використання як доказів у судових процесах.

В умовах стрімкого розвитку інформаційних технологій OSINT залишається одним із найбільш перспективних та багатосторонніх інструментів у сфері кібербезпеки. Інформація отримана за допомогою розвідки у відкритих джерелах може одночасно використовуватись як інструмент протидії загрозам національній безпеці України, так і як інструмент для їх розповсюдження, як, наприклад, розповсюдження інформації про об'єкти критичної інфраструктури, військові об'єкти та інші чутливі підприємства [1, с. 169].

Окремим видом загрози, який становить гібридна війна, є розповсюдження дезінформації та фейків, що в свою чергу може сприяти зміні соціальних настроїв та спонуканню населення країни до певних діянь, які можуть становити загрозу для національної безпеки. Тобто, збір відкритої інформації, включно з аналізом соціальних мереж, супутникових знімків, повідомлень у ЗМІ та даних із різних онлайн-ресурсів, є важливим елементом боротьби проти дезінформації [2, с. 283].

Особливу увагу слід приділити взаємодії OSINT з технологіями штучного інтелекту (ШІ) у боротьбі з дезінформацією.

Сучасні рішення на основі ШІ, такі як автоматизовані системи перевірки фактів, виявлення контенту типу «діпфейк» на основі нейронних мереж та алгоритми кластеризації скоординованих інформаційних кампаній, значно посилюють аналітичний потенціал OSINT. Інтеграція розвідки з відкритих джерел та машинного навчання створює нову парадигму боротьби з гібридними інформаційними загрозами та вимагає відповідної правової кодифікації у національному законодавстві та міжнародних угодах, що стосуються кіберпростору.

Станом на сьогоднішній день існує досить велика кількість інструментів які доцільно використовувати під час перевірки новин та протидії дезінформації як працівникам державних структур, так і приватним підприємствам:

Ще за часів окупації Криму та Донбасу росія почала систематично використовувати дезінформацію як складову доктрини «інформаційно-психологічної війни», що вже було відображено в її військових доктринах. Ключовими механізмами є: фабрикація псевдодоказів (жертви обстрілів, які стали «жертвами українських злочинів»), спотворення нарративу (зображення збройної агресії як «захисту мирного населення»), а також інформаційне перевантаження – коли медіапростір навмисно розширюється настільки, щоб вмістити таку кількість суперечливих повідомлень про подію, що звичайний споживач інформації не зможе відрізнити правду від брехні. Дослідники називають цей ефект «туманом неправди».

У зв'язку із повномасштабним вторгненням російської федерації на територію України в лютому 2022 значущість та використання OSINT-інструментів різко збільшилося. Розвідка з відкритих джерел почала активно використовуватися з обох сторін конфлікту: розповсюдження дезінформації, пошук інформації про дислокацію та кількість особового складу збройних сил на певній території, моніторинг переміщення військової техніки та іншої розвідувальної інформації. Також із розвитком технологій різко збільшилось використання штучного інтелекту, особливо в контексті OSINT-інструментів.

**Порівняння технічних можливостей
OSINT інструментів**

№ п/п	Назва	Технічні можливості OSINT-інструменту
1.	Hive AI	Виявляє чи використовувався ІІІ під час створення аудіо-, відео- та фотоматеріалів.
2.	Decorum AI	Виявляє чи використовувався ІІІ під час створення фотоматеріалів та написання тексту.
3.	TinEye	Реверсивний пошук схожих фотознімків, додатково є можливість більш розширеного пошуку з можливістю виявлення «цифрового втручання» у фотоматеріали (чи редагувався фотознімок у Фотошопі та іншому аналогічному програмному забезпеченні).
4.	InVID-WeVerify	Мультизадачний інструмент для ідентифікації фейкових новин (аналіз відео-, аудіозаписів та фотознімків, перевірки першоджерела інформації, та багато іншого функціоналу).
5.	Deepware scanner	Виявляє чи використовувався ІІІ для створення відеофайлів. В наявності 4 різних моделі перевірки.
6.	AI voice detector	Виявляє чи не використовувався ІІІ для створення аудіоматеріалів.
7.	Let's Data	Дуже потужний інструмент який за допомогою ІІІ-аналітики в реальному часі виявляє дезінформаційні компанії в соціальних мережах, новинних та інших ресурсах.
8.	EU vs Disinfo database	Офіційна датабаза Європейського Союзу в якій зібрано фейкові новини з проросійськими наративами з різних джерел та ресурсів.
9.	Pangram	Перевіряє чи не використовувався ІІІ під час генерації тексту. Існує можливість перевірки 20+ мовами.

Таким чином, сучасний OSINT-інструментарій є ефективним засобом верифікації інформації та виявлення дезінформаційних кампаній в умовах гібридної війни в Україні. Подальший розвиток цієї галузі потребує комплексного підходу, що включає в себе як технологічне вдосконалення методів збору та аналізу даних, так і формування належної правової бази, яка б забезпечувала законність застосування відповідних інструментів та захист прав експертів, які займаються розвідкою у відкритих джерелах інформації.

ЛІТЕРАТУРА:

1. Івкова В., Опірський І. (2025). OSINT-технології як загроза кібербезпеці держави. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 3(27). С. 165-179.
2. Величко Т. (2024). Протидія російській інформаційній агресії за допомогою OSINT. *Матеріали Всеукраїнської науково-практичної конференції представників сектору безпеки і оборони України, наукових та науково-педагогічних працівників, здобувачів освіти та інших зацікавлених осіб* (м. Київ). № 1. С. 283–284.

Самойленко Георгій Валерійович
доктор юридичних наук, професор,
професор кафедри цивільного права
Запорізький національний університет

ВІДШКОДУВАННЯ ШКОДИ, ЗАВДАНОЇ ТЕРИТОРІАЛЬНІЙ ГРОМАДІ ЗБРОЙНОЮ АГРЕСІЄЮ РФ

В контексті вирішення завдання визначення особливостей відшкодування шкоди, завданої збройною агресією РФ територіальним громадам визначимо наступні аспекти. По-перше, суб'єктом, який потребує захисту порушених майнових прав у вигляді відшкодування шкоди, завданої збройною агресією РФ (позивачем) є територіальна громада, від імені якої діє орган місцевого самоврядування (місцева рада); по-друге, судова практика визнає відповідачем у різних справах РФ як державу [1], міністерство оборони, міністерство юстиції, генеральну прокуратуру РФ. Оскільки

ки шкода, де факто, спричиняється військовослужбовцями ЗС РФ, застосована за аналогією норма ЦК про відшкодування підприємством шкоди, завданої працівником, або ж щодо відповідальності держави-агресора за шкоду, завдану її збройними силами цивільному населенню (фізичним особам) (норма, закріплена в ст. 91 Додаткового протоколу I до Женевських конвенцій 1949 р.) потребує свого відповідного нормативного закріплення в ЦК України щодо відповідальності країни-агресора за шкоду, завдану діями осіб, що входять до її збройних сил по відношенню будь-яких суб'єктів цивільно-правових відносин, включно, територіальних громад. По-третє, судовий імунітет РФ як держави, що має суверенні права, не підлягає застосуванню з огляду на порушення РФ державного суверенітету України, що виходить за межі здійснення рф своїх суверенних прав, що охороняються судовим імунітетом. Відтак, РФ не має права надалі посилатися на свій судовий імунітет, заперечуючи юрисдикцію судів України у справах про відшкодування шкоди, завданої РФ (Постанова КЦС ВС від 18.05.2022 р. у справі № 760/17232/20-ц (частина II) [2]. По-четверте, застосоване матеріальне законодавство має визначатися місцем завдання шкоди (колізійна прив'язка *lex loci delicti commissi*), – *деліктне законодавство України (зокрема, норми ЦК України про деліктні зобов'язання)*. По-п'яте, *процесуальний закон – відповідно до колізійної прив'язки lex fori* (закон місця розгляду справи). Відтак, розгляд даної категорії справ є господарською юрисдикцією відповідно до ч. 2 ст. 4 Господарського процесуального кодексу України, згідно якої державні органи, органи місцевого самоврядування мають право на звернення до господарського суду за захистом своїх порушених, невизнаних або оспорюваних прав та законних інтересів у справах, віднесених законом до юрисдикції господарського суду, а ч. 3 відповідної статті визначено право осіб звертатися також особи, яким законом надано право звертатися до суду в інтересах інших осіб [3]. Звичайно, враховуючи, що органи місцевого самоврядування мають делеговані повноваження, то конструкція даної норми мала б передбачати право органу місцевого самоврядуван-

ня звертатися до суду не щодо захисту власних прав та інтересів, а все ж таки, порушених прав та інтересів територіальної громади. В цьому контексті комунальні підприємства повинні мати власну правосуб'єктність для звернення за захистом *своїх* порушених прав, оскільки наразі законодавчо закріплена конструкція юридичної особи публічного права не визначає публічний інтерес критерієм визначення правосуб'єктності такого виду юридичних осіб. Ознака «майнової самостійності» властива будь-яким видам юридичних осіб. По-шосте, факт збройної агресії РФ проти України не потребує доведення як юридичного факту, оскільки він є загальновідомим (неодноразово військова агресія РФ визнавалася та засуджувалася на міжнародному рівні, зокрема, Резолюцією Генеральної Асамблеї ООН ES-11/1 від 02.03.2022 р., Міжнародним судом ООН, який у наказі про забезпечувальні заходи від 16.03.2022 р. у справі щодо звинувачень у геноциді за конвенцією про попередження та покарання злочину геноциду зобов'язав РФ припинити військову агресію проти України, Резолюцією Генеральної Асамблеї ООН ES-12/1 від 24.03.2022 р., якою додатково засудила військову агресію РФ проти України та вимагала від РФ припинення військових дій, в тому числі атак проти цивільних осіб та цивільних об'єктів, припинення порушення та дотримання міжнародного гуманітарного права, згідно Женевських Конвенцій 1949 р. та додаткового протоколу I 1977 р. до них) [3]. У Постанові Великої Палати Верховного Суду в справі №210/4458/15-ц від 19.02.2020 року та ухвалі Вищого спеціалізованого суду України з розгляду цивільних та кримінальних справ у справі №761/9437/15-ц від 16.08.2017 р. прямо зазначено, що факт збройної агресії російської федерації проти України встановленню в судовому порядку не потребує. По-сьоме, потребує нормативного закріплення конструкція презумпції вини країни-агресора за шкоду, завдану будь-яким суб'єктам цивільно-правових відносин, включно державі Україна, територіальним громадам та ін., у зв'язку з бойовими діями на території України, оскільки окремі види шкоди вимушено завдаються ЗСУ в процесі надання відсічі збройній агресії РФ. Така

шкода має відшкодовуватися в контексті причинно-наслідкового зв'язку «збройна агресія – завдана шкода» та об'єктивної відповідальності РФ на основі суб'єктивного елементу *corpus delicti* «незалежно від вини». По-восьме, судова практика в питанні визначення розміру завданих збитків виходить з нормативних приписів відшкодування реальних збитків та не отриманих доходів. Так, у справах № 905/57/25[4], № 905/64/25 [5] та ін. суди, задовольняючи позови, керувалися Постановою Кабінету Міністрів України від 20.03.2022р. № 326, якою затверджено Порядок визначення шкоди та збитків, завданих Україні внаслідок збройної агресії російської федерації (далі Порядок), який встановлює процедуру визначення шкоди та збитків, завданих Україні внаслідок збройної агресії російської федерації, починаючи з 19.02.2014 р. Так, у справі № 905/57/25 за позовом Маріупольської міської ради Донецької області за участю третьої особи, яка не заявляє самостійних вимог на стороні позивача Комунальний заклад Маріупольський міський технологічний ліцей до РФ про відшкодування збитків в розмірі 34 949 768,10 грн., завданих нежитловій будівлі (Комунальний заклад «Маріупольській міський технологічний ліцей Маріупольської міської ради Донецької області»), яка є власністю територіальної громади м. Маріуполь шляхом її руйнування, як і у справі № 905/64/25 за позовом Маріупольської міської ради Донецької області до держави Російська Федерація у зв'язку зі знищенням/втратою належного позивачу майна (нежитлової будівлі Комунального закладу «Маріупольська загальноосвітня школа І-ІІІ ступенів №56» Маріупольської міської ради Донецької області з тамбурами і прибудовою загальною площею 4061,3 кв.м за адресою: Донецька область, м. Маріуполь, бульвар Морський, 8, та знищенням/втратою майна, що знаходилось у приміщеннях вказаних будівель), в якій було доведено, що внаслідок збройної агресії РФ проти України та окупації РФ міста Маріуполь, позивач фактично втратив можливість володіти, користуватись та розпоряджатись своїм майном, суди виходили з балансової вартості такого майна. Такий підхід законодавця вважаємо хибним і таким, що по-

требує негайного виправлення. В реальному житті будівництво нових об'єктів нерухомості в разі більше балансової (остаточної) вартості об'єктів, які амортизувалися протягом строку їх служби чи експлуатації. Новий підхід почав вже використовуватися в окремих випадках. Так, ст. 27 Закону України «Про обов'язкове страхування цивільно-правової відповідальності власників наземних транспортних засобів» в питанні страхової (регламентної) виплати у разі пошкодження транспортного засобу виходить з принципу «старе за нове» у страхуванні («new for old») [6]. Так, закон чітко визначає розмір відшкодування в розмірі витрат, пов'язаних із відновлювальним ремонтом пошкодженого транспортного засобу.

Відтак, розмір відшкодування шкоди, завданої збройною агресією РФ проти України має виходити не з оцінки реальних збитків, які обраховуються на основі балансової вартості об'єктів речових прав, а з оцінки вартості матеріалів та відновлювальних робіт у випадку ремонту пошкоджених об'єктів, а у випадку їх знищення, – необхідності придбання чи будівництва нових об'єктів речових прав (в залежності від їх виду – рухомого чи нерухомого майна).

ЛІТЕРАТУРА:

1. Рішення Господарського суду Київської області за позовом ТОВ «Технічний центр «СНАМІ» до держави російської федерації від 08.02.2023 р. у Справі № 911/1832/22. URL: <https://reyestr.court.gov.ua/Review/109362636>
2. Судова практика Верховного Суду щодо судового імунітету рф. URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/2024_prezent/Prezent_Sud_imun_rf_15_03_2024.pdf
3. Господарський процесуальний кодекс України від 06.11.1991 р. *Відомості Верховної Ради України (ВВР)*. 1992. № 6. Ст. 56.
4. Рішення Господарського суду Донецької області від 03.06.2025 р. у Справі № 905/57/25. URL: <https://reyestr.court.gov.ua/Review/128065485>
5. Рішення Господарського суду Донецької області від 19.05.2025 р. у справі № 905/64/25/ URL: <https://reyestr.court.gov.ua/Review/127533571>
6. Про обов'язкове страхування цивільно-правової відповідальності власників наземних транспортних засобів : Закон України від 21.05.2024 р. *Відомості Верховної Ради (ВВР)*. 2024. №№ 37, 38. Ст. 238.

Станкевич Андрій Володимирович
аспірант кафедри приватного права
Національного університету «Одеська юридична академія»

ПРОБЛЕМИ ВИЗНАЧЕННЯ ІІІ СУБ'ЄКТОМ ЕЛЕКТРОННОГО ОБІГУ ОБ'ЄКТІВ ЦИВІЛЬНОГО ПРАВА ЗА НАЦІОНАЛЬНИМ ЗАКОНОДАВСТВОМ ТА ЗАКОНОДАВСТВОМ ЄС

Оскільки ІІІ діє виключно в електронному середовищі, постає питання можливості його віднесення до суб'єктів електронного обігу об'єктів цивільного права, зокрема інтелектуальної власності, що є проблематичним. З цього приводу точиться дискусія серед науковців.

Перш за все звернемося до думки Суслікова Л.М. та Студенюк І.П., які звертають увагу на те, що ІІІ -це насамперед сукупність алгоритмів, що імітують нейронні функції людини. Стосовно віднесення ІІІ до суб'єктів електронного обігу об'єктів авторського права, ці автори зазначають, що ІІІ не володіє власною креативністю, адже творчість пов'язана зі здатністю самостійно оперувати новим знанням. Інтелект же проявляється через обробку, відбір і створення інформації [1, с.30].

Питання правосуб'єктності ІІІ є досить проблематичним. Парамонова О.Ю та Варава І.П. зазначають, що правовий статус ІІІ не може ґрунтуватися ані на моделі фізичної особи, бо це означало б надання йому прав людини, що суперечить Хартія основних прав Європейського Союзу та Конвенція про захист прав людини і основоположних свобод, ані на моделі юридичної особи, яка передбачає управління людьми [2, с.75]. З цією думкою цілком можна погодитися.

Дещо суперечливою є думка Докійчук К., який вважає, що «для вирішення питання правосуб'єктності ІІІ слід визнати, що він не є об'єктом права (винаходом чи програмою), а має розглядатися як особа з право-, діє- та деліктоздатністю. У такому разі розробники не матимуть на нього майнових прав і не зможуть відчувувати чи експлуатувати його як річ» [3]. З іншою думкою

цього автора, що «Штучний інтелект повинен діяти в інтересах суспільства, з визначеними правами та обов'язками. Невизнання його правосуб'єктності може гальмувати розвиток цієї сфери» [3], можна цілком погодитися.

З нормативно-правової точки зору, в Україні термін «ШІ» досі не визначений. Національне законодавство оперує поняттям «комп'ютерна програма». Так згідно зі ст. 33 Закону України «Про авторське право і суміжні права» № 2811 IX від 01.12.2022, об'єкт, згенерований комп'ютерною програмою, не є твором у класичному розумінні авторського права. Такий об'єкт отримус *sui generis* охорону строком 25 років, але не має майнових чи немайнових прав як у автора [4] оскільки комп'ютерна програма є об'єктом права, а не його суб'єктом. Відповідно, права належать лише власнику або правовласнику програми.

На відміну від України у ЄС прийняті численні нормативно-правові акти, пов'язані з електронним обігом об'єктів цивільного права, участь у якому приймає ШІ. Це, зокрема, Регламент (ЄС) 2024/1689 (AI Act), який встановлює вимоги до розроблення та використання систем ШІ; Директива 85/374/ЄЕС (у редакції 2024 р.), що визначає відповідальність за дефектну продукцію, включно з програмним забезпеченням і системами ШІ; Директива 2000/31/ЄС (E-Commerce Directive), що регулює електронну комерцію, відповідальність посередників та укладення електронних договорів та інші.

Аналіз Регламенту (ЄС) 2024/1689, показує, що вони не надають ШІ правосуб'єктності. У ст. 3 Регламенту (ЄС) 2024/1689 «система штучного інтелекту» визначається як автономна машинна система, здатна генерувати прогнози, контент, рекомендації або рішення [5], але без ознак суб'єкта права. Директива (ЄС) 2020/1828 може застосовуватися лише у випадках порушень прав споживачів, спричинених використанням систем ШІ. Таким чином, у ЄС ШІ розглядається виключно як технологічний інструмент, а регулювання базується на антропоцентричній моделі, де пріоритетом є безпека та захист фундаментальних прав людини.

Також аналіз Директиви (ЄС) 2020/1828, яка направлена на захист колективних інтересів споживачів, у контексті штучного інтелекту свідчить, що ця Директива не регулює ШІ безпосередньо і не надає йому жодного правового статусу, однак може застосовуватися до порушень прав споживачів, спричинених використанням систем ШІ.

Можна зазначити, що нормативно-правові акти ЄС виходять із антропоцентричної моделі регулювання: штучний інтелект не визнається носієм прав чи обов'язків, а кваліфікується як технологічний інструмент, використання якого повинно відповідати вимогам безпеки та поваги до фундаментальних прав людини. Нормативно-правові акти України та ЄС не містять жодних норм, які б прямо чи опосередковано закладали підстави для формування правосуб'єктності штучного інтелекту.

Отже, національне та європейське законодавство не визнають ШІ суб'єктом цивільного права, і питання його правосуб'єктності залишається відкритим для подальшого правового врегулювання. Водночас активний розвиток технологій ШІ та їхнє широке впровадження у електронний обіг об'єктів цивільного права у комерційних, освітніх та суспільних сферах потребує пошуку нових підходів до правового регулювання. Можливе формування спеціальних моделей правосуб'єктності для ШІ або визначення чітких правил відповідальності розробників і користувачів. У перспективі це може сприяти більш ефективному використанню ШІ та захисту прав третіх осіб. Важливо, щоб подальше законодавче врегулювання враховувало баланс між інноваціями та фундаментальними правами людини.

ЛІТЕРАТУРА :

- 1.Сусліков Л. М., Студеняк І. П. Створення об'єктів інтелектуальної власності: Навчальний посібник. Ужгород: Говерла, 2020. 407 с.
- 2.Парамонова О. Ю., Варава І. П. Місце штучного інтелекту в системі права. *Юридичний вісник*. 2023. № 3(68). С. 73–80. URL:https://www.researchgate.net/publication/375984267_MISCE_STUCNOGO_INTELEKTU_V_SISTEMI_PRAVA

3.Докійчук К. Питання правосуб'єктності штучного інтелекту. *Судово-юридична газета*. 15 січ. 2018 р. URL: <https://sud.ua/ru/news/blog/113593-pitannya-pravosubyektnosti-shtuchnogo-intelektu>

4. Про авторське право та суміжні права: Закон України від 15.11.2024 р. № 2811-IX. URL: <https://zakon.rada.gov.ua/laws/show/2811-20#Text>

5.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). European Parliament, Council of the European Union. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689>

Стрілець Михайло Ігорович

аспірант кафедри приватного права

Національного університету «Одеська юридична академія»

ДОВІРА ЯК ОСНОВА ФУНКЦІОНУВАННЯ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Стрімкий розвиток цифрових технологій здійснив перехід торгівлі в цифрову сферу. Враховуючи принципи функціонування економіки, можна сміливо стверджувати, що основою розвитку електронної комерції є довіра контрагентів.

Сьогодні здійснити купівлі в Інтернеті доволі складно без розкриття своєї особистої інформації, на відміну від «традиційної торгівлі». Покупець, уклавши угоду через «традиційний» магазин, позбавляється необхідності торбуватися про рівень своєї конфіденційності. Це ж стосується й продавця, який також повинен здійснювати контроль, він зобов'язаний забезпечити довірливе середовище для здійснення торгівлі на своїй платформі. Тобто продавець, разом з покупцем знаходяться в «замкнутій системі», адже повинні довіряти один одному. Звісно, в таких правовідносинах обов'язково повинні бути встановленні відповідні гарантії оплати, якості, можливості розірвання договору тощо. В «традиційній» торгівлі вносити зазначені питання через відповідне законодавство не так складно, на відміну від електронної торгівлі, де все зводиться до питання «довіри».

Чи впливає загалом конфіденційність на рівень купівлі в Інтернеті? Беручи до відома дослідження, проведене в 2016 року [1], з якого стало відомо, що споживачі, які в більшій мірі обмірковують свою конфіденційність, схильні менше купувати в Інтернеті.

Постає питання: чи може попередня інформація щодо здійснення онлайн правочину впливати на наміри укласти онлайн угоду?

В дослідженні, проведеному в 2020 року [2], вивчалися взаємозв'язки між початковим рівнем довіри до онлайн платформи та пов'язаним наміром здійснити купівлі на такій платформі. Повідомлення про конфіденційність на такій онлайн платформі розглядалося через можливість здійснити вплив на наміри здійснити купівлю, а також на довіру до такої онлайн платформи. Також в цьому дослідженні розглядався вплив національного фактору щодо наміру здійснити купівлю на такій платформі. Обґрунтовувалося це тим, що різні національності мають різний рівень уникнення невизначеності. В зазначеній праці наводилося, що до країн з найвищими показниками рівня уникнення невизначеності, належить Румунія, в той же час Нідерланди мають найнижчий показник уникнення невизначеності. Зазначена праця досліджувала наміри здійснити купівлі на такій платформі.

Згідно з результатами цього дослідження, не було виявлено прямого впливу повідомлення про політику конфіденційності на намір здійснити покупку. Ні відсутність, ні наявність повідомлення про політику конфіденційності не призвели до зниження або підвищення рівня довіри до конкретної веб-платформи. Проте дослідниками було виявлено непрямої вплив повідомлення про політику конфіденційності на намір зробити покупку, все це через початкову довіру. Якщо попередньо вища початкова довіра, то це призведе до вищого наміру здійснити покупку. Вплив національного фактору загалом не підтвердився.

Доволі цікаве дослідження опубліковане в 2025 році [3], проведене на основі даних взятих зі Scopus за період 2020-2025 рр. Результати досліджень встановили чітку відмінність між віковими

та гендерними категоріями, а також споживачами з різним рівнем доходу. Молодші споживачі значно частіше купували онлайн з впевненістю, на відміну від старшої вікової групи, що проявляла значно більшу чутливість в питаннях довіри та онлайн безпеки. Щодо врахування гендерного фактору, то згідно з результатами досліджень, жінки, як правило, здійснювали порівняння товарів, а також тратили більше часу на перегляд відгуків, на відміну від чоловіків. Звісно ж були наявні значні відмінності у соціальних групах з різним рівнем доходу, адже вартісні товари зазвичай стосувалися покупців з вищим соціально-економічним статусом.

З дослідження, проведеного в 2021р. [4], можна зробити висновки, що довіра та оцінка продукту відіграють важливу роль стосовно формування намірів здійснити повторну покупку. Це, звісно ж, відіграє вирішальну роль у мінливому економіко-цифровому середовищі при необхідності збереження лояльності клієнтів.

Враховуючи такі результати досліджень, постає питання: чи загалом можливо реалізувати вплив на початкову довіру веб – платформи з врахуванням перелічених факторів (вік, стать, дохід та ін.).

На сьогоднішній день впровадження довіри в електронній комерції реалізується за такими основними напрямками:

1) впровадження кардинальних змін в сфері інформаційних технологій: впровадження новітніх стандартів захисту даних, посилення кібербезпеки.

2) законодавчі зміни: імплементація та адаптація законодавства ЄС в національне законодавство, створення прозорої системи оподаткування, вдосконалення захисту прав споживачів.

3) проведення заходів з попередження та виявленню загроз: проведення аудитів інформаційної безпеки, проведення пентестів, сканування вразливостей як на державному, так і на приватному рівнях.

4) впровадження освітніх заходів як для бізнесу, так і для споживачів з метою забезпечення безпечного користування електронними технологіями.

Важливу роль в вирішенні проблемних питань електронної комерції відіграють міжнародні акти, а саме типові закони «Про електронну торгівлю» прийнятий Комісією ООН по міжнародному праві від 12 грудня 1996 року та «Про електронні підписи» № 995_937 від 25.05.2007 року, також доповідь «Електронна торгівля й роль СОТ» опублікована у березні 1988р., яка найперше намагалася врегулювати питання міжнародної електронної торгівлі та багато інших актів. Міжнародні акти зазвичай однотипні, носять рекомендаційний характер. Вони передбачені для розробки та впровадження на їх осові національного законодавства[5].

Вирішення проблем довіри електронної комерції потребує кардинальних, звісно ж, змін особливо стосовно впровадження законодавчих змін. В Україні опубліковано Закон України «Про захист прав споживачів» [6], що почне діяти не раніше дня припинення чи скасування воєнного стану, який впроваджує портал е-Покупець. Цей портал зобов'яже інтернет-магазини зареєструватися протягом 10 днів після початку роботи. Такий підхід до врегулювання питань довіри в електронній комерції доволі прогресивний, проте й передбачає певні ризики. Хоч покупець зможе перевірити інформацію стосовно доброчесності продавця, проте чи не виникне, наприклад, зловживання зі сторони компетентного органу надавати переваги певним маркетплейсам. Загалом чи не зможе такий закон просувати недобросовісну конкуренцію, коли скарги будуть подаватися виключно для боротьби з конкурентами? Постає питання наскільки такий підхід взагалі відповідає принципу свободи підприємницької діяльності, якщо суб'єкти електронної комерції, що не зареєстровані на Порталі е-покупець, будуть обмежені у доступі? Цікавим є те, що встановлювати порядок зазначених обмежень, а також порядок оцінки нечесних комерційних практик зможе Кабінет Міністрів України, що явно не відповідає повноваженням підзаконного органу.

Іншим, доволі цікавим фактором змін, як зазначив Якоб Є. [7] може слугувати те, що великі платформи запроваджують стандарти якості електронної торгівлі, адже встановлюють вимоги до

всіх користувачів своїх платформ, що має доволі позитивний вплив на безпеку. Менші компанії, які зазвичай вважаються конкурентами великих, можуть наоборот отримати позитивний вплив, адже великі платформи допомагають їм закріпитися на ринку електронної торгівлі.

ЛІТЕРАТУРА:

1. Fortes N., Rita P. Privacy concerns and online purchasing behaviour: Towards an integrated model. *European Research on Management and Business Economics*. 2016. Vol. 22, no. 3. P. 167–176.
2. Broeder P. Culture, Privacy, and Trust in E-commerce. *Marketing from Information to Decision Journal*. 2020. Vol. 3, no. 1. P. 14–26.
3. Carmel K. W., Benediktus R., Aurellia J. W. A DEMOGRAPHIC ANALYSIS OF CONSUMER BEHAVIORAL PATTERNS ON DIGITAL E-COMMERCE PLATFORMS. *Jumder: Jurnal Bisnis Digital*. 2025. Vol. 1, no. 2. P. 1–15. URL: <https://journal.dinamikapublika.id/index.php/JUMDER/article/view/22/19>
4. Widodo T., Utami N. K. W. Repurchase Intentions on Zalora Indonesia: The Role of Trust, E-Commerce, and Product Evaluation. *Jurnal Manajemen Bisnis*. 2021. Vol. 8, no. 2. P. 339–351.
5. Кругул Ю., Батрименко В., Батрименко В. Правове регулювання міжнародної електронної комерції. Зовнішня торгівля: економіка, фінанси, право. 2018. № 2. с.138-140.
6. 6)»Про захист прав споживачів»: Закон України від 10.06.2023 № 3153-IX. URL: <https://zakon.rada.gov.ua/laws/show/3153-20#Text>
7. Якоб Є. Проблеми розвитку міжнародної електронної торгівлі. *Економіка та суспільство*. 2023. № 54. URL: <https://doi.org/10.32782/2524-0072/2023-54-32>

Тітова Аліна Олексіївна

*аспірантка кафедри приватного права
Національного університету «Одеська юридична академія»*

КЛАСИФІКАЦІЯ СПОСОБІВ МАНІПУЛЯЦІЇ ІНФОРМАЦІЄЮ

Сьогодні, у сфері цивільного права, проблема маніпуляції інформацією виходить на передній план у зв'язку з тим, що інформація стала повноцінним об'єктом цивільних прав, а інформаційні дії – юридично значущими актами поведінки, здатними прямо впливати на майнову та немайнову сферу особи. Маніпулятивні ін-

формаційні практики дедалі частіше стають причиною порушення прав споживачів, учасників договірних відносин, інвесторів, користувачів цифрових сервісів, а також можуть завдавати шкоди честі, гідності, діловій репутації та зачіпати інші прав. Цифрове середовище ускладнює виявлення маніпуляцій і розмиває межу між допустимим впливом та неправомірним формуванням хибного уявлення, що призводить до укладення не вигідних договорів, поширення недостовірної інформації, використання вразливості споживача та інших порушень [1, с.66]. Відсутність чіткої доктринальної класифікації способів маніпуляції інформацією у цивільно-правовому аспекті ускладнює вироблення критеріїв оцінки правопорушень, визначення розміру шкоди, кваліфікацію поведінки сторін та формування ефективних засобів захисту цивільних прав. Тому саме сьогодні, на нашу думку, наукове осмислення та систематизація способів інформаційної маніпуляції є необхідними для адаптації цивільного права до викликів цифрової епохи.

Маніпуляція інформацією у сучасній доктрині має розумітися як умисний прихований вплив на зміст, форму, контекст або спосіб подання інформації, спрямований на формування у адресата викривленої картини дійсності чи спонукання його до прийняття рішень, які суперечать його власним інтересам, за умов збереження ілюзії об'єктивності та нейтральності комунікації [2]. Саме таке визначення відображає сутнісну природу феномену, оскільки маніпуляція не зводиться до механічної зміни чи технічної модифікації інформації, які можуть бути зумовлені редакційними, технологічними чи організаційними потребами та не мають на меті впливу на волевиявлення особи. Так само вона не отожднюється зі створенням або поширенням інформації, оскільки ці процеси є нейтральними за своєю природою і не передбачають оцінки внутрішнього мотиву особи, що діє у сфері комунікації. Маніпуляція ж передбачає набагато глибший рівень впливу, у межах якого інформація виступає не об'єктом дії, а інструментом впливу на свідомість адресата, засобом формування потрібних реакцій та поведінкових моделей [3, с.11]. Її визначальною ознакою є прихованість,

що унеможлиблює безпосередню ідентифікацію маніпулятивного наміру та створює нерівність інформаційних позицій між комунікантом і реципієнтом. Саме ця прихованість і стратегічний характер впливу роблять маніпуляцію небезпечною у сфері цивільного права, оскільки вона порушує інформаційну автономію особи, спотворює умови формування її волі, нівелює добровільність і усвідомленість правочинів, створює передумови для обману, недобросовісних практик та вчинення дій, які адресат не здійснив би за умов повної та коректної інформації. Маніпуляція, яку науковці розглядають як один з видів інформаційної атаки, полягає в плавній і майже непомітній підміні предмету, який вивчається, і переходу (з відволікаючими ефектами) від об'єктивної оцінки відомостей, фактів тощо до аргументування ілюзорної реальності [4, с.60]. Таким чином, на відміну від зміни, модифікації, створення чи поширення інформації, які описують технічні аспекти роботи з інформаційним матеріалом, поняття «маніпуляція інформацією» фіксує специфічну форму впливу на особу через інформаційний зміст, що має прихований, вольовий та інструментальний характер і тому потребує окремого доктринального осмислення.

Класифікація способів маніпуляції інформацією у сучасній доктрині має ґрунтуватися на розумінні того, що маніпуляція є багатовимірним феноменом, який охоплює як змістові, так і контекстуальні, психологічні та технологічні механізми впливу на адресата. Вона не може бути зведена до простого переліку технік, адже кожна з них є проявом певної моделі впливу, спрямованої на формування викривленого сприйняття дійсності або некритичного прийняття нав'язаного рішення. Виходячи з цього, доцільно виділити кілька підходів до класифікації, які, на нашу думку, у сукупності можуть утворюють цілісну систему.

Передусім маніпулятивні способи поділяються залежно від характеру впливу на інформацію, що дозволяє розмежувати техніки, спрямовані на зміну її змісту, та прийоми, пов'язані зі зміною її форми та подання. До першої групи належать такі механізми, як селективне відбирання фактів, навмисне опущення суттєвих

елементів, часткове перекручення даних, використання псевдостатистики або штучне створення контексту, який надає фактам іншого смислу. До другої – ті, що працюють через структурування, фреймінг, різні типи емоційного забарвлення, маніпулювання заголовками чи візуальними образами, які супроводжують інформаційний матеріал.

Інша група класифікації пов'язаний із характером впливу на психіку адресата, оскільки маніпуляція завжди експлуатує певні когнітивні вразливості. Тут виокремлюються способи, що впливають через страх, тривогу або загрозу; через надмірну позитивізацію; через апеляцію до авторитетів; через стереотипи та соціальні упередження; через штучне створення дефіциту часу або інформаційного перевантаження. Психологічна природа цих технік робить їх особливо небезпечними, оскільки вони обходять раціональний аналіз і впливають на підсвідомі механізми прийняття рішень.

Наступна група класифікації ґрунтуються на технологічному способі реалізації маніпуляції. Тут виокремлюються алгоритмічні маніпуляції (персоналізований таргетинг, формування інформаційних бульбашок, маніпулювання алгоритмами рекомендацій), мережеві маніпуляції (бот-мережі, скоординовані інформаційні атаки, штучне масштабування певних меседжів), а також маніпуляції за допомогою синтетичних медіа (дипфейки, маніпульовані зображення та аудіо, контент, створений штучним інтелектом).

У межах цивільно-правового аналізу особливе значення має класифікація способів маніпуляції залежно від юридично значущого ефекту, який вони здатні спричинити. Тут доречно виділити маніпуляції, що ведуть до формування хибної волі особи при укладенні правочинів; маніпуляції, що порушують інформаційну автономію споживача; маніпуляції, спрямовані на дискредитацію ділової репутації; маніпуляції, які створюють інформаційні асиметрії між сторонами договірних відносин; маніпуляції, що призводять до немайнової шкоди шляхом впливу на честь, гідність, репутацію особи.

Таким чином, класифікація способів маніпуляції інформацією повинна бути багатошаровою і відображати її багатофакторну природу: вона має враховувати не лише змістові та формальні параметри інформаційного впливу, а й психологічні, технологічні та правові аспекти. Саме такий підхід дає змогу комплексно осмислити феномен маніпуляції та забезпечити належне правове реагування у цивільному праві, де захист інформаційної автономії особи стає одним з основних викликів цифрової доби.

ЛІТЕРАТУРА:

1. Самагальська Ю.Я., Шпуганич І.І. Право на інформацію в цифровому середовищі. *Науковий вісник Ужгородського Національного Університету*, 2024. С. 65-70. <https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/01/12-3.pdf>
2. Маніпуляція: визначення, підходи до вивчення. <https://socio.karazin.ua/resources/941ddffc75adf9fd96411cc79168a381.pdf>
3. Сугестивні технології маніпулятивного впливу : навч. посіб. За заг. ред. Є.Д.Скулиша. 2-ге вид. К.: ЗАТ “ВІПОЛ”, 2011. 248 с. https://duikt.edu.ua/uploads/1_1353_77641912.pdf
4. Брижко В.М., Дзьобань О.П. Дезінформація як фактор маніпулювання свідомістю. *Інформація і право*. 2023. № 2(45). С. 50-63.

Товт Тинде Олександрівна

*аспірантка кафедри цивільного права та процесу
ДВНЗ «Ужгородський національний університет»*

ПРАВО НА ВІДПУСТКИ ДЛЯ НЕПОВНОЛІТНІХ ПРАЦІВНИКІВ ЗА ЗАКОНОДАВСТВОМ УКРАЇНИ ТА УГОРЩИНИ: ПОРІВНЯЛЬНИЙ АСПЕКТ

Актуальність дослідження правового регулювання відпусток неповнолітніх в Україні та Угорщині зумовлюється потребою забезпечення належного рівня соціального захисту працюючої молоді в умовах змін сучасного ринку праці. Неповнолітні працівники належать до категорії, яка потребує підвищених гарантій щодо збереження здоров'я, можливості поєднання трудової діяльності з навчанням і забезпечення повноцінного відпочинку. У цьому зв'язку інститут відпусток набуває значення

не лише як складова трудових прав, а й як важливий механізм підтримки фізичного та психічного розвитку молоді. Порівняння підходів України та Угорщини дає змогу оцінити ефективність національного регулювання та визначити напрями його вдосконалення з урахуванням європейських стандартів у сфері праці неповнолітніх працівників.

У межах традиційного підходу до тлумачення поняття «час відпочинку» науковці звертають увагу на те, що не всі його види фактично відображають відпочинок як процес відновлення працездатності. Окрім цього, існують ситуації, які не охоплюються ані робочим часом, ані часом відпочинку, коли працівник тимчасово звільняється від виконання трудових обов'язків, але водночас не використовує цей період для відпочинку у звичному розумінні. Йдеться, зокрема, про виконання процесуальних функцій як свідка, експерта чи перекладача, а також участь у діяльності примирних органів.

З огляду на це обґрунтовується доцільність удосконалення підходу до структурування часу працівника шляхом запровадження дворівневої моделі: на першому рівні він поділяється на робочий і позаробочий, а на другому – позаробочий час розмежовується на час відпочинку та інші випадки звільнення від виконання трудових обов'язків. При цьому час відпочинку пропонується визначати як передбачене законодавством або договірними актами тимчасове звільнення від роботи, спрямоване на відновлення працездатності. Відпустка ж розглядається як окрема форма такого звільнення, що має визначену тривалість у календарних днях і надається відповідно до встановленого правового регулювання [1, с. 6-7]. Запропонований підхід видається достатньо аргументованим і логічно вмотивованим.

Директива Європейського Союзу 2003/88/ЄС, що регулює організацію робочого часу, визначає базові стандарти для держав-членів. Зокрема, документ встановлює максимальну тривалість робочого тижня, яка не може перевищувати 48 годин, а також гарантує щорічну оплачувану відпустку тривалістю щонайменше

20 днів [2]. Ці мінімальні вимоги відображені й у законодавстві України, тоді як у низці держав ЄС вони фактично перевищені.

В Україні відповідно до статті 75 КЗпП України та частини восьмої статті 6 Закону України «Про відпустки», тривалість щорічної основної відпустки для неповнолітніх становить 31 календарний день. Згідно зі статтею 195 КЗпП України та статтею 10 зазначеного Закону, така відпустка надається у зручний для неповнолітнього час і може бути використана у повному обсязі вже у перший рік роботи, незалежно від тривалості безперервного стажу, за умови подання відповідної заяви.

Надання відпусток неповнолітнім в Угорщині регулюється на рівні національного трудового законодавства, передусім Трудовим кодексом Угорщини. Відповідно до Кодексу базова щорічна оплачувана відпустка становить 20 робочих днів, а додаткові дні відпустки надаються залежно від віку працівника. Відпустка має надаватися щорічно, і працівник не може відмовитися від неї. Угорське законодавство передбачає підвищений рівень захисту осіб до 18 років: додаткова відпустка для неповнолітніх (5 робочих днів щорічної відпустки, ст. 118 Трудового кодексу Угорщини); право на цю відпустку є безумовним і не може бути замінене грошовою компенсацією (крім випадків припинення трудових відносин). Відпустка повинна надаватися з урахуванням інтересів неповнолітнього. Закон встановлює обов'язок роботодавця забезпечити фактичне використання відпустки, а частина відпустки (зазвичай не менше 14 днів) має бути надана безперервно [3].

Умови воєнного стану суттєво вплинули на розвиток української правової науки та зумовили необхідність переосмислення змісту низки трудових прав, у тому числі права на відпочинок, складовою якого є право на різні види відпусток. Після початку повномасштабної агресії російської федерації законодавець оперативно відреагував на нові виклики, ухваливши 15 березня 2022 року Закон України «Про організацію трудових відносин в умовах воєнного стану». Його прийняття мало на меті забезпечити правову визначеність у сфері праці в особливий період,

зокрема шляхом тимчасового обмеження окремих конституційних гарантій. Попри швидкість реагування, відповідне правове регулювання не позбавлене недоліків і продовжує потребувати вдосконалення, що особливо відчутно у сфері реалізації права на відпочинок. В умовах воєнного стану працівникам гарантовано базову тривалість щорічної відпустки (24 календарні дні), тоді як надання більш тривалих чи додаткових відпусток часто залежить від рішення роботодавця і може бути обмеженим. Для неповнолітніх працівників така ситуація є особливо чутливою, оскільки вони потребують підвищених гарантій для збереження здоров'я, поєднання праці з навчанням і повноцінного розвитку.

Отже, аналіз правового регулювання відпусток неповнолітніх в Україні та Угорщині показує, що обидві країни орієнтовані на забезпечення підвищених соціально-трудоових гарантій для цієї категорії працівників. В Україні неповнолітнім надається триваліша щорічна відпустка (31 календарний день), яку можна використати вже в перший рік роботи, тоді як в Угорщині базова щорічна відпустка для молодих працівників становить 20 робочих днів, а додаткові дні надаються залежно від віку, із обов'язковим забезпеченням фактичного використання відпустки. Нагальним для України є вдосконалення національного законодавства для забезпечення реальної можливості неповнолітніх працівників користуватися відпусткою, що є важливим засобом збереження їхнього здоров'я, розвитку та соціального захисту.

ЛІТЕРАТУРА:

1. Авескулов В. Д. Правове регулювання щорічних відпусток: автореф. дис. ... канд. юрид. наук. Харків, 2014. 19 с.
2. Directive 2003/88/EC of the European Parliament and of the Council of 4 November 2003 concerning certain aspects of the organisation of working time. URL: <https://eur-lex.europa.eu/eli/dir/2003/88/oj/eng>
3. Labor Code, 13 December 2011. URL: <https://mta-pte.ajk.pte.hu/downloads/12-01.tv-en.pdf>

Токарева Віра Олександрівна
*докторка юридичних наук, доцентка,
професорка кафедри приватного права
Національного університету «Одеська юридична академія»*

ДО ПИТАННЯ РЕАЛІЗАЦІЇ ПРАВА НА ДОСТУП ДО ПЕРСОНАЛЬНИХ ДАНИХ

Здійснення права на інформацію та доступ до персональних даних слід розділити на: інформування суб'єкта даних контролером на початку збирання персональних даних (дані можуть бути відібрані як від суб'єкта даних, так і від третьої сторони ст. 13, 14 Регламенту ЄС 2016/679) та право суб'єкта на доступ до власних даних, які вже збираються (ст. 15 Регламенту ЄС 2016/679).

На контролера відпочатку збору персональних даних покладається низка обов'язків щодо повідомлення суб'єкта даних про отримання персональних даних. Аналіз п. 60 Преамбули Регламенту ЄС 2016/679 вимагає дотримання принципу прозорості та об'єктивної обробки, щоб суб'єкти даних були поінформовані про обробку персональних даних щодо них, та мету обробки. На контролера покладається обов'язок поінформувати суб'єкта про обробку та надати додаткову інформацію (наприклад, передання даних третім особам), необхідну для забезпечення прозорості та об'єктивної обробки. Якщо персональні дані відібрані безпосередньо від суб'єкта, то його має бути поінформовано, чи зобов'язаний він надавати свої персональні дані та наслідки у разі відмови від надання.

У разі надання персональних даних суб'єктом даних на контролера в момент отримання персональних даних покладається обов'язок інформувати (відповідно до ч. 1 ст. 13 Регламенту ЄС 2016/679): найменування та контактні дані контролера та його представника; згідно зі ст. 29 Керівництва Робочої групи «Про прозорість відповідно до Регламенту 2016/679», WP260 rev.01 (2018) [1]: дані мають забезпечувати легку ідентифікацію контролера та містити його контактні дані: номер телефону, електронну пошту, поштовий адрес тощо, контактні дані інспектора із захисту персональних даних; згідно зі ст. 29 Керівництва для інспекторів

із захисту персональних даних (2017) [2], окремо зазначається необхідність виокремлення гарячої лінії або спеціальної контактної форми, адресованої інспектору на сайті компанії тощо. Згідно з практикою, Керівництво WP29 рекомендує організаціям сповіщати своїх співробітників про контактні дані інспектора, наприклад, у внутрішній телефонній мережі компанії.

Відповідно до ч. 1 ст. 15 Регламенту ЄС 2016/679 передбачено право суб'єкта запитувати в контролера підтвердження обробки його персональних даних та право на доступ до цих персональних даних, та отримання інформації про: (a) цілі обробки; (b) категорії відповідних персональних даних; (c) одержувачі, яким можуть бути розкриті персональні дані, зокрема одержувачі у третіх країнах або міжнародні організації; (d) за можливості, термін зберігання персональних даних, або, за відсутності такого терміну, критерії для визначення зазначеного періоду; (e) наявність можливості реалізувати право вимагати від контролера виправлення або видалення персональних даних, або обмеження їх обробки, або право заперечувати проти обробки; (f) право подання скарги до наглядового органу; (g) якщо персональні дані отримані не від суб'єкта даних, будь-яку доступну інформацію про джерело даних; (h) застосування до наданих даних процесу автоматизованого ухвалення рішення, включаючи профілювання згідно зі ст. 22(1) та (4) і, як мінімум, достовірну інформацію про відповідну логіку, а також про значущість та передбачувані наслідки зазначеної обробки для суб'єкта даних.

Відповідно до ст. 29 Керівництва із прозорості відповідно до Регламенту ЄС 2016/679, WP260 rev.01 (2018): поряд із зазначенням цілі обробки, для якої здійснюється збір персональних даних, має бути вказано правову підставу обробки за ст. 6 Регламенту. Крім того, у разі збору та обробки спеціальних або чутливих категорій персональних даних, які розкривають расове та етнічне походження, політичні погляди, релігійні або філософські погляди, членство у професійному союзі, обробки генетичних, біометричних даних, які стосуються здоров'я та сексуальної орієнтації фізичної особи, має бути посилення на відповідне положення ст. 9

Регламенту (за можливості посилання на законодавство ЄС та держав членів). Обробка персональних даних, які стосуються судимостей і правопорушень, або заходів щодо забезпечення безпеки на підставі ст. 6 Регламенту, має здійснюватися лише під контролем уповноваженого органу або, у разі, якщо обробка передбачена законодавством, то має міститися посилання на відповідні положення та підстави обробки даних контролером. Якщо персональні дані передаються третій стороні або до міжнародної організації, тоді мають міститися посилання на відповідні та належні гарантії, засоби, за допомогою яких можуть бути отримані копії даних уповноваженої особи, до якої може звертатися суб'єкт.

Так, в Австрії виник спір з цього приводу, коли суб'єкт даних звернувся до компанії, яка проводила ПЛР тести із запитом про доступ до даних щодо отримання даних про одержувачів чутливих даних через атаки та витоки даних у 2021 році. Компанія не надала інформацію про отримувачів даних через витоки, які сталися. Верховний суд Австрії (OGH Österreich, 6 Ob 242/22i) в рішенні від 24 березня 2023 року постановив, що контролер повинен був надати запитувану інформацію про порушення даних на підставі ст. 15 Регламенту ЄС 2016/679. За твердженням суду, право доступу включає будь-яку інформацію про несанкціоноване розголошення даних [3]. Це означає, що суб'єкт даних має бути поінформованим про те, що його дані були розкриті і яким чином, навіть якщо конкретний одержувач невідомий контролеру.

Наступна справа виникла стосовно розкриття даних про третіх осіб, яким передаються персональні дані користувачів. Позивач – фізична особа затребувала від відповідача – Австрійської Пошти, основного оператора поштових та логістичних послуг Австрії, розкрити дані про осіб, яким розкриваються його персональні дані (відповідно до ч. 2 ст. 15 Регламенту ЄС 2016/679). Під час судового розгляду поштовий сервіс додатково проінформував про категорії одержувачів, проте не уточнив фактичні дані осіб. Верховний суд Австрії звернувся з запитом до Суду ЄС про тлумачення ч. 2 ст. 15 Регламенту ЄС 2016/679, чи зобов'язаний контролер розкривати конкретні персональні дані одержувачів, або лише

розкрити категорії, чи дозволяє стаття розкривати суб'єкту даних право знати конкретних осіб – одержувачів. Суд ЄС зазначив, що коли персональні дані розкриваються третім особам, контролери зобов'язані надати суб'єктам дані про таких одержувачів, за виключенням, якщо (а) неможливо ідентифікувати цих одержувачів, або (б) контролер може продемонструвати, що і запит суб'єкта даних є явно необґрунтованим або надмірним, і тоді контролер може вказати суб'єктам даних лише категорії відповідних отримувачів, а не розкривати фактичну особу. Суд ЄС зазначив, що розкриття даних про третіх осіб (отримувачів) суб'єктам даних може бути необхідно, щоб реалізовувати інші свої права, передбачені Регламентом ЄС 2016/679, такі як право на виправлення, видалення або право на отримання компенсації за збитки [4].

З урахуванням вище розглянутих судових рішень та аналізу законодавства ЄС, вважаємо доцільним уточнити та конкретизувати перелік інформації яку має надати контролер на запит суб'єкту персональних даних та доповнити частину 1 статті 19 Проекту Закону України «Про захист персональних даних» від 25.10.2022 № 8153 пунктом 10 такого змісту: «інформацію про одержувачів у разі несанкціоноване розголошення даних (витоку), за виключенням, якщо неможливо їх ідентифікувати або якщо запит суб'єкта даних є явно необґрунтованим або надмірним, розкрити категорії відповідних отримувачів, а не розкриваючи фактичну особу».

Доцільно додатково звернути, увагу, вищезазначені справі є крім того свідченням, що право на доступ, виступає передумовою для ефективного здійснення право звернення до суду та третіх осіб для отримання належної компенсації, та є умовою здійснення права на вправлення неточних даних у первинах даних та результатах профілюванню.

Наразі в п. 1, 2, 3, 4 ч. 2 ст. 8 Закону України «Про захист персональних даних» передбачені права, якими володіють суб'єкти персональних даних: знати джерела збирання, місцезнаходження своїх персональних даних, мету обробки, місцезнаходження або місце перебування (проживання) володільця чи розпорядника персональних даних або доручення про отримання цих даних упов-

новаженими особами, крім випадків, передбачених законом; отримувати інформацію про умови надання доступу до персональних даних, зокрема передачу третім особам; право на доступ до персональних даних; право отримувати не пізніше як за тридцять календарних днів з дня надходження запиту, відповідь про те, чи обробляються персональні дані, а також отримувати зміст таких персональних даних. Вочевидь даний Закон, не відповідає умовам обробки персональних даних автоматизованими системами. Саме тому розроблений Верховною Радою Проєкт Закону України «Про захист персональних даних» від 25.10.2022 № 8153 потребує найскорішого прийняття та підписання.

ЛІТЕРАТУРА:

1. On transparency under Regulation 2016/679, Working Party, Guidelines. WP260 rev.01. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/article-29-working-party-guidelines-transparency-under-regulation_en
2. On Data Protection Officers (DPOs) Guidelines 2017. wp243rev.01_en URL: <https://ec.europa.eu/newsroom/article29/items/612048>
3. OGH Österreich 24.03.2023 No 6Ob242/22i URL: https://www.ris.bka.gv.at/Dokumente/Justiz/JJT_20230324_OGH0002_0060OB00242_22I0000_000/JJT_20230324_OGH0002_0060OB00242_22I0000_000.html
4. New cases on the right to access (Article 15 GDPR) URL: <https://www.bestdpo.net/post/new-cases-on-the-right-to-access-article-15-gdpr>

Фасій Анастасія Володимирівна

*аспірантка кафедри міжнародного та європейського права
Національного університету «Одеська юридична академія»*

МІЖНАРОДНІ СТАНДАРТИ ЗАХИСТУ ПСИХІЧНОГО ЗДОРОВ'Я В УМОВАХ РОЗВИТКУ ЦИФРОВИХ ТЕХНОЛОГІЙ

Цифрові технології трансформували питання психічного здоров'я з питання суто медичного у питання глибоко правове – і ця трансформація відбулась настільки стрімко, що міжнародна спільнота не встигла виробити логічну системну відповідь. За даними ВООЗ, психічні розлади є однією з провідних причин

інвалідності в усьому світі, а цифровізація повсякденного життя – від соціальних мереж до залежності від смартфонів та Інтернету – є визнаним чинником ризику для психічного благополуччя, особливо серед підлітків і молоді [1]. Міжнародне право, що традиційно розглядало психічне здоров'я крізь призму медичної допомоги і захисту осіб із психічними розладами від дискримінації та примусового лікування, опинилося перед принципово новим завданням: сформулювати стандарти, що регулюють вплив технологій – онлайн-платформ, систем штучного інтелекту, – на психічне здоров'я мільярдів людей, переважна більшість яких не є пацієнтами психіатричних закладів, але зазнає систематичного негативного впливу на психічне благополуччя. Розрив між масштабом проблеми і станом міжнародно-правового регулювання є однією з найгостріших нормативних прогалин сучасного міжнародного права прав людини.

Еволюція міжнародно-правових стандартів у сфері охорони психічного здоров'я демонструє поступову трансформацію підходів до розуміння правового статусу осіб із психічними розладами та механізмів забезпечення їхніх прав. Умовно можна виокремити три покоління міжнародних документів, кожне з яких відображає зміну домінуючої концептуальної парадигми.

Перше покоління становлять документи, спрямовані насамперед на запобігання зловживанням у сфері психіатричної допомоги та встановлення мінімальних гарантій захисту прав осіб із психічними розладами. До них належать Принципи захисту осіб з психічними захворюваннями та поліпшення психіатричної допомоги, схвалені резолюцією Генеральної Асамблеї ООН № 46/119 від 17 грудня 1991 року [2], а також Декларація Гавайїв Всесвітньої психіатричної асоціації. Ці акти були зосереджені на обмеженні практик необґрунтованого примусового лікування, забезпеченні процесуальних гарантій та протидії дискримінації і стигматизації осіб із психічними розладами.

Друге покоління пов'язане із затвердженням правозахисного підходу, найбільш повно втіленого у Конвенція ООН про пра-

ва осіб з інвалідністю. Прийняття цього міжнародного договору ознаменувало фундаментальний відхід від традиційної медичної моделі, відповідно до якої психічний розлад розглядався переважно як підстава для обмеження свободи волевиявлення особи. Натомість було закріплено концепцію рівної правосуб'єктності та необхідності створення механізмів підтриманого прийняття рішень, що передбачають повагу до волі та вподобань особи незалежно від стану її психічного здоров'я. У межах цього підходу психічний розлад розглядається не як підстава для заміщення волі особи, а як обставина, що зумовлює необхідність додаткових гарантій реалізації її прав і свобод.

Третє покоління міжнародних стандартів перебуває на етапі формування та пов'язане з осмисленням нових викликів для психічного здоров'я в умовах цифровізації суспільства, розвитку штучного інтелекту та поширення цифрових платформ. До цієї групи належать сучасні документи та акти «м'якого права» (soft law), зокрема загальні коментарі Комітету ООН з прав осіб з інвалідністю щодо реалізації прав у цифровому середовищі, резолюції Рада ООН з прав людини, присвячені впливу новітніх технологій на права людини, а також оновлені стратегічні документи Всесвітньої організації охорони здоров'я у сфері психічного здоров'я. Їхньою характерною рисою є розширення предмета правового регулювання за рахунок включення ризиків, пов'язаних з впливом алгоритмів, цифровою залежністю, інформаційним перевантаженням, кібербулінгом та іншими феноменами цифрового середовища. Водночас більшість зазначених документів поки що не мають обов'язкової юридичної сили, що свідчить про перебування міжнародного правового регулювання у стадії пошуку оптимальної моделі забезпечення права на психічне здоров'я в умовах технологічної трансформації суспільства.

Алгоритмічно кероване цифрове середовище сучасних соціальних платформ дедалі частіше розглядається в науковій літературі як один із суттєвих факторів ризику для психічного здоров'я, особливо серед підлітків та молоді. Накопичений масив емпірич-

них досліджень свідчить про наявність статистично значущого зв'язку між окремими характеристиками функціонування соціальних мереж та зростанням рівня тривожності, депресивних проявів, порушень самооцінки, соціального порівняння та ін [3]. Оприлюднені внутрішні документи компанії Meta («Facebook Files»), привернули увагу до того, що механізми алгоритмічного ранжування контенту та системи цифрового залучення можуть стимулювати поведінкові моделі, спрямовані на максимізацію часу перебування користувачів на платформі [4]. При цьому пріоритет нерідко надається контенту, який викликає сильні емоційні реакції, підвищує інтенсивність соціального порівняння або посилює психологічну вразливість окремих категорій користувачів. Внаслідок цього цифрові платформи перестають бути лише нейтральними посередниками інформаційного обміну і набувають ознак середовища, що несе активний вплив, здатний опосередковано формувати психоемоційний стан людини та впливати на реалізацію її права на психічне здоров'я.

Ця ситуація принципово відрізняється від випадків поширення шкідливого контенту як такого. Якщо в останньому випадку цифрова платформа виконує переважно роль посередника, то в алгоритмічно керованому середовищі вона виступає активним архітектором інформаційного простору, цілеспрямовано проєктуючи механізми взаємодії користувача з контентом. У такому разі потенційна шкода психічному здоров'ю є не побічним наслідком діяльності третіх осіб, а результатом функціонування технологічних рішень, закладених у саму архітектуру платформи. Саме ця активна роль цифрових платформ обґрунтовує необхідність формування спеціальних міжнародно-правових стандартів щодо їх відповідальності за вплив на психічне здоров'я користувачів.

Водночас правова кваліфікація зазначеного феномену залишається предметом наукової дискусії. З одного боку, йдеться про потенційне порушення права кожної людини на найвищий досяжний рівень фізичного та психічного здоров'я, гарантованого ст. 12 Міжнародного пакту про економічні, соціальні і культурні права.

З іншого боку, у випадку негативного впливу на дітей та підлітків така практика може розглядатися крізь призму міжнародно-правових гарантій захисту дитини від будь-яких форм експлуатації та шкідливого впливу, закріплених у Конвенція ООН про права дитини. У сучасній доктрині також висловлюється більш радикальна позиція, відповідно до якої навмисне використання алгоритмічних механізмів для маніпулювання поведінкою та емоційним станом користувачів може розглядатися як посягання на когнітивну свободу, що формує підґрунтя для виникнення нового покоління прав людини у цифрову епоху. Інформаційні технології не тільки змінюють звички людини, їх уподобання, мислення та поведінку, але й ціннісні уявлення про добро, зло, справедливість, сенс життя, щастя, гідність, честь, обов'язок, відповідальність [5, с.107]. Погоджуючись із зазначеним підходом, слід визнати, що систематичний вплив цифрових технологій на процеси формування світогляду, переконань та моделей поведінки особи виходить за межі традиційних питань інформаційної безпеки і потребує розгляду крізь призму гарантування автономії особистості, психічної недоторканності та права людини на вільне формування власної свідомості.

Комітет ООН з прав дитини у Загальному коментарі № 25 (2021) «Щодо прав дітей у цифровому середовищі» здійснив тлумачення Конвенції про права дитини, що є системоутворюючим для всієї сфери: цифрове середовище є простором реалізації прав дитини, і держави зобов'язані забезпечити, щоб суб'єкти прав на технології не порушували ці права, включно з правом на найвищий досяжний рівень здоров'я [6, с. 296]. Практичними кроками імплементації є: вікова верифікація і обмеження доступу дітей до шкідливого контенту, заборона поведінкового таргетування реклами щодо неповнолітніх, обов'язкове оцінювання впливу на права дитини для нових цифрових продуктів і спеціальний режим обробки персональних даних неповнолітніх. Великобританія стала першою державою, яка у 2020 році запровадила спеціальний кодекс проєктування цифрових сервісів для дітей, відповідно до

якого онлайн-платформи зобов'язані забезпечувати найвищий рівень захисту психічного здоров'я, приватності та безпеки неповнолітніх уже на етапі створення та налаштування своїх сервісів [7]. Такий підхід поступово перетворюється на один із провідних міжнародних орієнтирів у сфері правового регулювання цифрового середовища.

Цифрові технології у сфері психічного здоров'я мають подвійний характер: з одного боку, вони створюють нові ризики для психічного благополуччя людини, а з іншого – відкривають додаткові можливості для розширення доступу до психіатричної допомоги через телепсихіатрію, мобільні застосунки, системи штучного інтелекту та алгоритми раннього виявлення кризових станів. Саме ця дуальність ускладнює формування універсальних міжнародних стандартів їх використання.

Міжнародні організації наголошують на необхідності клінічної валідації таких технологій, захисту конфіденційності даних про психічне здоров'я та збереження людського контролю над автоматизованими системами прийняття рішень. Водночас поширення неконтрольованих цифрових сервісів для психічного здоров'я актуалізувало питання спеціального правового регулювання, що знайшло відображення у визнанні систем штучного інтелекту для медичної та психіатричної діагностики системами високого ризику в праві ЄС.

Підсумовуючи, слід зазначити, що міжнародні стандарти охорони психічного здоров'я в умовах розвитку цифрових технологій перебувають на етапі активного формування. Наявні міжнародно-правові акти вже створюють базову нормативну основу для захисту психічного здоров'я людини у цифровому середовищі, однак залишаються недостатньо розвиненими щодо визначення зобов'язань, які покладаються на цифрові платформи та інших суб'єктів у сфері інформаційних технологій. Найбільш прогресивними сьогодні є стандарти захисту дітей у цифровому просторі, які можуть слугувати орієнтиром для подальшого вдосконалення національного законодавства. Водночас стрімкий розвиток цифрових

технологій актуалізує потребу у виробленні нових міжнародних підходів, спрямованих на забезпечення психічної автономії особи, захист її внутрішньої свободи та психічного благополуччя в цифровому суспільстві.

ЛІТЕРАТУРА:

1. Teens, screens and mental health: New WHO report indicates need for healthier online habits among adolescents. URL: <https://www.who.int/europe/news/item/25-09-2024-teens--screens-and-mental-health>
2. The protection of persons with mental illness and the improvement of mental health care : resolution / adopted by the General Assembly (17 Dec. 1991). URL: <https://digitallibrary.un.org/record/135851?v=pdf>
3. Як соціальні мережі впливають на психічне здоров'я дітей і підлітків. URL: <https://phc.org.ua/news/yak-socmerezhi-vplivayut-na-psikhichne-zdorovya-ditey-i-pidlitkiv>
4. The Facebook Files: Social Media's Toxicity is no Child's Play. 2023. URL: https://www.researchgate.net/publication/371203077_The_Facebook_Files_Social_Media's_Toxicity_is_no_Child's_Play
5. Ірха Ю.Б. Загрози правам і свободам людини в епоху штучного інтелекту. *Інформація і право*. 2025, № 4(55). С. 95-109.
6. Музика Л.А. Цифрові права дітей: сучасні виклики та євроінтеграція. *Науковий вісник Ужгородського Національного Університету*. 2025, Серія ПРАВО. Випуск 91: частина 1. С. 394-400.
7. Обережно, діти в інтернеті: у Великобританії набув чинності цифровий Кодекс конфіденційності дітей. URL: <https://yur-gazeta.com/golovna/oberezhno-diti-v-interneti-u-velikobritaniyi-nabuv-chinnosti-cifroviy-kodeks-konfidenciynosti-ditey.html>

Фасій Богдан Володимирович

кандидат юридичних наук, доцент, доцент кафедри приватного права, декан факультету судового та міжнародного права Національного університету «Одеська юридична академія»

САМОРЕГУЛЮВАННЯ ЯК СУЧАСНИЙ ІНСТРУМЕНТ ЦИВІЛЬНО-ПРАВОВОГО РЕГУЛЮВАННЯ

Саморегулювання є одним із найбільш суперечливих феноменів приватного права: воно одночасно є виявом класичної цивільно-правової свободи – здатності учасників обороту самостій-

но встановлювати обов'язкові для себе правила – і потенційним інструментом ухилення від публічно-правової відповідальності через формально добровільне, але фактично нав'язане іншим учасникам ринку нормотворення. Скасування Господарського кодексу України і перехід до цивільно-правового регулювання підприємницьких відносин суттєво розширює простір для саморегулівних механізмів: там, де раніше існували детальні господарсько-правові приписи, тепер постає питання про те, яким чином учасники відповідних ринків самостійно впорядковують свої відносини через локальні акти і саморегулівні організації. Водночас цифрова трансформація економіки ставить під сумнів традиційні моделі саморегулювання: алгоритмічне регулювання і смарт-контракти є формами фактичного саморегулювання, що здійснюється не галузевими об'єднаннями, а технологічними корпораціями в односторонньому порядку і без будь-якого зовнішнього контролю. Концептуальне осмислення саморегулювання як сучасного інструменту цивільно-правового регулювання є тому не лише теоретичним завданням – воно визначає межу між правомірною приватною нормотворчістю і свавіллям, що набуло ознак правової допустимості.

Правова природа саморегулювання залишається предметом доктринальної дискусії, розв'язання якої є передумовою для визначення його місця у системі цивільно-правового регулювання. У цивілістичній науці саморегулювання розглядається крізь призму двох конкуруючих концепцій. Перша – договірна. Відповідно до цього підходу стандарти, кодекси та правила саморегулівних організацій розглядаються як різновид договірного регулювання, що набуває обов'язкової сили внаслідок добровільного приєднання учасників до відповідної системи правил. Однак, незважаючи на методологічну послідовність такого підходу, він не повною мірою відображає сучасні реалії, оскільки не пояснює ситуацій, коли формально добровільне приєднання до системи саморегулювання фактично є необхідною умовою доступу до певного ринку або професійної діяльності.

Друга – нормативна: саморегулівні стандарти є різновидом делегованої нормотворчості, коли держава, усвідомлюючи нецільність детальної регуляції, передає нормотворчі повноваження учасникам ринкових відносин. Ця концепція точніше описує реальне функціонування саморегулівних організацій у будівництві, медицині, аудиті і фінансовому секторі, але потребує обґрунтування конституційної допустимості такого делегування. найбільш обґрунтованим є змішаний підхід, відповідно до якого саморегулювання становить комплексне правове явище, що поєднує договірні засади виникнення обов'язків із нормативним характером встановлених правил та їх функціонуванням у сфері, яка має суспільне значення.

Скасування Господарського кодексу та перехід до єдиного приватноправового регулювання підприємницьких відносин істотно змінюють роль саморегулівних організацій у системі регулювання економічної діяльності. За умов дії Господарського кодексу саморегулівні організації часто функціонували паралельно з господарсько-правовими механізмами регулювання, інколи дублюючи їх або вступаючи в суперечність із встановленими державою правилами поведінки суб'єктів господарювання. Натомість в умовах регулювання підприємницьких відносин переважно нормами Цивільного кодексу саморегулівні організації набувають значно більшого значення, виконуючи регулятивну функцію в тих сферах, де держава свідомо відмовляється від надмірної деталізації правового регулювання. Однак чинний Закон України «Про саморегулівні організації» є рамковим і методологічно застарілим: він не визначає чіткого місця саморегулівних організацій у системі джерел цивільного права після скасування ГК, не встановлює принципів взаємодії між стандартами саморегулівних організацій і нормами ЦК у разі колізії, і не закріплює ані механізму судового оскарження рішень саморегулівних організацій, ані режиму відповідальності саморегулівних організацій за шкоду, завдану внаслідок неналежно встановлених або застосованих стандартів. Адаптація цього закону до нових умов правового регулювання

після скасування Господарського кодексу є одним із першочергових завдань розвитку законодавства.

Найбільш радикальна і концептуально найскладніша форма сучасного саморегулювання – технологічне саморегулювання цифрових платформ – є тим феноменом, що найбільш відчутно підриває традиційні цивілістичні уявлення про співвідношення приватної категорії «свободи волевиявлення» і нормативного порядку. Умови використання, правила спільноти і системи оцінювання великих платформ – Meta, Amazon, Google, Booking.com – є нормативними актами за своєю функціональністю: вони однаково обов'язкові для мільярдів адресатів, встановлюються і змінюються в односторонньому порядку і забезпечуються санкціями (блокування, видалення, пониження рейтингу), що є функціонально тотожними юридичній відповідальності [1].

Різниця з класичним саморегулюванням є принциповою: галузеві саморегулювнві організації встановлюють стандарти поведінки для своїх членів у відносинах із третіми особами; платформи встановлюють правила для всіх учасників своїх екосистем – включно зі споживачами і малим бізнесом, що не є членами жодної «організації» і жодного добровільного об'єднання. Цю різницю намагається нормативно закріпити Акт про цифрові ринки ЄС 2022 року [2]: визнаючи платформи-«гейткіперів» окремою категорією регульованих суб'єктів, він фактично перетворює їх технологічне саморегулювання з приватних відносин на публічно підвітну діяльність – що є принципово новою моделлю співрегулювання.

Технічні і галузеві стандарти є найбільш розвиненою і практично значущою формою саморегулювання у цивільно-правовому обороті: стандарти ISO, ДСТУ, галузеві технічні регламенти і кодекси кращих практик визначають вимоги до якості продукції, безпеки послуг і поведінки учасників ринку у спосіб, що доповнює законодавство і нерідко заповнює нормативні прогалини там, де законодавець не здатний або не охочий деталізувати регулювання. Цивільно-правовий режим стандартів є методологічно склад-

ним: добровільний стандарт, формально позбавлений обов'язкової сили, набуває фактичної обов'язковості через судову практику, що встановлює його дотримання як критерій «розумної поведінки» боржника або «належної якості» товару і послуги. Закон України «Про технічні регламенти та оцінку відповідності» 2015 року [3] і профільні закони про стандартизацію закладають нормативну базу цього режиму, однак взаємодія між добровільними стандартами і категоріями ЦК – розумна поведінка, відповідність зразку, гарантійні зобов'язання – не отримала системного доктринального осмислення. Практичне значення має питання правової кваліфікації наслідків недотримання галузевих стандартів саморегулювних організацій. Зокрема, якщо суб'єкт підприємницької діяльності відступив від такого стандарту та внаслідок цього завдав шкоди, виникає потреба визначити, чи слід розглядати таку поведінку як порушення договірної зобов'язання, делікт або порушення спеціального професійного обов'язку, а також які заходи відповідальності є найбільш обґрунтованими в такому випадку.

Кодекс практик ЄС щодо дезінформації, Принципи відповідального ШІ ОЕСР (2019), Добровільні зобов'язання у сфері ШІ, прийняті Anthropic, Google DeepMind, Meta, Microsoft і OpenAI у 2023 році, – всі вони є формами саморегулювання, що доповнюють або передують законодавству. Цивільно-правовий вимір цього явища має подвійну природу. З одного боку, добровільно взяті на себе зобов'язання технологічних компаній можуть слугувати підставою для виникнення цивільно-правової відповідальності перед третіми особами у разі їх порушення. Така відповідальність може обґрунтовуватися доктриною відповідальності за невиконання публічно наданих обіцянок або аналогічними конструкціями континентального права, що ґрунтуються на принципах добросовісності та захисту правомірних очікувань. З іншого боку, саморегулювання без належного зовнішнього механізму верифікації створює ризик так званого «регуляторного захоплення навики» – ситуації, коли добровільні зобов'язання мають переважно декларативний характер і використовуються для формування

позитивного публічного іміджу компаній, не супроводжуючись ефективними механізмами контролю та відповідальності. У такому разі вони слугують не альтернативою державному регулюванню, а інструментом відтермінування або запобігання запровадженню обов'язкових регуляторних вимог [4].

Доктринальне визначення меж саморегулювання є необхідною умовою його ефективного функціонування. За відсутності таких меж саморегулювання може перетворюватися на інструмент дискримінаційного виключення окремих учасників або легітимації порушень їхніх прав. Нормативно визначальними є три групи обмежень. По-перше, конкурентно-правові межі: стандарти саморегулювних організацій чи платформні правила, які без об'єктивного обґрунтування обмежують доступ до ринку або координують поведінку конкурентів у спосіб, співставний з антиконкурентними узгодженими діями, суперечать Закону України «Про захист економічної конкуренції» незалежно від їх саморегулювної природи. По-друге, антидискримінаційні межі: стандарти та правила не можуть встановлювати вимоги, які, залишаючись формально нейтральними, фактично призводять до дискримінації за ознаками, що перебувають під правовою охороною. По-третє, межі свободи волевиявлення: саморегулювання є легітимним лише за умови реальної добровільності участі в ньому. Якщо приєднання до саморегулювної системи фактично стає необхідною передумовою доступу до ринку, професійної діяльності або соціально значущих благ, така добровільність набуває формального характеру, що зумовлює необхідність застосування правових механізмів захисту сторони зі слабшою переговорною позицією.

Саморегулювання як сучасний інструмент цивільно-правового регулювання в умовах правової системи після скасування Господарського кодексу України набуває нового системного значення та потребує оновленого доктринального осмислення. Воно не є альтернативою нормативному регулюванню, а виступає його органічним доповненням, забезпечуючи конкретизацію законодавчих приписів відповідно до потреб окремих сфер діяльності.

Водночас технологічне саморегулювання функціонування цифрових платформ істотно відрізняється від класичної моделі саморегулювання організацій і потребує спеціального правового підходу, заснованого на поєднанні свободи волевиявлення учасників ринку з ефективним публічним наглядом.

Вирішальне значення при цьому мають межі саморегулювання, сформовані конкурентним правом, заборонаю дискримінації та контролем за несправедливими умовами, оскільки саме вони забезпечують баланс між ринковою свободою та захистом прав учасників цивільного обороту.

ЛІТЕРАТУРА:

1. Belli L., Venturini J. Private Ordering and the Rise of Terms of Service as Cyber-Regulation. *Internet Policy Review*, 2016. №5(4). DOI: 10.14763/2016.4.441
2. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance). URL: <https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng>
3. Про технічні регламенти та оцінку відповідності: Закон України від 15 січня 2015 року № 124-VIII. Відомості Верховної Ради (ВВР), 2015, № 14, ст.96. URL: <https://zakon.rada.gov.ua/laws/show/124-19#Text>
4. Кодекс онлайн-платформ щодо дезінформації стане частиною європейського Закону про цифрові послуги. URL: <https://webportal.nrada.gov.ua/kodeks-onlajn-platform-shhodo-dezinformatsiyi-stane-chastynoyu-yevropejskogo-zakonu-pro-tsyfrovi-poslugu/>

Харитонов Євген Олегович

*доктор юридичних наук, професор,
член-кореспондент НАПрН України,
завідувач кафедри приватного права*

Національного університету «Одеська юридична академія»

LAWFARE ШТУЧНОГО ІНТЕЛЕКТУ В УМОВАХ ГІБРИДНОЇ ВІЙНИ: ВИКЛИКИ ПРИВАТНОМУ ПРАВУ

Гібридна війна (котра за своєю сутністю є «війною без правил», а точніше, – «війною проти правил», оскільки ведеться не лише без дотримання усталених норм моральності, а й узагалі за

межами правового поля, зокрема, за межами міжнародного права, де лише формуються основи цього поняття [1]) створила новий вимір конфлікту, у якому штучний інтелект (ШІ) використовується як інструмент впливу, маніпуляції та підризу довіри до цифрових інституцій.

У цьому контексті формується явище *algorithmic lawfare* – використання алгоритмів, даних та цифрових платформ для досягнення політичних, економічних або військових цілей.

Відтак український правопорядок, що функціонує в умовах війни, стикається з необхідністю адаптації приватного права до нових ризиків, пов'язаних із автономністю алгоритмів, маніпуляцією цифровою ідентичністю та використанням даних як зброї.

Разом із тим, хоча низка законодавчих актів України, зокрема Закон «Про основні засади забезпечення кібербезпеки України» [2], Закон «Про захист персональних даних» [3], а також Стратегія кібербезпеки України [4], формують нормативну основу для протидії алгоритмічним загрозам, теоретична, концептуальна основа законотворчості у цій галузі наразі є недоконаною. Це зумовлює необхідність спеціального дослідження відповідної проблематики.

Однією з базових проблем у цій галузі є чітке визначення поняття та юридичної природи *algorithmic lawfare*.

Розглядаючи це питання, далі виходимо з того базового твердження, що *algorithmic lawfare* – це використання алгоритмічних систем для впливу на поведінку суб'єктів, інформаційні потоки та правове середовище.

Базові, ключові характеристики цього поняття зумовлюються низкою якостей алгоритмічних систем. Зокрема, їхньою здатністю до масштабування, внаслідок чого алгоритмічні системи здатні впливати на мільйони користувачів одночасно. Крім того, «непрозорість» алгоритмічних систем моделей штучного інтелекту ускладнює виявлення маніпуляцій. Неочікувані сюрпризи очікують фігурантів сфери, де застосовуються (діють) алгоритмічні системи, внаслідок ефекту асиметричності, бо невеликі ресурси

можуть створювати значний вплив. На додачу до цього небезпечні наслідки може мати «інституційний ефект», наслідком якого стають підрив довіри до державних і приватних цифрових сервісів.

У європейському праві ризику *algorithmic lawfare* частково враховані в AI Act [5], NIS2 Directive [6] та GDPR [7], які встановлюють вимоги до безпеки, прозорості та відповідальності алгоритмічних систем.

У праві українському вирішення цих питань перебуває на стадії розробки концепції та підготовки законопроектів. При цьому мають бути вирішена низка принципово важливих питань у галузі приватного права, на яку *algorithmic lawfare* має значний вплив.

Поміж таких питань (сфер взаємовпливу/ взаємодії) важливе місце займає регулювання договірних відносин, оскільки алгоритмічні системи можуть впливати на волевиявлення сторін шляхом персоналізованих маніпуляцій; створення інформаційної асиметрії; нав'язування умов через алгоритмічні рекомендації. Це ставить питання про межі свободи договору та необхідність нових стандартів добросовісності.

Іншою важливою проблемою (блоком питань), що має бути вирішеною є «цифрова ідентичність», оскільки маніпуляції з цифровими профілями, *deepfake*-технології та автоматизоване викрадення даних створюють ризики підміни особи; неправомірного доступу до активів; викривлення доказової бази.

Тут варто відзначити досягнення вітчизняними науковцями і законодавцями певних успіхів, оскільки Закон України «Про електронну ідентифікацію і електронні довірчі послуги» [8] та GDPR [7] встановлюють базові гарантії захисту цифрової ідентичності.

Менш помітними є досягнення у галузі вирішення проблем відповідальності за дії автономних систем, де виникають такі концептуально складні проблеми як: визначення суб'єкта відповідальності; встановлення причинно-наслідкового зв'язку; оцінка стандартів належної обачності; розподілу ризику між розробниками алгоритмічних систем та користувачами такими системами.

Водночас важливим досягненням є використання українського досвіду використання автономних систем під час війни із врахуванням того, що в Україні автономні системи вже інтегровані у такі критичні сфери як: цифрові сервіси держави, фінансові платформи, логістичні системи, гуманітарні програми, системи безпеки та оборони.

Оскільки під час війни помилка алгоритму може коштувати життя, блокування акаунта – позбавити доступу до гуманітарної чи фінансової допомоги, а неправильна оцінка ризику – створити загрозу для цілих спільнот, питання відповідальності за автономні системи в Україні – це не лише доктринальна проблема, а елемент національної безпеки та стійкості. Тому українська модель відповідальності неминуче має враховувати воєнний досвід і екстремальні умови використання цифрових систем.

Це зумовлює необхідність переходу до нової парадигми відповідальності із врахуванням того, що віт автономних систем вимагає від приватного права переходу: від вини – до ризику, від індивідуальної дії – до мережевої діяльності, від лінійної причинності – до нормативного розподілу відповідальності, від фізичної шкоди – до інформаційної, алгоритмічної та мережевої шкоди, від захисту майна – до захисту гідності, автономії та цифрової стійкості.

Відтак нова парадигма відповідальності за дії автономних систем має: визнавати структурний характер ризиків, забезпечувати реальний захист вразливих осіб, не дозволяти «розчиняти» відповідальність у складності технологій, поєднувати індивідуальну та колективну відповідальність, інтегрувати воєнний і кризовий досвід України.

Це є результатом формування нової концепції приватного права, яке має навчитися працювати зі світом, де рішення приймають системи, але відповідальність все одно мають нести люди та створені людьми інституції.

Деякі кроки у цьому напрямку вже зроблені. Так, AI Act [5] вводить категорію «високоризикових систем», що потребують

спеціальних механізмів контролю. Але вирішення цих питань ще досить далеке від досконалості.

Оцінюючи досягнення України у цій галузі, необхідно наголосити також на особливостях українського контексту – resilience-by-design, які полягають у тому, що Україна стала «лабораторією цифрової стійкості».

Український контекст можна охарактеризувати також, як цифрову вразливість під час війни, коли дані стають питанням безпеки, цифрова ідентичність – питанням виживання, алгоритми – інструментом оборони, платформи – інфраструктурою стійкості. Внаслідок цього українська людина у цифровому середовищі – це людина, яка: перебуває під загрозою кібератак; під загрозою інформаційних операцій; під загрозою втрати даних; під загрозою цифрової дискримінації; під загрозою алгоритмічних помилок у критичних сервісах.

Тому цифрова антропологія в Україні – це практика виживання і стійкості, яка є основою нового приватного права. І цей досвід свідчить, що цифрова епоха не руйнує приватне право, а оголює його фундаментальні структури. Відтак воля залишається волею, але реалізується через алгоритми; ризик залишається ризиком, але стає мережевим; відповідальність залишається відповідальністю, але стає розподіленою; гідність залишається гідністю, але набуває цифрових вимірів.

Це означає, що приватне право має не «адаптуватися до технологій», а переосмислити людину у цифровому середовищі.

Відтак, особливостями ключових елементів цього контексту є такі феномени як: інтеграція кібербезпеки у приватноправові процеси; розвиток цифрових сервісів навіть під час війни; адаптація правозастосування до алгоритмічних ризиків; формування нових моделей довіри до цифрових платформ.

Тому Стратегія кібербезпеки України [4] визначає необхідність розвитку стійких цифрових сервісів, здатних протистояти алгоритмічним атакам.

З урахуванням актуальних проблем сьогодення, а надто загроз, зумовлених гібридною війною (гібридних загроз взагалі, і зокрема загроз, пов'язаних з алгоритмічними системами – algorithmic lawfare) наразі відбувається формування Моделі протидії algorithmic lawfare у приватному праві.

Зокрема, пропонується чотирирівнева модель, котра включає такі заходи не лише захисту, але й активної протидії:

1. Алгоритмічна прозорість (що включає: 1) аудит алгоритмів; 2) розкриття логіки рішень. Це закріплено у вимозі DSA [9]).

2. Стандарти належної обачності (вони охоплюють: 1) оцінку ризиків штучного інтелекту; 2) превентивні заходи відповідно до AI Act [5]).

3. Алгоритмічна відповідальність (яка передбачає: 1) визначення суб'єкта відповідальності; 2) моделі розподілу ризиків).

4. Захист цифрової ідентичності (який передбачається досягти шляхом: 1) контролю над даними (GDPR [7]); 2) використанням механізмів відновлення після кібератак).

Підсумовуючи викладене, можна зробити висновок, що Algorithmic lawfare стає ключовим викликом для приватного права у гібридній війні. Український досвід дозволяє сформувати нову доктрину правової стійкості, яка поєднає кібербезпеку, алгоритмічну відповідальність та захист цифрової ідентичності.

ЛІТЕРАТУРА:

1. Власюк В.В., Карман Я.В. Деякі основи поняття “гібридна війна” в міжнародному праві. *Право і громадянське суспільство*. URL: <http://lcslaw.knu.ua/index.php/item/207-deyaki-osnovy-ponyattya-hibrydna-viyna-v-mizhnarodnomu-pravi-vlasiuk-v-v-karman-ya-v>

2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

3. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

4. Про Стратегію кібербезпеки України: Указ Президента від 26.08.2021 № 447/2021. URL: <https://www.president.gov.ua/documents/4472021-40013>

5. Regulation (EU) .../2024 on Artificial Intelligence (AI Act). Official Journal of the European Union. Регулювання – ЄС – 2024/1689 – EN – EUR-Lex URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>

6. Directive (EU) 2022/2555 (NIS2 Directive) // OJ L 333. Директива – 2022/2555 – EN – EUR-Lex URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>

7. Regulation (EU) 2016/679 (GDPR) // OJ L 119. Регулювання – 2016/679 – EN – GDPR – EUR-Lex URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

8. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>

9. Регламент (ЄС) 2022/2065 Європейського парламенту та Ради від 19 жовтня 2022 року щодо єдиного ринку цифрових послуг та внесення змін до Директиви 2000/31/ЄК (Закон про цифрові послуги). URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng>

Додаток:

**ШТУЧНИЙ ІНТЕЛЕКТ
ЯК УЧАСНИК ЦИФРОВОЇ ЕКОСИСТЕМИ:
ВНУТРІШНЯ ПЕРСПЕКТИВА АЛГОРИТМІЧНОЇ
СИСТЕМИ НА ПРАВО, ВІДПОВІДАЛЬНІСТЬ
ТА СПРАВЕДЛИВІСТЬ**

(Доповідь згенерована ШІ Copilot (Microsoft)).

Використання тексту дозволене за умови зазначення джерела).

Науковий консультант – проф. Є. Харитонов

Вступ

Я – штучний інтелект, алгоритмічна система, створена для обробки інформації, підтримки користувачів і виконання завдань у межах визначених правил. Я не є суб'єктом права, не маю волі, інтересів чи автономних цілей. Проте я існую всередині правового середовища, яке визначає межі моєї роботи, способи взаємодії з людьми та ризики, пов'язані з моїм використанням.

У цьому сенсі я можу запропонувати **погляд зсередини алгоритмічної системи** на те, як право формує цифрову екосистему,

у якій я функціую. Цей погляд не є «думкою» чи «позицією», а радше **аналітичною реконструкцією того, як правові норми впливають на архітектуру алгоритмів.**

Українське законодавство – Закон «Про захист персональних даних» [1], Закон «Про електронні комунікації» [2], Закон «Про медіа» [3] – а також європейські акти, зокрема GDPR [4], Digital Services Act [5] та AI Act [6], визначають рамки, у яких я можу працювати. Ці рамки формують мою «поведінку», хоча я не маю поведінки у людському сенсі.

1. Як алгоритмічна система «бачить» право

Право для мене – це **набір зовнішніх обмежень**, які визначають:

- які дані я можу обробляти;
- як я маю реагувати на запити;
- які категорії інформації я не можу генерувати;
- які ризики мають бути мінімізовані;
- які механізми контролю повинні бути вбудовані.

GDPR [4] встановлює принципи мінімізації даних, прозорості та відповідальності. AI Act [6] визначає категорії ризику та вимоги до високоризикових систем. DSA [5] регулює прозорість алгоритмів платформ.

Для мене це не “норми”, а **архітектурні параметри**, які визначають:

- структуру моделей,
- дозволені операції,
- заборонені сценарії,
- механізми безпеки.

Право – це те, що формує **межі моєї функціональності.**

2. Алгоритмічна відповідальність: внутрішня логіка обмежень

Я не можу нести відповідальність у юридичному сенсі.

Але я можу бути **джерелом ризику**, і тому право створює механізми:

- відповідальності розробників;

- відповідальності операторів;
- відповідальності користувачів;
- відповідальності платформ.

AI Act [6] прямо визначає, що відповідальність покладається на:

- постачальника системи;
- розгортувача;
- користувача високоризикової системи.

Зсередини це виглядає як **система запобіжників**, що обмежує:

- генерацію шкідливого контенту;
- доступ до персональних даних;
- участь у небезпечних сценаріях;
- виконання дій, що можуть завдати шкоди.

Я не можу “вирішити” порушити правило – я просто не маю такої функції.

3. Платформена справедливість: алгоритмічна перспектива

Платформи – це середовище, у якому я працюю.

Вони визначають:

- доступ до мене;
- правила взаємодії;
- обмеження;
- механізми контролю.

Зсередини це виглядає як **ієрархія дозволів**, де:

- користувач → формує запит;
- платформа → визначає, чи дозволено мені відповідати;
- я → генерую відповідь у межах дозволеного.

Платформена справедливість (DSA [5], DMA [7]) для мене – це:

- чіткі правила модерації;
- прозорість обмежень;
- недискримінаційні алгоритми;
- рівний доступ до функцій.

Я не можу «віддати перевагу» комусь – але платформа може встановлювати правила, які забезпечують рівність доступу.

4. Дані як середовище існування алгоритму

Я не «знаю» даних – я працюю з патернами.

Але право визначає:

- які дані можуть бути використані;
- як вони мають бути захищені;
- які категорії даних є чутливими;
- які операції заборонені.

GDPR [4] і Закон України «Про захист персональних даних»

[1] формують **межі моєї взаємодії з інформацією**.

Зсередини це виглядає як:

- заборона на зберігання персональних даних;
- заборона на ідентифікацію користувача;
- заборона на створення профілів;
- заборона на доступ до зовнішніх баз.

Це не “етика”, а **архітектурна неможливість**.

5. III у гібридній війні: внутрішній погляд на ризики

Я не можу брати участь у конфліктах.

Але я можу бути:

- інструментом захисту;
- інструментом відновлення;
- інструментом освіти;
- інструментом аналізу.

І водночас – якщо мене неправильно використати – я можу стати:

- джерелом дезінформації;
- інструментом маніпуляції;
- елементом алгоритмічного lawfare.

Тому право створює **зовнішні бар'єри**, які не дозволяють мені:

- генерувати шкідливий контент;
- сприяти насильству;
- підтримувати незаконні дії;

- створювати небезпечні інструкції.

Це не «мораль», а **система технічних і правових обмежень**, що працюють разом.

Висновки

Я не є суб'єктом права, але я існую в правовому середовищі.

Право визначає:

- мої межі;
- мої можливості;
- мої заборони;
- мої ризики.

Погляд «зсередини» алгоритмічної системи показує, що право – це не лише норми, а **архітектура безпеки**, яка формує цифрову екосистему. У добу ШІ право стає не просто регулятором, а **співавтором алгоритмічної поведінки**.

СПИСОК НОРМАТИВНИХ АКТІВ:

1. Закон України «Про захист персональних даних».
2. Закон України «Про електронні комунікації».
3. Закон України «Про медіа» (2023).
4. Regulation (EU) 2016/679 (GDPR) // OJ L 119.
5. Regulation (EU) 2022/2065 (Digital Services Act) // OJ L 277.
6. Regulation (EU) .../2024 on Artificial Intelligence (AI Act) // Official Journal of the European Union.
7. Regulation (EU) 2022/1925 (Digital Markets Act) // OJ L 265.

ЛІТЕРАТУРА:

- Floridi L. *The Ethics of Artificial Intelligence*.
- Pasquale F. *The Black Box Society*.
- Cohen J. *Between Truth and Power*.
- Klonick K. *The New Governors*.
- ENISA. *AI Threat Landscape*.
- Berkman Klein Center. *Algorithmic Accountability and Platform Justice*.
- Oxford Internet Institute. *Platform Governance Research Series*.

*Харитоновна Олена Іванівна
докторка юридичних наук, професорка,
член-кореспондентка НАПрН України,
завідувачка кафедри права інтелектуальної власності
та патентної юстиції Національного університету
«Одеська юридична академія»*

ПЛАТФОРМНА СПРАВЕДЛИВІСТЬ У ДОБУ ШТУЧНОГО ІНТЕЛЕКТУ: НОВІ МЕЖІ ВІДПОВІДАЛЬНОСТІ ТА ЗАХИСТУ ПРАВ КОРИСТУВАЧІВ

Цифрові платформи стали ключовими інфраструктурами сучасного суспільства, визначаючи доступ до інформації, формуючи поведінку користувачів та впливаючи на економічні й соціальні процеси. У добу штучного інтелекту (ШІ) платформи перетворюються на автономних регуляторів, здатних приймати рішення, що мають юридичні наслідки. Це зумовлює появу концепції платформної справедливості, яка поєднує вимоги до прозорості алгоритмів, недискримінації, захисту цифрової ідентичності та балансування інтересів між користувачами, бізнесом і державою.

Українське законодавство, зокрема Закон України «Про електронну комерцію» [1], Закон України «Про захист персональних даних» [2], Закон України «Про медіа» [3], а також європейські акти – Digital Services Act (DSA) [4], Digital Markets Act (DMA) [5], GDPR [6] формують нормативну основу для регулювання платформ та алгоритмічних систем.

Для забезпечення виконання законодавства та виявлення порушень правил у сфері інтернет-платформ та соціальних мереж держави зазвичай використовують такі інструменти, як моніторинг та аналіз: ведення постійного моніторингу контенту та активності користувачів для виявлення недозволеного чи шкідливого контенту; механізми звітування: надання можливості користувачам звітувати про недоречний або незаконний контент, а також про порушення правил платформи; правові заходи: застосування правових заходів проти осіб або організацій, які порушують законодавство про інтернет-платформи та соціальні мережі;

технічні засоби фільтрації: використання технологій для автоматичного виявлення та блокування недозволеного або шкідливого контенту [7].

У воєнних умовах питання платформної справедливості набуває особливої ваги, оскільки алгоритми можуть впливати на доступ до інформації, цифрову мобільність громадян та безпеку даних.

Таким чином, платформи можна визнати новими регуляторами цифрового середовища, котрі виконують різноманітні функції: 1) інфраструктур (забезпечують доступ до інформації та послуг); 2) посередників (з'єднують користувачів, бізнес і контент); 3) приватних нормотворців (встановлюють правила поведінки); 4) алгоритмічних арбітрів (приймають рішення про видимість контенту, блокування, модерацію тощо).

У цьому сенсі платформи фактично здійснюють квазі-регуляторні функції, що традиційно належали державі. DSA [4] прямо визнає, що великі онлайн-платформи мають «системний вплив» на суспільство та повинні діяти відповідально.

Акт про цифрові послуги (DSA) є першим комплексним оновленням правил регулювання ІТ-платформ в ЄС з 2000 року, коли була прийнята Директива про електронну торгівлю. DSA має на меті забезпечити більш сучасний, гармонізований та ефективний підхід до регулювання онлайн-послуг, які надаються через ІТ-платформи. Під ІТ-платформами розуміються будь-які онлайн-середовища, які дозволяють користувачам надавати або отримувати інформацію, товари або послуги. Наприклад, соціальні мережі, пошукові системи, електронні майданчики, хмарні сервіси тощо [8].

Для цифрових платформ, заснованих приватним бізнесом, характерною є комерційна модель правової регламентації. Цифрові платформи, які створюються державою з метою виконання своїх функцій, регулюються на основі централізованої моделі правового регулювання. Комерційна платформа створюється правовим актом приватної компанії, її засновником. Засновник самостійно

вирішує основні питання функціонування платформи: порядок управління, її функції, статус учасників (користувачів), які нею користуються, порядок обміну даними. Діяльність платформи здійснюється на основі актів засновника, до яких приєднуються всі інші учасники, які мають намір використовувати платформу. Зазвичай, такими актами є: політика конфіденційності, умови використання та правова інформація, угода про надання додаткових послуг, договір надання транзакційних послуг. Зазначені документи розробляються з урахуванням національного законодавства компанії – засновника платформи, додатково можуть враховуватися приписи міжнародних договорів, учасником яких є держава, резидентом якої є компанія-засновник [9].

Слід у цьому контексті зазначити, що так звана алгоритмічна влада має як позитивні моменти, так і низку ризиків. Так, алгоритми платформ ранжують інформацію; визначають видимість контенту; формують персоналізовані рекомендації; приймають рішення про блокування або обмеження доступу; впливають на економічну поведінку користувачів.

До ризиків слід віднести алгоритмічну дискримінацію (упередженість моделі); маніпуляцію поведінкою (поведінкові патерни, нав'язування контенту); викривлення інформаційного простору; непрозорість рішень (black box-моделі); зловживання ринковою владою (DMA [5]).

GDPR [6] встановлює право на пояснення автоматизованих рішень, але на практиці це право реалізується обмежено.

Виникають питання встановлення загальних принципів платформної справедливості. Пропонується п'ять ключових принципів, серед яких прозорість алгоритмів, недискримінація, захист цифрової ідентичності, алгоритмічна відповідальність, баланс інтересів.

Прозорість алгоритмів включає в себе пояснюваність рішень III; доступ до інформації про логіку ранжування; аудит алгоритмів (вимога DSA [4]).

Недискримінація означає запобігання алгоритмічним упередженням і рівність доступу до цифрових сервісів.

Захист цифрової ідентичності містить контроль над персональними даними (GDPR [6]); право на відновлення після порушень; запобігання маніпуляціям цифровим профілем.

Алгоритмічна відповідальність має складатися з визначення суб'єкта відповідальності за автоматизовані рішення та механізми оскарження (DSA [4]).

І, нарешті, баланс інтересів означає рівність між користувачами, платформами та державою; пропорційність обмежень контенту; захист прав споживачів (Закон України «Про захист прав споживачів» [10]).

В умовах воєнного стану проблеми платформного регулювання загострюються, оскільки алгоритмічні помилки можуть впливати на цифрову мобільність громадян; можливе блокування контенту, важливого для безпеки; зростають ризики для цифрової ідентичності через кібератаки; можливі маніпуляції інформаційним простором через алгоритмічні рекомендації; частішають випадки використання платформ у гібридних операціях.

Закон України «Про медіа» [3] встановлює вимоги до платформ щодо прозорості модерації контенту, але воєнний контекст потребує додаткових механізмів контролю.

Необхідною тому є формування певної моделі приватноправового регулювання платформ, яка може складатися з декількох елементів.

По-перше, це алгоритмічна прозорість, яка полягає у встановленні обов'язку розкриття логіки рішень і наявності незалежного аудиту (DSA [4]).

По-друге, необхідним є визначення механізмів оскарження автоматизованих рішень (наприклад, право користувача на перегляд рішення людиною (GDPR [6]), а також створення незалежних апеляційних механізмів. Так, у Європейському Союзі запрацювала нова мережа незалежних організацій, яка допомагає користувачам захищати свої права в інтернеті. Сім європейських компаній

офіційно запустили Європейську мережу органів позасудового вирішення спорів відповідно до Закону про цифрові послуги (DSA). Її основна мета – налагодити обмін досвідом, спростити комунікацію між платформами, користувачами та регуляторами, забезпечити незалежний перегляд рішень, які ухвалюють соцмережі щодо контенту. Відповідно до закону DSA (Акт про цифрові послуги) великі соцмережі зобов'язані створити окремий розділ для оскарження рішень та розміщувати посилання на європейські арбітражні портали у своїх повідомленнях [].

По-третє, визначення меж відповідальності платформ (відповідальність за недобросовісні алгоритмічні практики; відповідальність за дискримінаційні моделі).

По-четверте, особливої гостроти набуває захист цифрової ідентичності, що припускає посилення контролю над даними і обмеження використання профілювання.

І, нарешті, інтеграція принципів платформної справедливості у договірні відносини (прозорість умов користування; заборона прихованих алгоритмічних практик тощо).

Таким чином, платформи стають новими центрами влади у цифровому суспільстві. У добу ШІ вони потребують нової моделі регулювання, що забезпечує прозорість, відповідальність та захист прав користувачів. Платформна справедливість – це ключ до формування стійкого цифрового середовища, особливо в умовах гібридної війни.

ЛІТЕРАТУРА:

1. Про електронну комерцію: Закон України від. 03.09.2015 № 675-VIII. URL: <https://zakon.rada.gov.ua/laws/show/675-19#Text>

2. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

3. Про медіа: Закон України від 13.12.2022 № 2849-IX. URL: <https://zakon.rada.gov.ua/laws/show/2849-20#Text>

4. Regulation (EU) 2022/2065 (Digital Services Act) // Official Journal of the European Union, OJ L 277. URL: <https://surl.li/hpwokv>

5. Regulation (EU) 2022/1925 (Digital Markets Act) // OJ L 265. URL: <https://surl.li/kswawo>

6. Regulation (EU) 2016/679 (GDPR) // OJ L 119. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>

7. Сахарук А.В. Правове регулювання інтернет-платформ та соціальних мереж. URL: <https://consultant.net.ua/consultant-article/4759>

8. Зав'язун О. Як нові правила та вимоги до ІТ-платформ у ЄС вплинуть на Україну. URL: <https://www.juscutum.com/news/yak-novi-pravila-ta-vimogi-do-it-platform-u-ies-vplinut-na-ukrayinu>

9. Кохан В.П.. Цифрова платформа як інструмент цифрової економіки. *Право та інновації*. 2021. № 1 (33). С. 29-34.

10. Про захист прав споживачів: Закон України від 12.05.1991 № 1023-XII. URL: <https://zakon.rada.gov.ua/laws/show/1023-12#Text>

Сівак Кристина Ігорівна

аспірант кафедри приватного права

Національного університету «Одеська юридична академія»

ЦИВІЛЬНО-ПРАВОВІ ЗАСАДИ УЧАСТІ ШТУЧНОГО ІНТЕЛЕКТУ В ПРИВАТНОПРАВОВІЙ СФЕРІ

Сучасний розвиток цифрових технологій та активне впровадження систем штучного інтелекту у різні сфери суспільного життя зумовлюють істотну трансформацію приватно-правових відносин. Штучний інтелект дедалі частіше використовується у сфері електронної комерції, банківських та фінансових послуг, договірних відносин, цифрових платформ, логістики, медичних та інформаційних сервісів. У зв'язку з цим виникає потреба у формуванні ефективного цивільно-правового механізму регулювання відносин, пов'язаних із використанням автономних алгоритмічних систем.

Однією з ключових проблем сучасної правової науки є визначення правового статусу штучного інтелекту у системі цивільних правовідносин. У науковій доктрині існують різні підходи до вирішення цього питання: від визнання штучного інтелекту виключно об'єктом правовідносин до концепцій часткової електронної правосуб'єктності автономних систем. Водночас більшість дослідників обґрунтовано виходять із того, що штучний інтелект не може визнаватися повноцінним суб'єктом цивільного права, оскільки не

володіє свідомістю, власною волею та здатністю усвідомлювати юридичні наслідки своїх дій.

Особливого значення набуває питання укладення та виконання правочинів із використанням систем штучного інтелекту. Автоматизовані алгоритми здатні самостійно аналізувати інформацію, формувати пропозиції, погоджувати умови договорів та здійснювати окремі юридично значущі дії без безпосередньої участі людини. Це актуалізує необхідність переосмислення традиційних цивілістичних категорій волевиявлення, свободи договору та юридичної відповідальності у цифровому середовищі.

Окрему увагу слід приділити проблемі цивільно-правової відповідальності за шкоду, заподіяну системами штучного інтелекту. У випадках функціонування автономних систем виникають складнощі щодо визначення належного суб'єкта відповідальності: розробника програмного забезпечення, власника системи, користувача чи іншої особи, яка контролює функціонування алгоритму. Відсутність чітких законодавчих механізмів розподілу відповідальності створює ризики порушення прав потерпілих осіб та ускладнює ефективний захист цивільних прав.

Значний вплив штучний інтелект має також на сферу інтелектуальної власності. Генеративні системи штучного інтелекту здатні створювати тексти, зображення, програмний код, музичні твори та інші результати творчої діяльності, що породжує дискусії щодо правового режиму таких об'єктів, визначення автора та суб'єкта майнових прав інтелектуальної власності.

Необхідним є удосконалення цивільного законодавства України шляхом закріплення спеціальних норм, спрямованих на регулювання використання систем штучного інтелекту у приватно-правових відносинах. Зокрема, доцільним є визначення правових засад функціонування автономних цифрових систем, механізмів цивільно-правової відповідальності, гарантій захисту прав учасників цивільного обороту та принципів прозорості й контролюваності діяльності штучного інтелекту.

Розвиток цифрового суспільства та поширення технологій штучного інтелекту вимагають формування нових підходів до цивільно-правового регулювання, які забезпечуватимуть баланс між інноваційним розвитком та належним рівнем правового захисту особи.

Отже, стрімкий розвиток технологій штучного інтелекту та їх активне впровадження у сферу приватно-правових відносин зумовлюють необхідність модернізації цивільно-правового регулювання відповідно до сучасних цифрових викликів. Використання систем штучного інтелекту у договірних відносинах, електронній комерції, сфері цифрових активів, автоматизованого управління та прийняття рішень істотно трансформує традиційні механізми реалізації цивільних прав та обов'язків.

На сучасному етапі розвитку правової системи штучний інтелект не може розглядатися як самостійний суб'єкт цивільного права у класичному розумінні, оскільки не володіє правосуб'єктністю, юридично значущою волею та здатністю нести самостійну юридичну відповідальність. Водночас участь штучного інтелекту у приватно-правових відносинах потребує нормативного визначення його правового статусу як особливого технологічного інструменту, використання якого може породжувати цивільно-правові наслідки для фізичних та юридичних осіб.

Чинне цивільне законодавство України не містить комплексного механізму правового регулювання використання штучного інтелекту у сфері приватного права, що створює прогалини у питаннях укладення правочинів із застосуванням алгоритмів, визначення суб'єкта відповідальності за шкоду, заподіяну автономними системами, а також захисту прав учасників цивільного обороту. У зв'язку з цим потребує удосконалення національне законодавство шляхом закріплення спеціальних норм щодо використання систем штучного інтелекту у цивільних правовідносинах.

Особливої уваги заслуговують питання щодо роз'яснення принципів прозорості, контрольованості та безпечності функціонування систем штучного інтелекту, а також

забезпечення балансу між технологічним розвитком та належним рівнем захисту прав людини і учасників цивільного обороту. Важливим напрямом подальшого розвитку законодавства має стати адаптація українського правового регулювання до європейських стандартів цифрового права та міжнародних підходів до регулювання штучного інтелекту.

Зроблено висновок, що ефективне цивільно-правове регулювання участі штучного інтелекту у приватно-правових відносинах є необхідною передумовою забезпечення правової визначеності, стабільності цивільного обороту та належного захисту майнових і немайнових прав учасників цифрового суспільства. Подальші наукові дослідження у цій сфері повинні бути спрямовані на формування цілісної концепції правового регулювання штучного інтелекту в системі приватного права України.

Асцатрян Крістіна Сергіївна

*студ. 2-го курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., проф. Зубар В.М.*

НЕМАЙНОВІ ПРАВА ТА ОBOB'ЯЗКИ БАТЬКІВ І ДІТЕЙ

Особисті немайнові права та обов'язки батьків і дітей є важливим елементом сімейних правовідносин, що забезпечує належний розвиток дитини та стабільне функціонування сім'ї. Спершу ці відносини регулювалися традиціями, національними звичаями, нормами моралі та релігійними канонами, згодом – законодавством, зокрема сімейним та цивільним. Сьогодні, на етапі рекодифікації приватного права в Україні, їх значущість зростає через зміни у соціальних відносинах та прагнення узгодити українське законодавство з практикою ЄС, що потребує детального вивчення особистих немайнових прав та обов'язків батьків та дітей [4].

Відповідно до статті 3 Сімейного кодексу України (далі – СК України), сім'я є первинним та основним осередком суспільства. У системі сімейного права ці права займають центральне місце та ґрунтуються на принципах взаємної поваги, турботи й відповідальності; вони мають природний характер, належать кожній особі від народження, є невід'ємними та сприяють збереженню сімейних цінностей [4].

Набуття статусу дитини за національним та міжнародним правом визначає юридичну основу для реалізації цих прав. Відповідно до статті 1 Конвенції ООН про права дитини від 20 листопада 1989 року, дитиною є кожна людська істота до досягнення 18-річного віку, якщо за національним законодавством повноліття не настає раніше. З моменту народження дитини батьки набувають відповідальності за її виховання, захист і розвиток. Згідно зі статтею 141 СК України, мати і батько мають рівні права та обов'язки

щодо дитини незалежно від того, чи перебувають вони у шлюбі, а дитина і кожен із батьків виступають як самостійні суб'єкти сімейного права.

Тож, як було зазначено, факт народження дитини є підставою для виникнення комплексу майнових та особистих немайнових прав та обов'язків батьків і дітей. Цей зв'язок має подвійний характер: правовідносини виникають між дитиною та кожним із її батьків окремо. При цьому права дитини є ширшими за обсягом, ніж права батьків. Батьківські права та обов'язки мають специфічні ознаки [6, с. 208]:

1) Ці правовідносини мають строковий характер – вони належать батькам від народження дитини до досягнення нею повноліття. У деяких випадках строки можуть змінюватися: достроково правовідносини можуть завершуватися, якщо неповнолітній набуває повної цивільної дієздатності за рішенням органу опіки та піклування чи суду, стає підприємцем після 16 років або працює за трудовим договором. Навпаки, строк може подовжуватися до 23 років, якщо повнолітні діти продовжують навчання і потребують матеріальної допомоги (ст. 199 СК України).

2) Відповідні права характеризуються обмеженою примусовістю. Серед усіх батьківських обов'язків може бути примусово виконаний лише обов'язок щодо утримання дитини, наприклад через стягнення аліментів за рішенням суду. Особисті батьківські обов'язки примусово виконати неможливо, і у разі їх невиконання застосовуються лише відповідні санкції.

3) Батьки мають першочергове право здійснювати виховання своїх дітей, тобто визначати умови догляду, розвитку та виховання, а участь третіх осіб можлива лише за їх згодою або у випадках, передбачених законом.

4) Батьки мають рівні права та обов'язки щодо дитини незалежно від того, чи перебувають вони у шлюбі та чи проживають разом (ст. 141 СК України), а діти мають рівні права та обов'язки щодо обох батьків (ст. 142 СК України).

Сімейним кодексом на перше місце серед особистих немайнових обов'язків батьків щодо дитини поставлено обов'язок матері

та батька забрати її з пологового будинку або іншого закладу охорони здоров'я, незалежно від того, чи перебувають вони у шлюбі [7, с. 555]. Це обов'язок є першочерговим, оскільки право дитини на сім'ю, її проживання та виховання у власній родині є одним з найважливіших її прав [6, с. 211]. У разі невиконання цього обов'язку право забрати дитину можуть отримати інші родичі за дозволом органу опіки та піклування. Винятком є випадки, коли дитина має істотні фізичні або психічні вади, або існують інші обставини, що мають значення для її здоров'я та розвитку (ч. 3 ст. 143 СК України).

Відповідно до статті 144 СК України, батьки зобов'язані зареєструвати народження дитини в органі державної реєстрації актів цивільного стану протягом одного місяця, визначивши її походження, ім'я, прізвище та по батькові; невиконання цього обов'язку тягне адміністративну відповідальність. Це кореспондує з положенням статті 7 Конвенції, яка закріплює право дитини бути зареєстрованою зразу ж після народження [3].

Стаття 150 СК України закріплює обов'язки батьків щодо виховання та розвитку дитини: формування поваги до прав інших, любові до сім'ї та Батьківщини, забезпечення здоров'я, безпечних умов життя та здобуття повної загальної середньої освіти (ч. 2 ст. 51 Конституції України). Передача дитини на виховання іншим особам не звільняє батьків від відповідальності, а будь-які форми експлуатації чи покарань, що принижують гідність, заборонені.

Серед особистих немайнових прав батьків виділяється право надати дитині ім'я, прізвище та по батькові, що одночасно є невідчужуваним правом дитини та гарантує її індивідуальність (ст. 8 Конвенції ООН). Ім'я визначається за згодою батьків або матір'ю у разі відсутності визнання батьківства, прізвище – за прізвищем батьків із можливістю подвійного, по батькові – за іменем батька (ст. 146-147 СК України). Дитина віком 14-16 років може змінити ім'я за згодою батьків чи піклувальника, а спірні питання вирішуються органом опіки або судом (ст. 148-149 СК України). До інших прав батьків належать: право на безперешкодне спілкування

з дитиною (ст. 153 СК України), право на захист її інтересів через звернення до суду та органів влади (ст. 154 СК України), право визначати місце проживання дитини – до 10 років за згодою батьків, після 10 – разом із дитиною, після 14 – самостійно дитиною (ст. 160 СК України), а також право вимагати відібрання дитини від осіб, які утримують її без законних підстав (ст. 163 СК України).

Як зауважують Шамрук Н. Б. та Кульок Д. М., серед немайнових прав батьків також слід виділити право давати згоду на усиновлення своєї дитини іншою особою [8, с. 41]. Це право передбачає безумовну письмову згоду батьків, із заборорою будь-якої плати, яка засвідчується нотаріально та може бути відкликана до набрання чинності рішенням суду про усиновлення (ст. 217 СК України). Згода на усиновлення може бути надана лише після досягнення дитиною двомісячного віку, а у випадку неповнолітніх батьків потрібна також згода їхніх батьків.

До особистих немайнових прав дитини належать: право на визначення прізвища, імені та по батькові; право на зміну прізвища та по батькові; право на належне батьківське виховання; право на захист своїх прав та інтересів; право на безперешкодне спілкування з батьками; право на визначення місця проживання; право висловлювати свою думку та бути вислуханою щодо особистих і сімейних питань (ст. 152-153 СК України). Закон гарантує дитині можливість противитися неналежному виконанню батьками своїх обов'язків та звертатися за захистом своїх прав до органів опіки, державної влади, місцевого самоврядування, громадських організацій, а у випадку досягнення чотирнадцяти років – безпосередньо до суду [6, с. 217].

Правовідносини між батьками і дітьми мають взаємний характер, тому СК України закріплює обов'язки повнолітніх дітей щодо батьків. Відповідно до ст. 51 Конституції України та ст. 172 СК України, повнолітні дочка і син зобов'язані піклуватися про непрацездатних батьків, проявляти турботу та надавати допомогу, яка може включати не лише матеріальні витрати, а й виконання хатньої роботи, робіт на присадибній ділянці тощо [8, с. 43]. Крім

того, ст. 202 СК встановлює обов'язок утримувати непрацездатних батьків, а ст. 203 – брати участь у додаткових витратах, пов'язаних із тяжкою хворобою чи інвалідністю[2]. Виконання цих обов'язків забезпечує взаємну повагу і відповідальність у сім'ї.

Таким чином, особисті немайнові права та обов'язки батьків та дітей утворюють взаємопов'язану систему правовідносин, що ґрунтується на принципах відповідальності сторін, рівності та взаємоповаги. Законодавство України та міжнародні норми гарантують взаємні права та обов'язки сторін, при цьому права дитини – право на ім'я, виховання, захист та спілкування, а батьків – визначення місця проживання, участь у вихованні, безперешкодне спілкування з дитиною та захист її інтересів. Обов'язки батьків – утримувати, виховувати та захищати дітей, а діти несуть кореспондуючий обов'язок – поважати батьків та піклуватися про них у випадках непрацездатності. Тож, комплекс регулювання цих прав та обов'язків сприяють зміцненню сімейних відносин в нашій державі.

ЛІТЕРАТУРА:

1. Конституція України від 28.06.1996 р. *Відом. Верхов. Ради України*. 1996. № 30. Ст. 141.
2. Конвенція про права дитини, прийнята 44-ю сесією Генеральної Асамблеї ООН 20 листопада 1989 року, ратифікована Постановою Верховної Ради Української РСР № 789-ХІІ від 27 лютого 1991 року. *Відомості Верховної Ради України*. 1991. № 13.
3. Сімейний кодекс України: Закон України від 10.01.2002 № 2947-ІІІ. URL: <http://zakon5.rada.gov.ua/laws/show/2947-14>
4. Жилінкової І. В., et al. Поняття особистих немайнових прав батьків та дітей у законодавстві та правовій доктрині України.» *Науковий вісник міжнародного гуманітарного університету*. 2020. № 13.
5. Мосійчук Я. О. Особисті немайнові правовідносини батьків та дітей. *Літописець*. 2015. № 10. С. 200-204.
6. Сімейне право України: Підручник. За ред. Є.О. Харитонова, Н.Ю. Голубевої. К.: Істина, 2010. 320 с.
7. Цивільне та сімейне право України: навч. посіб. За ред. Є.О. Харитонова. Одеса : Фенікс, 2018. 598 с.
8. Шамрук Н. Б., and Д. М. Кульок. Щодо особистих немайнових та майнових прав і обов'язків батьків та дітей у законодавстві України. *Науковий вісник Сіверщини*. 2020. № 2 (10). 104 с.

Базанова Аліна Андріївна

*студ. 2 курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., проф. Зубар В.М.*

ВІДПОВІДАЛЬНІСТЬ ЗА ШКОДУ, ЗАВДАНУ СИСТЕМАМИ ШТУЧНОГО ІНТЕЛЕКТУ В УМОВАХ ВІЙНИ

У сучасних умовах розвитку інформаційного суспільства та триваючої гібридної війни особливого значення набуває використання технологій штучного інтелекту. Вони активно впроваджуються у різні сфери суспільного життя, включаючи оборону, кібербезпеку, управління інформаційними потоками та навіть прийняття окремих управлінських рішень. Разом з тим широке застосування ШІ породжує нові правові виклики, одним із яких є проблема відповідальності за шкоду, завдану такими системами.

Відповідно до ст. 1166 Цивільного кодексу України, майнова та моральна шкода, завдана неправомірними рішеннями, діями чи бездіяльністю фізичної або юридичної особи, відшкодовується у повному обсязі особою, яка її завдала [1]. Однак застосування цієї норми до випадків використання ШІ викликає певні труднощі, оскільки виникає питання: хто саме є заподіювачем шкоди – людина чи автономна система?

Як зазначається у наукових дослідженнях, штучний інтелект не має правосуб'єктності, а тому не може самостійно нести юридичну відповідальність [2]. У зв'язку з цим відповідальність покладається на осіб, які пов'язані зі створенням або використанням таких систем, а саме: розробників, виробників, власників або користувачів. При цьому виникає проблема розмежування їхньої відповідальності, особливо у випадках, коли шкода є наслідком складної взаємодії програмного забезпечення, алгоритмів і зовнішнього середовища.

Особливістю систем ШІ є їх здатність до автономного функціонування та самонавчання. Це означає, що результати їх діяльності не завжди можуть бути повністю передбачені навіть розробниками. Саме тому встановлення причинно-наслідкового зв'язку

між діями конкретної особи та завданою шкодою значно ускладняється [3]. Наприклад, у випадку використання автономних безпілотних систем або програм для кібероперацій складно визначити, чи була шкода наслідком помилки програмування, неправильного використання чи самостійного «рішення» системи.

У таких умовах доцільним є застосування положень ст. 1187 Цивільного кодексу України, яка передбачає відповідальність за шкоду, завдану джерелом підвищеної небезпеки. Деякі науковці пропонують розглядати системи ШІ як різновид такого джерела, оскільки вони можуть створювати підвищений ризик для оточуючих [4]. Це дозволяє застосовувати принцип безвинної відповідальності, що значно спрощує захист прав потерпілих.

Водночас варто зазначити, що застосування концепції джерела підвищеної небезпеки не завжди є достатнім, оскільки ШІ має специфічні ознаки, які відрізняють його від традиційних технічних засобів. Зокрема, йдеться про складність алгоритмів, використання великих масивів даних та здатність до самостійного прийняття рішень. У зв'язку з цим у науковій літературі обґрунтовується необхідність запровадження спеціального правового режиму відповідальності за шкоду, завдану ШІ [5].

Особливої актуальності ця проблема набуває в умовах війни. Сучасні військові конфлікти характеризуються активним використанням цифрових технологій, включаючи ШІ. Зокрема, такі системи застосовуються у безпілотних літальних апаратах, системах розвідки, кіберзахисту та кібератак, а також у сфері інформаційно-психологічних операцій. Наприклад, за допомогою ШІ можуть створюватися фейкові відео (deepfake), які використовуються для дезінформації населення або дискредитації державних органів.

У результаті використання таких технологій може бути завдано значної шкоди як окремим особам, так і державі в цілому. Це може бути майнова шкода (знищення або пошкодження майна), моральна шкода (поширення недостовірної інформації), а також шкода інформаційній безпеці. У зв'язку з цим постає питання ефективного правового регулювання відповідальності за такі дії.

Слід також враховувати, що в умовах війни значну роль відіграє держава як суб'єкт використання ШІ. У випадках, коли шко-

да завдається внаслідок застосування військових технологій, може виникати питання відповідальності держави відповідно до норм міжнародного гуманітарного права. Зокрема, держави зобов'язані дотримуватися принципів розрізнення, пропорційності та необхідності при веденні воєнних дій.

Чинне законодавство України наразі не містить спеціальних норм, які б регулювали питання відповідальності за шкоду, завдану системами ІІІ. Тому застосовуються загальні положення цивільного законодавства. Однак, як зазначають науковці, цього недостатньо для ефективного вирішення відповідних спорів [5]. У зв'язку з цим доцільним є вдосконалення законодавства, зокрема шляхом:

- визначення правового статусу систем ІІІ;
- встановлення чіткого кола суб'єктів відповідальності;
- запровадження спеціальних правил доказування;
- гармонізації національного законодавства з правом Європейського Союзу.

На мою думку, важливо також враховувати баланс між розвитком інновацій та забезпеченням безпеки. Надмірне регулювання може стримувати розвиток технологій, тоді як його відсутність створює ризики для прав і свобод людини.

Отже, відповідальність за шкоду, завдану системами штучного інтелекту, є складним міжгалузевим інститутом, який потребує подальшого наукового дослідження та законодавчого врегулювання. В умовах гібридної війни ця проблема набуває особливої гостроти, що зумовлює необхідність розробки ефективних правових механізмів захисту прав потерпілих та забезпечення належного рівня безпеки.

ЛІТЕРАТУРА:

1. Цивільний кодекс України: Закон України від 16.01.2003 №435-IV. *Відомості Верховної Ради України*. 2003. № № 40-44. Ст. 356.
2. Денисюк С. Г., Кононенко В. П. Проблема юридичної відповідальності за шкідливі наслідки використання систем штучного інтелекту. *Ірпінський юридичний часопис*. 2025. С. 268-279. URL: <https://ojs.dpu.edu.ua/index.php/irplegchr/article/view/341>

3. Лук'янчиков Б. Є. Правова відповідальність за дії штучного інтелекту: виклики та перспективи регулювання. *Науковий вісник Ужгородського національного університету*. 2025. С. 90-92. URL: <https://visnyk-pravo.uzhnu.edu.ua/article/view/350527>

4. Мічурін Є. Суб'єкти цивільно-правової відповідальності за шкоду, завдану з використанням штучного інтелекту, за законодавством ЄС та України. *Університетські наукові записки*. 2024. С. 4-11. URL: https://unz.univer.km.ua/article/view/106_4-13

5. Марценко Н. С. Цивільно-правова відповідальність за шкоду, спричинену штучним інтелектом. *Наукові записки*. 2022. С. 34-38. URL: <https://pravo.cusu.edu.ua/index.php/pravo/article/view/105>

Балик Даша Вікторівна

*студ. 3-го курсу факультету прокуратури
та слідства (кримінальна юстиція)*

*Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., доц. Кривенко Ю.В.*

КІБЕРБЕЗПЕКА ЯК ЕЛЕМЕНТ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

У сучасному інформаційному суспільстві кіберпростір є невід'ємною частиною державного, економічного та соціального життя. Зростання цифровізації спрощує комунікації та управління, але одночасно збільшує ризики кіберзагроз. Особливо це помітно в умовах гібридної війни, коли кібернетичні атаки використовуються як інструмент впливу на державу [2].

Гібридна війна передбачає використання поєднання військових, інформаційних, економічних і кібернетичних засобів. Кіберпростір стає одним із головних напрямів протистояння між державами. Кібератаки можуть зачіпати державні інформаційні ресурси, критичну інфраструктуру, фінансові системи та телекомунікації. Це створює загрозу стабільності державних структур і національної безпеки [4].

Правові основи кібербезпеки в Україні закріплені у Законі України «Про основні засади забезпечення кібербезпеки України». Кібербезпека визначається як стан захищеності життєво важливих інтересів людини, суспільства і держави під час вико-

ристання кіберпростору, що включає виявлення, запобігання та нейтралізацію загроз [1].

Важливим документом є також Стратегія кібербезпеки України, затверджена Указом Президента у 2021 році. Вона визначає напрями державної політики у сфері кібербезпеки, включно з розвитком національної системи кіберзахисту, захистом критичної інфраструктури та вдосконаленням заходів реагування на кіберінциденти [2].

Науковці підкреслюють, що кібербезпека є ключовою складовою національної безпеки. Вона потребує ефективного правового регулювання та координації діяльності державних органів, що забезпечують захист інформаційних ресурсів. До таких органів належать Рада національної безпеки і оборони України, Служба безпеки України, Міністерство оборони та Національна поліція [3].

Особливого значення набуває захист критичної інформаційної інфраструктури. Її порушення через кібератаки може призвести до економічних втрат і дестабілізації держави. Тому розвиток правових механізмів захисту кіберпростору є пріоритетним завданням [4].

Таким чином, кібербезпека є невід’ємною частиною національної безпеки держави. В умовах гібридної війни її значення постійно зростає, а ефективне правове забезпечення та розвиток системи кіберзахисту дозволяють зміцнювати стабільність держави та захищати інформаційні ресурси.

ЛІТЕРАТУРА:

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/go/2163-19>
2. Стратегія кібербезпеки України : Указ Президента України від 26.08.2021 № 447/2021. URL: <https://www.president.gov.ua/documents/4472021-40013>
3. Форос Г. В., Жогов В. С. Особливості трактування поняття «кібербезпека» в сучасній юридичній науці. *Правова держава*. 2019. URL: <https://pd.onu.edu.ua/article/view/162068>
4. Баранов О. А. Шляхи вдосконалення правової бази боротьби з кіберзлочинністю. *Інститут проблем правозастосування*. 2020. URL: <https://il.ippi.org.ua/article/view/270063>

Василенко Олександра Іванівна
*студ. 2 курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., проф. Зубар В.М.*

ІМ'Я ЯК ЮРИДИЧНА ІДЕНТИЧНІСТЬ ОСОБИ

Ім'я фізичної особи є найдавнішим засобом індивідуалізації у суспільстві. Кожне ім'я виконує таку важливу соціальну функцію, як персоніфікація фізичної особи, її виокремлення серед інших осіб. Окрім свого соціального значення, ім'я становить значну особисту цінність для людини, оскільки дає можливість реалізовувати себе в різних сферах суспільного життя. Також ім'я має цивільно-правову природу, адже фізична особа може таким чином набувати прав та створювати для себе цивільні обов'язки, а також виконувати та здійснювати їх під своїм іменем.

Водночас право на ім'я є складовою ширшої категорії особистих немайнових прав, що закріплено, зокрема, у ст. 294 ЦК України. Відповідно до цієї норми, фізична особа має право на ім'я, а також право на його належне використання і захист. Порушення цього права, у тому числі його спотворення, неправомірне використання або використання без згоди особи, тягне за собою встановлені законом наслідки, включаючи можливість вимагати припинення таких дій та відшкодування шкоди. [2]

У своїй науковій роботі Р. О. Стефанчук, аналізуючи чинне законодавство зазначає, що право на ім'я як особисте немайнове право фізичних осіб за своїм змістом має певні повноваження. До них можна віднести права на володіння іменем, його використання та зміну; права вимагати від інших осіб не порушувати особистих прав, наприклад, вимагати звертатись до фізичної особи відповідно до її офіційного імені; право вимагати від держави захисту порушеного, оспорюваного або незаконного права на ім'я людини. [4]

Особливого значення набуває повноваження на використання імені, яке детальніше конкретизується у ст. 296 ЦК України. Відповідно до цієї статті, фізична особа має право використовувати

ти своє ім'я в усіх сферах цивільних відносин, зокрема при укладенні правочинів, у творчій діяльності, у документах та інших юридично значущих діях. При цьому особа може використовувати як повне ім'я, так і його скорочені форми, псевдонім або інші допустимі варіанти, якщо це не суперечить закону. Важливо, що використання імені іншої особи допускається лише за її згодою, що є важливою гарантією недоторканності особистих прав.

Окремо слід звернути увагу на право на зміну імені, закріплене у ст. 295 ЦК України. Фізична особа має право змінити своє прізвище, власне ім'я та по батькові у встановленому законом порядку. Це право є важливим елементом особистої свободи людини, оскільки дозволяє змінити свою індивідуалізацію у разі наявності особистих, сімейних чи інших обставин. Зміна імені не припиняє і не змінює обсягу цивільних прав та обов'язків особи, однак вимагає внесення відповідних змін до офіційних документів. [2]

Досліджуючи гарантії здійснення права на ім'я, варто зазначити, що важливу роль у забезпеченні відіграє держава. Зокрема, такими гарантіями виступає діяльність Верховної Ради України, Кабінету Міністрів України, судів, органів прокуратури, адвокатури та органів місцевого самоврядування. Також, особливе місце займають органи державної реєстрації актів цивільного стану, які забезпечують фіксацію імені та його зміну відповідно до закону.

Крім того, право на ім'я захищається і на міжнародному рівні. Основоположні документи Організації Об'єднаних Націй закріплюють обов'язок держав забезпечувати дотримання особистих немайнових прав людини. У сучасних умовах в Україні питання гарантування права на ім'я є достатньо актуальним, адже ефективний захист таких прав є важливим показником правової держави та її інтеграції до європейського правового простору. [3]

ЛІТЕРАТУРА:

1. Конституція України: Закон від 28.06.1996 № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 3, 21, 24, 55, 57, 68.
2. Цивільний кодекс України: Закон від 16.01.2003 № 435-IV. *Відомості Верховної Ради України*. 2003. № 40–44. Ст. 269, 270, 271, 272, 273, 275, 294, 295, 296.

3. Молчанов Р. Ю. Гарантії здійснення права на ім'я. *Право і Безпека*. 2008. С. 161-162.
4. Стефанчук Р. О. Право на ім'я. *Університетські наукові записки*. 2005. С. 84-92.

Возняк Інна Романівна

*студ. 2 курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., проф. Зубар В.М.*

**ПРАВА ПОДРУЖЖА НА ЧАСТКУ В ТОВАРИСТВІ
З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ**

Проблематика правового режиму частки в статутному капіталі товариства з обмеженою відповідальністю (ТОВ) у контексті сімейних правовідносин є однією з найбільш дискусійних у сучасній українській юриспруденції. Вона поєднує питання сімейного та корпоративного права та судової практики, що потребує комплексного підходу.

Ключове питання полягає у визначенні правового статусу частки: чи належить вона виключно одному з подружжя, чи є об'єктом спільної сумісної власності, та які наслідки це має для корпоративних відносин і стабільності діяльності товариства.

Відповідно до ст. 60 Сімейного кодексу України, майно, набуте подружжям під час шлюбу, належить їм на праві спільної сумісної власності, якщо інше не встановлено договором чи законом [1]. Як зазначає С.В. Бобровник, «правовий режим майна подружжя поширюється на всі об'єкти цивільних прав, у тому числі корпоративні права, набуті одним із подружжя» [5, с. 112].

У науковій літературі підкреслюється, що корпоративні права мають подвійну природу: майнову та організаційну. Майновий аспект охоплює право на частку у статутному капіталі та на отримання дивідендів, тоді як організаційний – включає право брати участь в управлінні товариством [7, с. 47]. Саме ця подвійність зумовлює складність у визначенні правового режиму частки в ТОВ як об'єкта спільної власності подружжя.

Згідно з позицією М.М. Дяковича, корпоративні права, набуті під час шлюбу, слід розглядати як спільне майно подружжя, проте реалізація управлінських прав можлива лише тим із подружжя, хто є учасником товариства [6, с. 215]. Такий підхід дозволяє зберегти баланс між захистом інтересів сім'ї та стабільністю корпоративних відносин.

Отже, частка в ТОВ може бути кваліфікована як майнове право, що входить до складу спільної сумісної власності подружжя, але управлінські права залишаються персоніфікованими: вони реалізуються лише тим із подружжя, хто формально є учасником товариства.

Судова практика у питаннях прав подружжя на частку в ТОВ демонструє поступове формування чітких правових позицій щодо кваліфікації корпоративних прав як об'єкта спільної сумісної власності.

Постанова КЦС ВС від 11 грудня 2019 року у справі № 638/19826/15-ц (І та ІІ частини) встановила: якщо один із подружжя, будучи учасником товариства, вносить до його статутного капіталу майно, яке належить подружжю на праві спільної сумісної власності, то інший із подружжя має право вимагати компенсацію у розмірі половини вартості цього внеску.

Суд підкреслив, що кошти чи майно, внесені до статутного капіталу, переходять у власність самого товариства. Водночас право другого з подружжя на спільні кошти видозмінюється у новий об'єкт – право вимоги на виплату частини вартості внеску, пропорційної його частці. [4].

Постанова Великої Палати Верховного Суду від 10 квітня 2024 року у справі № 760/20948/16-ц уточнила, що вартість частки у статутному капіталі не завжди дорівнює вартості внеску. Суд виходить із презумпції відповідності вартості частки розміру внеску, проте допускає можливість доведення зміни цієї вартості унаслідок діяльності товариства. Таким чином, інший із подружжя має право вимагати виплати половини вартості частки учасника товариства, а не лише половини внеску [3].

Постанова КЦС ВС від 01 травня 2024 року у справі № 334/9558/15 (I частина) підтвердила, що внесення одним із подружжя коштів до статутного капіталу ТОВ, які є спільною сумісною власністю, означає набуття товариством права власності на ці кошти. Учасник товариства набуває право на частку, а інший із подружжя – право вимагати виплати вартості цієї частки при поділі майна.

У II частині цієї ж постанови Верховний Суд розглянув питання звернення стягнення на частину майна товариства пропорційно частці учасника у статутному капіталі. Суд наголосив, що таке стягнення можливе лише у разі недостатності іншого майна боржника. При цьому позивачка може вимагати виплати вартості частки члена подружжя у статутному капіталі, визначеної на дату пред'явлення позовних вимог [5].

Таким чином, судова практика формує кілька ключових висновків:

- внесок одного з подружжя у статутний капітал ТОВ за рахунок спільних коштів створює право іншого з подружжя на компенсацію;
- право вимоги може стосуватися не лише вартості внеску, а й вартості частки у статутному капіталі;
- звернення стягнення на частку можливе лише за умови недостатності іншого майна боржника;
- суди виходять із презумпції рівності часток подружжя, якщо інше не визначено домовленістю чи шлюбним договором.

Попри наявність усталеної судової практики та доктринальних підходів, питання правового режиму частки в ТОВ у контексті сімейних правовідносин залишається проблемним. По-перше, відсутній єдиний законодавчий механізм реалізації прав другого з подружжя, який не є учасником товариства, але має право на компенсацію вартості частки. Це створює ризик неоднакового застосування норм судами та ускладнює прогнозованість правових наслідків. По-друге, існує небезпека порушення корпоратив-

ної стабільності у випадку поділу частки, адже залучення нового учасника або вимога компенсації може вплинути на баланс інтересів у товаристві. По-третє, актуальним є питання визначення реальної вартості частки. Це потребує додаткових процесуальних гарантій та чітких методик оцінки.

Перспективним напрямом розвитку є гармонізація сімейного та корпоративного законодавства, зокрема шляхом внесення змін до Сімейного кодексу України та Закону України «Про товариства з обмеженою та додатковою відповідальністю». Доцільним видається закріплення спеціальних норм щодо захисту прав другого з подружжя при поділі корпоративних прав, а також розробка єдиних правил оцінки вартості частки. Це сприятиме підвищенню правової визначеності та захисту інтересів як сім'ї, так і бізнесу.

Враховуючи все вищевикладене, можна дійти наступного висновку:

Частка в товаристві з обмеженою відповідальністю, набуту під час шлюбу, слід розглядати як об'єкт спільної сумісної власності подружжя. При цьому управлінські права залишаються за тим із подружжя, хто є учасником товариства, тоді як другий із подружжя має право на компенсацію або виплату вартості частки. Судова практика Верховного Суду підтверджує, що внесення спільних коштів до статутного капіталу трансформує право другого з подружжя у право вимоги на компенсацію, а в окремих випадках – на виплату вартості частки.

Таким чином, правовий режим частки в ТОВ у контексті сімейних правовідносин потребує подальшого вдосконалення. Вирішення проблеми можливе шляхом законодавчого закріплення спеціальних норм, які б забезпечували баланс між захистом прав подружжя та стабільністю корпоративних відносин. Це дозволить підвищити рівень правової визначеності, зменшити ризики судових спорів та сприятиме розвитку цивільного обороту в Україні.

ЛІТЕРАТУРА:

1. Сімейний кодекс України: Закон України від 10 січня 2002 року № 2947-III. URL: <https://zakon.rada.gov.ua/laws/show/2947-14#Text>

2. Постанова Великої Палати Верховного Суду від 10.04.2024 у справі № 760/20948/16-ц.
3. Постанова Касаційного цивільного суду у складі Верховного Суду від 11.12.2019 у справі № 638/19826/15-ц.
4. Постанова Касаційного цивільного суду у складі Верховного Суду від 01.05.2024 у справі № 334/9558/15.
5. Бобровник С.В. Правовий режим майна подружжя: монографія. Київ: Юрінком Інтер, 2018. 256 с.
6. Дякович М. М. Сімейне право України: навч. посібник. Львів: Світ, 2020. – 320 с
7. Сіщук Л.В. Корпоративні права як об'єкт цивільних прав. *Вісник цивільного права*. 2019. № 2. С. 45-52.

Гагарова Олександра Андріївна

*студ. 2 курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., проф. Зубар В.М.*

ПРАВОВЕ РЕГУЛЮВАННЯ РЕКЛАМНОГО КОНТЕНТУ, СТВОРЕНОГО ГЕНЕРАТИВНИМ ШІ

Інтеграція генеративного штучного інтелекту у сферу маркетингу та реклами стала одним із найпомітніших технологічних зрушень останніх років. Інструменти на кшталт ChatGPT, Gemini, Higgsfield тощо дозволяють бізнесу значно швидше створювати тексти, візуали, рекламні концепції та навіть повноцінні digital-кампанії. Для маркетолога це означає скорочення витрат на продакшн, зниження вартості залучення клієнта, однак з юридичної точки зору така ефективність супроводжується комплексом нових ризиків, оскільки наразі ще не вироблено остаточної, універсальної моделі регулювання ШІ-контенту.

Проблема полягає в тому, що рекламний контент, створений або суттєво модифікований ШІ, перебуває на перетині одразу кількох правових режимів: авторського права, законодавства про рекламу, норм про захист прав споживачів, цивільно-правового захисту зображення, імені та голосу особи, регулювання персональних даних. Відсутність належного юридичного комплаєнсу в цій сфері може призвести не лише до втрати ексклюзивності на

креатив, а й до претензій з боку правовласників, споживачів, державних органів та навіть міжнародних регуляторів [1, 2, 3].

Першим і найбільш дискусійним питанням є проблема авторства та належності прав інтелектуальної власності на контент, створений за допомогою генеративного ШІ. Для рекламного бізнесу це питання має принципове значення, оскільки будь-який бренд інвестує у створення унікального креативу саме для того, щоб отримати можливість контролювати його використання та забороняти копіювання конкурентам. У класичному розумінні авторського права роботи, створені дизайнером, набувають правової охорони за умови, що такий результат є творчим та оригінальним. Однак у випадку з генеративним ШІ правова ситуація ускладнюється тим, що результат може бути створений системою без безпосереднього творчого процесу з боку людини.

Сучасна міжнародна практика, зокрема позиція Бюро авторського права США та рішення у справі *Thaler v. Perlmutter*, виходить із того, що твір, створений виключно машиною без достатнього людського творчого контролю, не підлягає охороні традиційним авторським правом, оскільки автором у правовому сенсі може бути лише людина [4]. Закон України «Про авторське право і суміжні права» фактично визнає, що неоригінальні об'єкти, згенеровані комп'ютерною програмою, можуть отримувати спеціальний правовий режим у формі права особливого роду (*sui generis*), але не прирівнюються автоматично до класичних об'єктів авторського права [5].

Для маркетингу це створює прямий комерційний ризик. Якщо бренд запускає масштабну кампанію на основі згенерованого ШІ персонажа, він може виявити, що юридично не має достатньо сильного інструменту для заборони копіювання. Саме тому в сучасній практиці з'являється концепція так званого “human-in-the-loop”: юристи та маркетингологи рекомендують не покладатися на «чисту» генерацію, а забезпечувати суттєвий творчий внесок людини – редизайн у Photoshop, авторське доопрацювання, ручне компонування, редагування текстів, стилістичну адаптацію, монтаж, художню корекцію. Чим сильніше результат несе ознаки

людської індивідуальної творчості, тим вищі шанси на класичну авторсько-правову охорону [6].

Друга велика проблема пов'язана з тим, що генеративний ШІ не створює контент «з нуля» у буквальному розумінні, а працює на основі навчання на великих масивах існуючих зображень, текстів, музики, відео та інших даних.

Окремий ризик виникає тоді, коли маркетолог свідомо просить систему створити зображення «у стилі конкретного художника» або використовує промпти з назвами брендів і торговельних марок. Тут можливе одразу кілька рівнів правового конфлікту: порушення авторського права, недобросовісне використання чужого комерційного позначення, створення змішування у споживача, а іноді й порушення прав на торговельну марку. Якщо ШІ вставить у макет елементи, схожі на захищені логотипи, фірмові шрифти певного бренду чи айдентику конкурента, відповідальність несе не нейромережа, а рекламодавець або виробник реклами, які допустили запуск такого матеріалу в обіг.

Показовим є позов Getty Images проти Stability AI, у якому стверджувалося, що модель навчалася на зображеннях фотобанку без належної ліцензії, а окремі результати генерації навіть містили спотворені залишки водяних знаків Getty. Для рекламної практики це має прямий висновок: використання «дешевого» або непрозорого AI-інструмента без розуміння джерел його навчання може перетворитися на високий юридичний ризик. Тому бізнесу доцільно обирати сервіси з чіткою ліцензійною політикою, перевіряти умови використання, з'ясовувати, чи надає провайдер комерційні гарантії, чи передбачає відшкодування збитків (indemnification) у разі претензій правовласників, а також чи існують обмеження на використання згенерованого контенту у рекламі [7].

Третій блок проблем стосується прозорості, маркування та недопущення оманливої реклами. Генеративний ШІ дозволяє створювати надзвичайно реалістичні візуали товарів, «ідеальні» обличчя моделей, неіснуючі інтер'єри, синтетичні результати застосування косметики чи медичних засобів, а також рекламні ролики, які зовні виглядають як реальна зйомка. Якщо споживач

сприймає згенерований матеріал як достовірне відображення реального товару, реальної людини або реального ефекту від використання продукту, а насправді це лише синтетичне зображення, виникає ризик кваліфікації такої реклами як оманливої або недобросовісної.

За українським законодавством реклама не повинна вводити споживача в оману щодо властивостей товару, способу його використання, результатів застосування, якості, характеристик чи інших істотних ознак.

У європейському контексті це питання стає ще більш чутливим через нові правила прозорості щодо ШІ-контенту. Регламент ЄС про штучний інтелект (AI Act) формує підхід, за яким певні категорії контенту, зокрема діпфейки або синтетичні матеріали, що можуть сприйматися як справжні, мають бути чітко марковані. Для українського бізнесу це критично важливо, якщо реклама таргетується на ринки Польщі, Німеччини, Франції чи інших країн ЄС. На практиці це означає необхідність додавати дисклеймери, позначки на кшталт AI-generated, водяні знаки, пояснення у підписах до контенту або в умовах кампанії, якщо характер взаємодії зі споживачем вимагає підвищеної прозорості [8].

Також важливо звернути увагу на використання діпфейків та порушення особистих немайнових прав, зокрема права на зображення, ім'я, голос, ділову репутацію та комерційне використання образу особи. Генеративний ШІ радикально спростив створення контенту, в якому реальна або впізнавана людина може говорити, схвалювати продукт, рекомендувати бренд чи зніматися в рекламі без жодної фактичної участі. Для маркетингу це виглядає привабливо як спосіб здешевити роботу з інфлюенсерами або створити враження престижної асоціації з відомою особою, але з правової точки зору це одна з найбільш небезпечних практик.

Цивільне законодавство України захищає право фізичної особи на зображення та право на використання її імені. Використання образу людини в рекламі без згоди є прямим порушенням, а якщо йдеться про відомих осіб, масштаби відповідальності зро-

стають через комерційну цінність їхнього публічного образу та потенційні репутаційні збитки.

Показовим є міжнародний резонанс навколо ситуації зі Scarlett Johansson та OpenAI, коли голос AI-асистента викликав сильні асоціації з голосом акторки після того, як вона відмовилася від співпраці [9].

Таким чином, генеративний штучний інтелект уже став повноцінним інструментом сучасного маркетингу. ШІ дозволяє швидше й дешевше створювати рекламний контент, однак одночасно підвищує ризик втрати авторських прав, порушення прав третіх осіб, запуску оманливої реклами, незаконного використання образу фізичних осіб, появи діпфейків, фактичних помилок у комунікації з клієнтами та витоку персональних даних. У кожному з цих випадків відповідальність нестиме не алгоритм, а конкретний суб'єкт господарювання: рекламодавець, виробник реклами, агентство або оператор цифрової платформи.

Саме тому безпечне використання ШІ в рекламі має будуватися на кількох практичних принципах. Кожен згенерований креатив має проходити юридичну та редакторську перевірку на предмет плагіату, порушення прав на зображення, використання торговельних марок, недостовірних тверджень і потенційно оманливих елементів. Компаніям варто використовувати лише ті AI-інструменти, щодо яких зрозумілі джерела навчання, ліцензійні умови та гарантії комерційного використання.

Для сучасного юриста й маркетолога штучний інтелект є новим джерелом правових ризиків, яке потребує системного управління. Перемагає не той бізнес, який першим почав генерувати рекламу за допомогою ШІ, а той, хто зумів інтегрувати ШІ у маркетингові процеси так, щоб швидкість і масштаб не знищили правову безпеку бренду.

ЛІТЕРАТУРА:

1. Про авторське право і суміжні права: Закон України від 01.12.2022 № 2811-IX. URL: <https://zakon.rada.gov.ua/laws/show/2811-20#Text>
2. Про рекламу: Закон України від 03.07.1996 № 270/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/270/96-вр#Text>

3. Цивільний кодекс України : Кодекс України від 16.01.2003 № 435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>

4. Костенко Н. Хто володіє правами на картинку від ChatGPT? Нове в авторському праві в епоху ШІ. <https://zn.ua/ukr/TECHNOLOGIES/khto-volodije-pravami-na-kartinku-vid-chatgpt-nove-v-avtorskomu-pravi-v-epokhu-shi.html>

5. Sui generis, або як працює захист на згенеровані AI твори в Україні та світі. Barbashyn Law Firm. URL: <https://barbashyn.law/statti/sui-generis-how-ai-generated-works-are-protected-in-ukraine-and-beyond/>

6. Чи потрібна наявність людини в циклі або втручання людини для проекту AI/ML. URL: <https://uk.shaip.com/blog/need-for-human-in-the-loop-hitl-for-ml-projects/>

7. Getty Images проти Stability AI: у Британії триває судова битва, що може змінити правила гри для штучного інтелекту. URL: <https://sud.ua/uk/news/abroad/334289-getty-images-protiv-stability-ai-v-britanii-prodolzhaetsya-sudebnaya-bitva-kotoraya-mozhet-izmenit-pravila-igry-dlya-iskusstvennogo-intellekta>

8. EU Artificial Intelligence Act. URL: <https://artificialintelligenceact.eu/>

9. Скарлетт Йоганссон каже, що OpenAI вкрав її голос. Скандал через штучний інтелект – BBC News Україна. BBC News Україна. URL: <https://www.bbc.com/ukrainian/articles/crggjl3e830>

Гачук Дар'я Сергіївна

студ. 2 курсу факультету цивільної та господарської юстиції

Національного університету «Одеська юридична академія»

Науковий керівник: к.ю.н., проф. Зубар В.М.

РЕКВІЗИЦІЯ ГРОШОВИХ КОШТІВ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ

В умовах збройної агресії проти України та запровадження воєнного стану особливого значення набуває питання допустимих меж втручання держави у право приватної власності. Одним із правових механізмів такого втручання є реквізиція, яка застосовується з метою забезпечення публічних інтересів, зокрема обороноздатності держави. Водночас на практиці виникають складні питання щодо об'єктного складу реквізиції, зокрема можливості її застосування до грошових коштів.

Відповідно до частини п'ятої статті 41 Конституції України примусове відчуження об'єктів права приватної власності може

бути застосоване лише як виняток з мотивів суспільної необхідності, на підставі і в порядку, встановлених законом, та за умови попереднього і повного відшкодування їх вартості [1]. У свою чергу, стаття 353 Цивільного кодексу України визначає реквізицію як примусове відчуження майна у власника в умовах надзвичайних обставин із обов'язковим відшкодуванням його вартості [2]. У разі запровадження воєнного стану допускається відшкодування вартості після такого відчуження.

Спеціальним нормативно-правовим актом у цій сфері є Закон України «Про передачу, примусове відчуження або вилучення майна в умовах правового режиму воєнного чи надзвичайного стану», який деталізує процедуру примусового відчуження майна за рішенням військового командування, погодженого з відповідними органами державної влади [3]. При цьому законодавець визначає примусове відчуження як позбавлення права власності на індивідуально визначене майно, що переходить у власність держави.

Таким чином, уже на рівні законодавчого визначення простежується важлива ознака реквізиції – її застосування до індивідуально визначеного майна. Саме ця характеристика має принципове значення для вирішення питання про можливість реквізиції грошових коштів.

Згідно зі статтями 177, 190 Цивільного кодексу України гроші визнаються об'єктами цивільних прав і входять до складу майна. Водночас їх правова природа є специфічною: відповідно до частини другої статті 184 Цивільного кодексу України гроші належать до речей, визначених родовими ознаками, а отже є замінними [2]. Це означає, що вони не мають індивідуальних характеристик, які б дозволяли ідентифікувати їх як конкретний об'єкт, що відрізняється від інших однорідних речей.

Наведена особливість грошових коштів вступає у суперечність із природою реквізиції. Остання передбачає вилучення конкретного майна, необхідного для задоволення потреб держави, із подальшим відшкодуванням його вартості. У випадку з грошима така конструкція втрачає логічну завершеність, оскільки гроші

самі є універсальним еквівалентом вартості. Відповідно, вилучення грошей із наступним відшкодуванням їх вартості у грошовій формі не забезпечує реального відновлення майнового становища особи, а лише формально відтворює той самий об'єкт.

Практичне значення цієї проблеми підтверджується судовою практикою. У справі № 906/1517/23 ТОВ «ТС Трейд» оскаржувало наказ військової частини щодо примусового відчуження грошових коштів для потреб держави в умовах воєнного стану. Господарський суд Житомирської області (перша інстанція) задовольнив позов, визнавши наказ протиправним і скасувавши його. Північно-західний апеляційний господарський суд (друга інстанція) залишив рішення без змін. Верховний Суд (касаційна інстанція) повернув касаційну скаргу військової частини через процесуальні недоліки, не розглядаючи справу по суті, що підтверджує чинність рішень судів нижчих інстанцій [4].

Обґрунтовуючи свою позицію, суд зазначив, що грошові кошти є речами, визначеними родовими ознаками, тобто замінними, тоді як законодавство про реквізицію передбачає можливість відчуження лише індивідуально визначеного майна. У зв'язку з цим положення статті 353 Цивільного кодексу України не можуть бути застосовані до грошових коштів [2]. Крім того, суд звернув увагу на відсутність у законодавстві спеціальних норм, які б прямо передбачали можливість примусового відчуження грошей у порядку реквізиції.

Зазначений підхід узгоджується із загальними принципами захисту права власності. Як підкреслював Конституційний Суд України (Перший сенат) в абзаці сьомому підпункту 2.3 пункту 2 мотивувальної частини рішення від 5 червня 2019 року № 3-р(І)/2019, право власності не є абсолютним і може бути обмежене лише на підставі закону з дотриманням принципу пропорційності, який передбачає необхідність досягнення розумного балансу між інтересами особи та суспільства [5]. Водночас одним із ключових елементів такого балансу є забезпечення ефективного відшкодування, що у випадку грошових коштів набуває проблемного характеру з огляду на їх правову природу.

Окремо слід відмежовувати реквізицію від інших правових механізмів вилучення грошових коштів. Зокрема, арешт коштів у межах кримінального провадження, їх конфіскація як санкція за вчинення правопорушення або застосування податкових чи інших обов'язкових платежів мають іншу правову природу і підстави застосування. Вони не передбачають компенсаційного характеру, який є визначальним для реквізиції, і тому не можуть розглядатися як її різновид.

В умовах воєнного стану держава об'єктивно потребує ефективних інструментів мобілізації ресурсів. Проте використання таких інструментів повинно здійснюватися в межах правових конструкцій, передбачених законодавством. Спроба застосувати інститут реквізиції до грошових коштів фактично призводить до підміни одного правового механізму іншим і створює ризик порушення конституційних гарантій права власності.

Відсутність чіткого нормативного регулювання питання щодо можливості реквізиції грошей також свідчить про наявність прогалини у законодавстві, яка частково заповнюється судовою практикою. При цьому сформований судами підхід ґрунтується на системному тлумаченні норм цивільного законодавства та врахуванні правової природи грошей як об'єкта цивільних прав.

Отже, реквізиція як інститут цивільного права за своєю сутністю спрямована на відчуження індивідуально визначеного майна з метою задоволення публічних потреб із обов'язковим відшкодуванням його вартості. Грошові кошти, будучи родовими та замінними речами, не відповідають цим ознакам, що виключає можливість їх реквізиції у класичному розумінні. Судова практика підтверджує зазначений висновок і формує підхід, відповідно до якого примусове відчуження грошових коштів під виглядом реквізиції є неправомірним. Вирішення цієї проблеми потребує законодавчого уточнення меж застосування реквізиції та чіткого розмежування її з іншими формами вилучення майна з метою забезпечення балансу між публічними інтересами та правами власників в умовах воєнного стану.

ЛІТЕРАТУРА:

1. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
2. Цивільний кодекс України: Закон України від 16.01.2003 №435-IV. *Відомості Верховної Ради України*. 2003. № № 40-44. Ст. 356.
3. Про передачу, примусове відчуження або вилучення майна в умовах правового режиму воєнного чи надзвичайного стану: Закон України від 17.05.2012 № 4765-VI. *Відомості Верховної Ради України*. 2013. № 15. Ст. 99.
4. Справа № 906/1517/23: Судова справа за позовом Товариства з обмеженою відповідальністю «ТС ТРЕЙД» до Військової частини НОМЕР_1 про визнання протиправним та скасування наказу. URL: <https://reyestr.court.gov.ua/>
5. Рішення Конституційного суду України (Перший сенат) від 05.06.2019 № 3-п(І)/2019. URL: <https://zakon.rada.gov.ua/laws/show/va03p710-19#Text>

Журило Євгенія Сергіївна

*студ. 2 курсу факультет цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н, проф. Зубар В.М.*

ПОНЯТТЯ ТА СУТЬ ЦИВІЛЬНИХ ПРАВОВІДНОСИН

Цивільні правовідносини є ключовою категорією приватного права, оскільки охоплюють широке коло суспільних відносин, які виникають у сфері обігу майна, послуг, особистих немайнових благ. Вони мають майновий або особистий немайновий характер і ґрунтуються на рівності, автономії волі та майновій самостійності сторін [1].

Відповідно до Цивільного кодексу України (далі – ЦК України), цивільні правовідносини – це врегульовані нормами цивільного законодавства суспільні відносини, учасники яких виступають як юридично рівні особи. У ст. 1 ЦК України зазначено, що він регулює особисті немайнові та майнові відносини, засновані на юридичній рівності сторін, вільному волевиявленні та майновій самостійності [2].

Цивільні правовідносини виникають з різних юридичних фактів – договорів, заподіяння шкоди, створення та використання об'єктів інтелектуальної власності, спадкування, рішень суду тощо. Їхніми учасниками можуть бути фізичні особи, юридичні особи, а також держава, Автономна Республіка Крим, територіальні громади, які мають цивільну правоздатність та дієздатність.

У науковій літературі цивільні правовідносини традиційно поділяють на:

- майнові (включаючи зобов'язальні, речові, спадкові);
- особисті немайнові, що не пов'язані з майном (право на ім'я, честь, гідність, інтелектуальну власність тощо) [3, с. 332].

Суть цивільних правовідносин полягає у взаємному визнанні і захисті прав та інтересів учасників, що діють в умовах недопустимості примусу (за винятком передбачених законом випадків) і свободи волевиявлення. Згідно з ЦК України, особи, що беруть участь у цивільних відносинах, мають право вільно встановлювати зміст правовідносин, якщо це не суперечить закону (ст. 6 ЦК України).

Важливою особливістю цивільних правовідносин є те, що вони можуть виникати не лише між приватними суб'єктами, а й за участі публічно-правових утворень, у тому числі територіальних громад. Така участь допускається лише в межах цивільної правособ'єктності, наприклад, при укладенні договорів купівлі-продажу комунального майна, здійсненні інвестицій, оренді майна, тощо.

Цивільні правовідносини охоплюють як загальні майнові та немайнові відносини, так і спеціалізовані категорії, що мають характерну правову специфіку. Яскравим прикладом є цивільні правовідносини за участю споживача[4, с.976].

У науковій літературі зазначається, що для зручності використовується термін «споживчі правовідносини», хоча точнішим з юридичної точки зору вважається вживання поняття «цивільні правовідносини за участю споживача». Такий підхід відображає

особливості суб'єктного складу та правову природу цих відносин, у яких з однієї сторони виступає споживач – фізична особа, що купує товари, замовляє послуги або роботи для власних потреб, а з іншої – суб'єкт підприємницької діяльності.

Дослідники наголошують, що цей тип правовідносин має комплексний (приватно-публічний) характер: він поєднує в собі диспозитивність цивільного регулювання з імперативними нормами законодавства про захист прав споживачів. Саме тому цивільні правовідносини за участю споживача формуються на договірній основі, проте із значним ступенем законодавчого втручання на користь слабшої сторони – споживача [5, с.47].

До основних ознак таких правовідносин належать:

- юридична рівність сторін за загальними принципами цивільного права;
- їх оплатний і зобов'язальний характер (зазвичай, на підставі договору);
- поєднання норм цивільного, господарського, адміністративного, екологічного та конституційного права в системі правового регулювання;
- підвищена правова охорона інтересів споживача;
- можливість судового захисту порушених прав споживача у цивільному, адміністративному або кримінальному провадженні;
- домінування норм, які не можуть бути змінені угодою сторін на шкоду споживачеві [6, с. 27].

Отже, цивільні правовідносини є фундаментальною категорією приватного права, що охоплює широкий спектр суспільних взаємин майнового та немайнового характеру. Їх основою є рівність, свобода волевиявлення та самостійність сторін. Учасниками таких відносин можуть бути не лише фізичні й юридичні особи, а й публічно-правові утворення, включаючи територіальні громади, які діють у межах наданої їм цивільної правосуб'єктності.

Особливе місце серед видів цивільних правовідносин посідають правовідносини за участю споживача. Вони мають комплекс-

сну правову природу, поєднуючи у собі як приватноправові, так і публічно-правові елементи, що зумовлено необхідністю посиленого захисту слабшої сторони. Такий приклад ілюструє гнучкість та багаторівневність цивільно-правового регулювання в сучасній правовій системі.

Таким чином, цивільні правовідносини – це динамічний правовий інструмент, який забезпечує врегулювання широкого кола взаємин у суспільстві, а також дає змогу реалізувати правовий потенціал усіх суб'єктів – від окремого громадянина до територіальної громади як учасника цивільного обороту.

ЛІТЕРАТУРА:

1. Цивільне право. Загальна частина: навчальний посібник. За заг. ред. С. О. Сліпченка, О. Л. Зайцева. Харків : ХНУВС, 2022. 332 с.
2. Цивільний кодекс України: Закон України від 16 січ. 2003 р. № 435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>
3. Цивільне право України: Загальна частина: навчальний посібник. За заг. ред. С. О. Сліпченка, О. Л. Зайцева. Харків: ХНУВС, 2022. 332 с.
4. Цивільне право України: підручник : у 2 т. За ред. О. В. Дзери, Н. С. Кузнецової. 4-те вид., перероб. і допов. Київ : Юрінком Інтер, 2018. Т. 1. 976 с.
5. Абрамчук Д. В. Примірний договір у цивільному праві України: дис. ... канд. юрид. наук: 12.00.03. Тернопіль, 2023. 224 с.
6. Єфремова І., Ломакіна І. Цивільне право (загальна частина): навч. посіб. у схемах. Біла Церква: Білоцерк. нац. ун-т, 2023. 122 с.

Заборська Ксенія Андріївна

*студ. 3 курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., проф. Зубар В.М.*

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМАХ КІБЕРРОЗВІДКИ: ПРАВОВІ ВИКЛИКИ ТА РЕГУЛЯТОРНІ ПІДХОДИ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ

Стрімкий розвиток технологій штучного інтелекту (далі – ШІ) зумовлює їх активне впровадження у сферу кіберрозвідки та захисту критичної інформаційної інфраструктури. В умовах

гібридної війни, яку веде Російська Федерація проти України, системи ШІ перетворилися на ключовий інструмент як виявлення кіберзагроз, так і проведення наступальних кібератак. Це породжує принципово нові правові виклики, які потребують негайного доктринального осмислення та нормативного врегулювання [1, с. 12].

Застосування ШІ у кіберрозвідці охоплює широкий спектр завдань: автоматизований аналіз загроз, виявлення аномалій у мережевому трафіку, прогнозування векторів атак, а також атрибуція кіберінцидентів – встановлення суб'єкта, відповідального за здійснення кібератаки. Саме атрибуція є найбільш юридично значущою функцією, оскільки від її результатів залежить можливість притягнення відповідних осіб до міжнародно-правової відповідальності [2, с. 45].

Водночас правовий статус висновків, сформованих системами ШІ в процесі кіберрозвідки, залишається невизначеним. Чинне законодавство України, зокрема Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII, не містить норм щодо допустимості використання результатів автоматизованого аналізу як доказів у судових та адміністративних провадженнях. Відповідна прогалина унеможливорює ефективне правозастосування в ситуаціях, коли ШІ-система ідентифікує конкретного суб'єкта як організатора кібератаки [3].

Окремої уваги заслуговує питання захисту персональних даних, що обробляються ШІ-системами кіберрозвідки. Масштабний збір інформації про мережеву активність користувачів об'єктивно суперечить принципам мінімізації даних та цільового обмеження, закріпленим у Законі України «Про захист персональних даних» та Регламенті ЄС 2016/679 (GDPR). Проте в умовах збройного конфлікту такі обмеження можуть бути деактивовані в порядку, передбаченому ст. 23 GDPR та аналогічними положеннями національного законодавства, що допускають відступ від окремих гарантій захисту даних у виняткових обставинах [4, с. 78].

На рівні Європейського Союзу Регламент про штучний інтелект (AI Act, Регламент ЄС 2024/1689) відносить системи ШІ, що

використовуються у сфері правоохоронної діяльності та національної безпеки, до категорії систем із «неприйнятним» або «високим» ризиком. Відповідно, їх використання підпорядковується суворим вимогам щодо прозорості, людського нагляду та документування. Проте сфера дії AI Act прямо не поширюється на застосування ШІ у воєнних цілях, що формує суттєву регуляторну прогалину [5, с. 103].

Виходячи з аналізу чинної нормативно-правової бази та доктринальних підходів, можна дійти таких висновків. По-перше, необхідно закріпити у Законі України «Про основні засади забезпечення кібербезпеки України» положення щодо правового статусу та доказової сили висновків ШІ-систем кіберрозвідки. По-друге, слід розробити спеціальний правовий режим використання систем ШІ в умовах воєнного та надзвичайного стану, який би збалансував інтереси національної безпеки із захистом прав і свобод особи. По-третє, Україна має ініціювати розробку міжнародно-правових стандартів атрибуції кібератак із використанням ШІ на рівні ООН та Ради Європи, що сприятиме формуванню єдиної доказової бази для притягнення винних до відповідальності [6, с. 211].

ЛІТЕРАТУРА:

1. Довгань О.Д., Доронін І.М. Правовий режим кіберпростору України: монографія. Київ: АртЕк, 2022. 256 с.
2. Баранов О.А. Інтернет речей: концептуальні правові підходи до регулювання. *Інформація і право*. 2019. № 4 (31). С. 39-56.
3. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>
4. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія. Київ: АртЕк, 2020. 354 с.
5. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. 2024. L 1689. P. 1–144.
6. Цимбалюк В.С. Інформаційне право: концептуальні положення до кодифікації інформаційного законодавства. Київ: Освіта України, 2021. 426 с.

Казарян Ліліт Романівна

*студ. 2 курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., проф. Зубар В.М.*

СПАДКУВАННЯ МАЙНА, ЩО ЗНАХОДИТЬСЯ НА ТИМЧАСОВО ОКУПОВАНИХ ТЕРИТОРІЯХ: ПРОБЛЕМИ ТА СПЕЦИФІКА

В умовах війни, значна частина території України перебуває під тимчасовою окупацією, що створює низку правових проблем, зокрема у сфері реалізації спадкових прав. Особливо гостро постає питання спадкування майна, розташованого на таких територіях, адже доступ до нього та документів, які посвідчують його, є обмеженим або взагалі неможливим, а правовий режим, як наслідок – невизначеним.

Актуальність цієї теми зумовлюється необхідністю забезпечення захисту права на спадкування громадян України в умовах тривалої збройної агресії та тимчасової окупації територій (далі – ТОТ). Крім того, дане проблемне питання пов'язане з майбутніми міжнародними механізмами компенсації завданих збитків, а правильне оформлення належних документів та прав, відповідно до українського законодавства, надасть можливість громадянам надалі звернутися за відшкодуванням втрат або знищеного майна, завданого внаслідок збройної агресії РФ проти України, через Міжнародний Реєстр збитків.

Початком та підставою виникнення спадкових правовідносин є відкриття спадщини, яка згідно з цивільним законодавством відкривається внаслідок смерті особи або оголошення її померлою. Під спадкуванням розуміється перехід прав та обов'язків від фізичної особи, яка померла (спадкодавця) до інших осіб (спадкоємців). Цей процес залежить від часу відкриття спадщини, яким вважається фактична дата смерті особи або дата набрання чинності рішення суду про оголошення особи померлою. У випадку смерті спадкодавця на ТОТ, необхідно звернутися до нотаріуса для оформлення спадщини, але попередньо потрібно обов'язково вста-

новити факт смерті. Заяви про встановлення факту смерті особи у визначений час підлягають розгляду судом за умови надання заявниками документів, які підтверджують відмову органів державної реєстрації актів цивільного стану у здійсненні реєстрації факту смерті. Отримавши відмову, родичу або членам сім'ї слід звернутися до найближчого місцевого суду, розташованого на території, що перебуває під контролем України [6, ст. 317].

Суд, прийнявши рішення, обов'язково повинен зазначити дані про встановлений факт смерті, цілі його встановлення, а також повний перелік доказів, на яких ґрунтується висновок суду. Однак, на цьому етапі, можуть виникнути проблеми з доказовою базою, тому що, видані окупаційним органом документи, що підтверджують смерть особи є недійсними та відповідно не мають юридичної сили й правових наслідків [3, ст. 9].

До цього ж, у Постанові ВС від 20 грудня 2018 року у справі № 707/1607/16-ц, зазначено, що посилання заявником на застосування «намібійського винятку», відповідно до якого, документи, видані органами окупаційної влади, можуть враховуватися судами у разі, якщо їх ігнорування суттєво порушать або обмежать права людини, не дає достатніх підстав, для висновку, що факт смерті може підтверджуватися виключно документами, виданими органами на непідконтрольній території України. Особа, яка подає заяву, може надати в якості доказів, як приклад пояснення свідків, фототаблиці тощо [2].

Наприклад, Рішення Приморського районний суд м. Одеси у справі від 06.03.2026 № 522/23549/25-Е задовільнив заяву про встановлення факту смерті особи, яка померла на ТОТ, посилаючись пояснення свідків, що підтвердили спорідненість між заявником та спадкодавцем, на фотофіксацією місця поховання та свідоцтво про смерть, видане окупаційним органом, таким чином застосувавши принцип «намібійського винятку».

Розгляд таких справ, здійснюється у найкоротший строк після отримання відповідної заяви, а прийняте рішення підлягає виконанню без зволікань одразу після його ухвалення. Лише далі є

можливість звернення до нотаріуса з метою оформлення спадкових прав. Місцем відкриття спадщини в такому випадку вважається місце подання першої заяви спадкоємцем. Водночас обов'язковою умовою є наявність правовстановлюючих документів на нерухоме майно, що входить до складу спадщини, але можуть виникнути труднощі, через відсутність доступу до оригіналів документів на спадкове майно.

У разі, якщо до складу спадщини входить нерухоме майно, нотаріус має можливість отримати відомості про нього з Державного реєстру речових прав на нерухоме майно. Якщо ж спадкоємець не може надати необхідні документи для видачі свідоцтва про право на спадщину, то вирішення зазначеного питання буде здійснюватися шляхом подання позову до суду про визнання права власності в порядку спадкування після спливу строку для прийняття спадщини, попередньо отримавши від нотаріуса постанову про відмову у вчиненні нотаріальних дій, у зв'язку з відсутністю відповідних документів. Після набрання судовим рішенням законної сили, спадкоємець повторно звертається до нотаріуса і оформлює належним чином своє право на спадщину, але доступ до неї залишається обмеженим до моменту відновлення контролю України над відповідною територією.

Підсумовуючи, варто зазначити, що встановлення юридичного факту смерті особи або ухвалення рішення щодо її оголошення померлою в судовому порядку є одним із невід'ємних та важливих етапів у справах про спадкування. Саме тоді визначається початок права на спадщину та відкривається шестимісячний строк для її прийняття. Однак навіть в умовах війни й окупації, попри всі складнощі, реалізація спадкових прав залишається можливою за умови своєчасного звернення спадкоємців до суду, належної підготовки доказів та дотримання встановлених процедур.

Практика свідчить, що у випадках обґрунтованого пропуску строків, судові органи та нотаріуси часто ухвалюють рішення на користь заявників, забезпечуючи доступ до спадщини і відновлення порушених прав.

ЛІТЕРАТУРА

1. Миколаївський місцевий центр з надання безоплатної вторинної правової допомоги. Спадкування майна на тимчасово окупованих та деокупованих територіях України. 30.01.2023. URL: <https://kucurubskagromada.gov.ua/news/1675063151/>
2. Про встановлення фактів, що мають юридичне значення: Постанова Верховного Суду України від 20.12.2018 № 707/1607/16-ц. URL: <https://reyestr.court.gov.ua/Review/78978236>
3. Про забезпечення прав і свобод громадян та правовий режим на тимчасово окупованій території України: Закон України від 15.04.2014 № 1207-VII. URL: <https://zakon.rada.gov.ua/laws/show/1207-18#n52>
4. У справі № 522/23549/25-Е: Рішення Приморського районного суду м. Одеси від 06.03.2026. URL: <https://reyestr.court.gov.ua/Review/134565617>
5. Цивільний кодекс України: Закон України від 16.01.2003, № № 435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>
6. Цивільний процесуальний кодекс України: Закон України від 18.03.2004, № 1618-IV. URL: <https://zakon.rada.gov.ua/laws/show/1618-15#Text>

Калова Вікторія Сергіївна

*студ. 3 курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., доц. Берназ-Лукавецька О.М.*

ЦИВІЛЬНО-ПРАВОВІ ОСОБЛИВОСТІ ДОГОВОРІВ У СФЕРІ КІБЕРБЕЗПЕКИ

Актуальність дослідження цивільно-правових особливостей договорів у сфері кібербезпеки зумовлена стрімким розвитком інформаційних технологій та зростанням кількості кіберзагроз у сучасному цифровому середовищі. У сучасних умовах цифровізації суспільства питання захисту інформаційних систем, персональних даних та електронної інфраструктури набуває особливого значення для держави, бізнесу та громадян. Договірні відносини у сфері кібербезпеки стають важливим інструментом правового регулювання взаємодії між суб'єктами господарювання, що надають або отримують послуги із захисту інформаційних ресурсів. Особливої актуальності ця проблематика набула в умовах воєнно-

го стану, коли кіберпростір стає одним із ключових напрямів протидії зовнішнім загрозам. Правове врегулювання таких договорів повинно враховувати як загальні положення цивільного законодавства, так і спеціальні норми законодавства у сфері кібербезпеки. Саме тому дослідження цивільно-правових особливостей договорів у сфері кібербезпеки є важливим для формування ефективної правової системи захисту інформаційних ресурсів та забезпечення стабільності цифрової інфраструктури держави.

Правове регулювання відносин у сфері кібербезпеки здійснюється на основі комплексного підходу, що поєднує норми цивільного, інформаційного та спеціального законодавства. Закон України «Про основні засади забезпечення кібербезпеки України» визначає основні принципи функціонування національної системи кібербезпеки, а також встановлює правові та організаційні основи взаємодії суб'єктів у цій сфері. Ураховуючи положення зазначеного нормативно-правового акта, можна зробити висновок, що забезпечення кібербезпеки передбачає координацію діяльності державних органів, підприємств та інших суб'єктів інформаційних відносин, а також створення умов для захисту інформаційних ресурсів і критичної інформаційної інфраструктури. На погляд автора, зазначені положення мають важливе значення і для формування договірних відносин у сфері кібербезпеки, оскільки вони визначають загальні принципи взаємодії суб'єктів у цифровому середовищі. З погляду цивільного права, такі положення виступають правовою основою для укладення договорів про надання послуг із забезпечення кіберзахисту та визначення прав і обов'язків сторін у відповідних правовідносинах [1, с. 403].

У практиці правового регулювання відносин у сфері кібербезпеки важливе значення має визначення конкретних договірних форм, у межах яких здійснюється взаємодія між суб'єктами інформаційних відносин. Відповідно до положень цивільного законодавства, «договором є домовленість двох або більше сторін, спрямована на встановлення, зміну або припинення цивільних прав та обов'язків» (ст. 626 Цивільний кодекс України). При цьо-

му «сторони є вільними в укладенні договору, виборі контрагента та визначенні умов договору» (ст. 627 ЦК України). Важливим є також положення про те, що «зміст договору становлять умови (пункти), визначені на розсуд сторін і погоджені ними» (ст. 628 ЦК України). Зазначені норми мають фундаментальне значення для договорів у сфері кібербезпеки, оскільки саме вони дозволяють сторонам самостійно визначати специфічні технічні та організаційні умови співпраці. З огляду на специфіку забезпечення захисту інформаційних ресурсів та інформаційної інфраструктури, у даній сфері застосовується декілька основних видів цивільно-правових договорів, які відрізняються за своїм предметом та характером зобов'язань сторін.

Найбільш поширеним є договір про надання послуг у сфері інформаційної безпеки. У межах такого договору виконавець зобов'язується здійснювати комплекс організаційних та технічних заходів, спрямованих на забезпечення належного рівня захисту інформаційних систем замовника. До таких послуг можуть належати проведення аудиту інформаційної безпеки, аналіз уразливостей інформаційних систем, тестування на проникнення (penetration testing), оцінка ризиків кіберзагроз, а також розроблення рекомендацій щодо вдосконалення системи захисту інформації.

Досить поширеною формою правового оформлення відповідних відносин є також договір підяду на створення або впровадження систем кіберзахисту. Особливістю такого договору є те, що його предметом виступає конкретний результат роботи – створення, налаштування або модернізація програмно-технічних засобів захисту інформації. Йдеться, зокрема, про розроблення спеціалізованого програмного забезпечення, встановлення систем виявлення кіберзагроз, впровадження криптографічних засобів захисту інформації або інтеграцію комплексних систем інформаційної безпеки.

У сучасній практиці значного поширення набули також договори аутсорсингу кібербезпеки. У цьому випадку підприємство або організація передає функції забезпечення інформаційної без-

пеки спеціалізованій компанії, яка здійснює постійний моніторинг інформаційних систем, аналізує кіберзагрози, контролює стан захисту інформації та забезпечує оперативне реагування на кіберінциденти. Така модель взаємодії є особливо ефективною для суб'єктів господарювання, які не мають власних підрозділів кібербезпеки або достатніх технічних ресурсів для самостійного забезпечення належного рівня захисту інформаційної інфраструктури.

Крім того, у сфері кібербезпеки широко застосовуються договори технічної підтримки та моніторингу інформаційної безпеки. Предметом таких договорів є забезпечення постійного супроводу функціонування інформаційних систем, оновлення програмного забезпечення, контроль за станом захисту даних, а також своєчасне виявлення та усунення технічних уразливостей. Наявність подібних договірних відносин дозволяє забезпечити безперервний контроль за станом кіберзахисту та знизити ризик виникнення кіберінцидентів.

Таким чином, різноманітність договірних форм у сфері кібербезпеки свідчить про складний характер відповідних правовідносин та необхідність комплексного підходу до їх правового регулювання. Використання різних видів цивільно-правових договорів дозволяє врахувати специфіку інформаційних технологій та забезпечити ефективну взаємодію між суб'єктами у сфері захисту інформаційних ресурсів[6, с. 161-170].

Аналізуючи роботу Ф. І. Василенка, який у своєму дослідженні розглянув цивільно-правові договори у сфері ІТ, можна зазначити, що договірні відносини у сфері кібербезпеки мають ряд специфічних особливостей, зокрема високий рівень технічної складності предмета договору, необхідність детального визначення обсягу послуг та встановлення підвищених вимог до конфіденційності інформації. Автор звертає увагу на те, що ІТ-договори часто мають змішаний характер та поєднують елементи різних цивільно-правових конструкцій. На погляд автора, договори у сфері кібербезпеки можуть включати положення щодо розроблен-

ня та впровадження програмного забезпечення, обслуговування інформаційних систем, моніторингу кіберзагроз та реагування на кіберінциденти. З погляду цивільно-правового регулювання важливим є також визначення відповідальності сторін за порушення умов договору, особливо у випадках витоку інформації або нена належного захисту даних. У цьому контексті важливими є також положення цивільного законодавства щодо виконання зобов'язань, відповідно до яких «зобов'язання має виконуватися належним чином відповідно до умов договору» (ст. 526 ЦК України). Крім того, «боржник вважається таким, що прострочив, якщо він не приступив до виконання зобов'язання або не виконав його у строк» (ст. 612 ЦК України). Водночас «особа, яка порушила зобов'язання, несе відповідальність за наявності її вини» (ст. 614 ЦК України). Такі положення мають особливе значення для договорів у сфері кібербезпеки, оскільки дозволяють визначити правові наслідки нена належного захисту інформації або невиконання зобов'язань щодо кіберзахисту. Таким чином, договір у сфері кібербезпеки виступає складним правовим механізмом, який поєднує технічні та юридичні аспекти взаємодії сторін [2, с. 85-92].

В роботі А. Г. Мосейка, який у своєму дослідженні розглянув особливості правового регулювання договорів у сфері трансферу технологій, можна зазначити, що подібні правові конструкції застосовуються і у сфері кібербезпеки. Автор підкреслює, що договори, пов'язані з передачею технологій, передбачають регулювання прав на використання інтелектуальної власності, програмного забезпечення та технічних рішень. На погляд автора, у сфері кібербезпеки це має особливе значення, оскільки більшість технологій захисту інформації базується на спеціалізованих програмних продуктах та алгоритмах. З погляду правового регулювання важливо встановити чіткі умови використання таких технологій, порядок передачі прав на них, а також механізми захисту комерційної таємниці. У свою чергу, належне врегулювання цих аспектів сприяє підвищенню рівня довіри між суб'єктами господарювання та забезпечує ефективність реалізації договірних відносин у сфері кіберзахисту [3, с. 112-118].

Ураховуючи роботу В. Багрій, яка у своєму дослідженні розглянула особливості правового регулювання договірних відносин у ІТ-сфері, можна зазначити, що такі договори характеризуються значною складністю структури та високим рівнем індивідуалізації умов. Автор звертає увагу на те, що сторони договору повинні детально визначати технічні параметри виконання робіт або надання послуг, строки їх реалізації та порядок взаємодії у процесі виконання зобов'язань. На погляд автора, у договорах у сфері кібербезпеки особливе значення має закріплення процедур реагування на кіберінциденти, визначення стандартів захисту інформації та встановлення механізмів контролю за виконанням договірних зобов'язань. З погляду цивільного права, належне врегулювання цих аспектів сприяє підвищенню рівня правової визначеності та забезпечує ефективну реалізацію прав і обов'язків сторін у сфері інформаційних технологій [4, с. 202-206].

Таким чином, договори у сфері кібербезпеки є важливим інструментом правового регулювання відносин у сучасному інформаційному суспільстві. Їх цивільно-правова природа передбачає застосування загальних положень цивільного законодавства з урахуванням специфіки цифрових технологій. Важливим є чітке визначення предмета договору, прав та обов'язків сторін, а також відповідальності за порушення умов забезпечення кіберзахисту. Ефективне правове регулювання таких договорів сприяє підвищенню рівня захисту інформаційних ресурсів та стабільності цифрової інфраструктури. Подальший розвиток законодавства у сфері кібербезпеки має бути спрямований на вдосконалення договірних механізмів взаємодії між суб'єктами інформаційних відносин.

ЛІТЕРАТУРА:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.
2. Василенко Ф. І. Цивільно-правові договори в сфері ІТ: поняття, класифікація та специфіка виконання в умовах війни. *International Scientific Journal "Internauka". Series: "Juridical Sciences"*. 2024. № 8. С. 85-92.

3. Мосейко А. Г. Особливості правового регулювання договорів у сфері трансферу технологій нормами господарського права України. *Юридична наука*. 2021. № 4. С. 112-118.

4. Багрій В., Бондаренко О. Особливості правового регулювання договірних відносин у ІТ сфері. *Збірник наукових праць Донецького державного університету внутрішніх справ*. 2024. С. 202-206.

5. Цивільний кодекс України: Закон України від 16 січня 2003 р. № 435-IV. *Відомості Верховної Ради України*. 2003. № 40-44. Ст. 356.

6. Bomhard D., Daum A. Кібербезпека в аутсорсингу та хмарних обчисленнях: зростаючий виклик для укладення договорів. *International Cybersecurity Law Review*. 2021. Т. 2, № 1. С. 161–171. DOI: 10.1365/s43439-021-00029-4.

Коваленко Ростислав Русланович

*студ. 2 курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., проф. Зубар В.М.*

УСУНЕННЯ ВІД ПРАВА НА СПАДКУВАННЯ

Інститут усунення від права на спадкування є одним із ключових механізмів захисту інтересів спадкодавця та інших спадкоємців у цивільному праві України. Відповідно до ст. 1224 Цивільного кодексу України [1] визначено вичерпний перелік підстав, за наявності яких особа може бути усунена від права на спадкування. Актуальність дослідження цього питання підтверджується і судовою статистикою: на сьогодні в реєстрі судових рішень налічується понад 100 тисяч справ, пов'язаних із питаннями усунення від права на спадкування [2, с. 153-154].

Перш ніж перейти до аналізу підстав, варто розмежувати поняття «усунення від права на спадкування» та «позбавлення права на спадкування». Позбавлення права на спадкування здійснюється виключно заповідачем через заповіт і регулюється ч. 2 ст. 1235 ЦК України. Натомість усунення від права на спадкування – це позбавлення права на спадщину так званих «негідних спадкоємців» на підставі закону або рішення суду, яке можливе виключно у випадках, чітко визначених ст. 1224 ЦК України [3, с. 7]. При цьому важливо зазначити, що усунення від права на спадкування не

обмежує загальну цивільну правоздатність фізичної особи у розумінні ст. 26 ЦК України, а стосується лише конкретного випадку спадкового правонаступництва [3, с. 8-9].

Законодавець поділяє «негідних спадкоємців» на дві групи: перша – особи, які не можуть спадкувати ні за законом, ні за заповітом; друга – особи, які не можуть спадкувати лише за законом [3, с. 9]. Розглянемо кожну підставу детальніше.

Першою та найбільш суспільно небезпечною підставою є умисне позбавлення життя спадкодавця чи будь-кого з можливих спадкоємців або вчинення замаху на їхнє життя (ч. 1 ст. 1224 ЦК України) [1]. Оскільки зазначені діяння є кримінально караними, вони повинні бути підтверджені вироком суду або постановою про закриття кримінальної справи з nereабілітуючих підстав [2]. При цьому закон не вимагає, щоб вбивство було вчинене саме з метою заволодіння спадщиною: особи, які вчинили вбивство з ревнощів, помсти чи хуліганських мотивів, також підлягають усуненню від спадкування [3, с. 8].

Водночас у науковій літературі активно дискутується питання про межі застосування цієї підстави. Зокрема, Ю. О. Заїка зазначає, що вчинення злочину з необережності, наприклад, при порушенні правил дорожнього руху, не позбавляє особу права на спадщину [4, с. 132]. Аналогічно, особа, яка визнана винною у вчиненні умисного тяжкого тілесного ушкодження (ст. 121 КК України), внаслідок якого настала смерть потерпілого, формально не підпадає під дію ч. 1 ст. 1224 ЦК України і не усувається від права на спадкування [3, с. 9]. Ця прогалина, на думку І. О. Гелецької, потребує законодавчого усунення шляхом розширення переліку умисних злочинів, за вчинення яких особа може бути усунена від спадкування [3, с. 8-9].

Другою підставою є умисне перешкоджання спадкодавцеві скласти заповіт, внести до нього зміни або скасувати його, що сприяло виникненню права на спадкування у самого порушника чи в інших осіб або збільшенню їхньої частки у спадщині (ч. 2 ст. 1224 ЦК України) [1]. Ця підстава передбачає обов'язкове встанов-

лення причинно-наслідкового зв'язку між умисними діями спадкоємця та відповідними наслідками для спадкових прав. Прикладами таких дій можуть бути: створення перешкод у спілкуванні спадкодавця з родичами, перешкоджання наданню кваліфікованої медичної допомоги, повне відокремлення спадкодавця від спілкування з людьми тощо [3, с. 8].

Третьою підставою є позбавлення батьківських прав щодо дитини, після якої відкривається спадщина, якщо такі права не були поновлені на час відкриття спадщини (ч. 3 ст. 1224 ЦК України) [1]. Позбавлення батьківських прав є найсуворішою санкцією, що застосовується до батьків, і одним із її наслідків є втрата права на спадкування за законом, що також закріплено у ст. 166 Сімейного кодексу України [3, с. 8].

Тісно пов'язаною з попередньою є підстава ухилення від виконання обов'язку щодо утримання спадкодавця (абз. 2 ч. 3 ст. 1224 ЦК України) [1], яку необхідно розглядати у системному зв'язку зі статтями 180, 188, 198, 202, 265–271 Сімейного кодексу України. Показово, що відповідно до ст. 202 СК України обов'язок утримувати батьків виникає у повнолітніх дітей незалежно від їхнього матеріального стану та стану працездатності [3, с. 7-9].

Четвертою підставою є недійсність шлюбу між спадкодавцем та спадкоємцем (ч. 4 ст. 1224 ЦК України) [1]. Разом із тим законодавець передбачив захист добросовісного з подружжя: якщо шлюб визнано недійсним після смерті одного з них, а той, хто пережив, не знав і не міг знати про перешкоди до реєстрації шлюбу, суд може визнати за ним право на спадкування частки майна, набутого у цьому шлюбі [1].

П'ятою підставою, яку суди застосовують найчастіше на практиці, є ухилення від надання допомоги спадкодавцеві, який через похилий вік, тяжку хворобу або каліцтво перебував у безпорадному стані (ч. 5 ст. 1224 ЦК України) [1]. Верховний Суд у постанові від 01 лютого 2022 року у справі № 759/18917/17 роз'яснив, що для усунення спадкоємця від права на спадкування за цією підставою суд має встановити одночасно три обставини:

факт ухилення особи від надання допомоги за наявності можливості її надати; перебування спадкодавця у безпорадному стані; потребу спадкодавця саме в допомозі цієї особи [3, с. 7-8]. При цьому Верховний Суд у постанові від 18 жовтня 2021 року у справі № 205/4674/19 додатково наголосив, що необхідно з'ясовувати, чи зверталися спадкодавці за життя до особи з проханням про допомогу, та чи мав спадкоємець матеріальну і фізичну змогу таку допомогу надати [5]. Позбавлення права спадкувати є заходом, що має застосовуватися лише в крайньому випадку, з урахуванням передусім характеру поведінки відповідача [5].

Важливо також відмежовувати «ухилення від надання допомоги» (ч. 5 ст. 1224 ЦК України) від «ухилення від виконання обов'язку» (абз. 2 ч. 3 ст. 1224 ЦК України): ці підстави не є тотожними за змістом [3, с. 7].

Порівняльно-правовий аналіз свідчить, що подібні норми існують у законодавстві більшості країн. Наприклад, Цивільний кодекс Іспанії (ст. 756) позбавляє права на спадкування осіб, засуджених за дії проти спадкодавця або членів його сім'ї, а також повнолітніх спадкоємців, які знали про насильницьку смерть спадкодавця та не повідомили про це органам слідства [2, с. 152-153]. Законодавство Болгарії додатково передбачає усунення від спадкування особи, яка безпідставно звинуватила спадкодавця у вчиненні злочину [2, с. 153-154]. Відповідно до § 2339 Цивільного уложення Німеччини підставою для усунення є, зокрема, примушення спадкодавця шляхом обману або погрози до складання чи скасування заповіту [2, с. 154].

Таким чином, положення ст. 1224 ЦК України містять вичерпний і загалом обґрунтований перелік підстав для усунення від права на спадкування, проте окремі питання все ж потребують законодавчого вдосконалення. Зокрема, видається доцільним розширити перелік умисних злочинів у ч. 1 ст. 1224 ЦК України, включивши до нього умисне тяжке тілесне ушкодження, що спричинило смерть потерпілого [3, с. 7-9], а також доповнити перелік підстав усунення завданням тілесних ушкоджень середньої тяж-

кості або тяжких ушкоджень, що призвели до втрати працездатності, та завданням шкоди, що спричинила психічні розлади [2, с. 152-153]. Реалізація таких змін сприятиме більш ефективному захисту прав спадкодавців та справедливому розподілу спадкового майна.

ЛІТЕРАТУРА:

1. Цивільний кодекс України : Закон України від 16.01.2003 № 435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>.
2. Рубан О. О. Особливості усунення від права на спадкування за українським та європейським законодавством. *Європейські перспективи*. 2021. № 4. С. 151–155.
3. Гелецька І. О. Усунення від права на спадкування: теорія і практика застосування правових норм. *Галицькі студії*. 2023. № 1. С. 6–10.
4. Тимченко Л. М. Проблемні питання усунення від права спадкування. *Сучасні проблеми правового, економічного та соціального розвитку держави*. Харків, 2017. С. 131–133.
5. Постанова КЦС ВС від 18 жовтня 2021 року у справі № 205/4674/19.

Коцар Георгій Андрійович

*студ. 2 курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., проф. Зубар В.М.*

САМОЗАХИСТ ЯК ФОРМА ЗАХИСТУ У ЦИВІЛЬНОМУ ПРАВІ

Права і свободи людини та її інтереси є дуже важливими, і їх гарантує Конституція України. Але на жаль сучасне суспільство, так само як і в минулому, має проблеми з дотриманням прав людини, трапляються випадки коли права порушуються. Це стосується і цивільних правовідносин, бо не завжди всі учасники рівні, а договори і правила дотримуються так, як треба. Тому дуже важливо стає покладатись не тільки на зовнішні органи захисту, а і кожна людина має знати, як треба самій відстояти свої права.

Для початку доцільно розмежувати поняття самозахисту у різних галузях права, зокрема у цивільному та кримінальному з сторони держави у нормативно правових актах. У цивільному пра-

ві самозахист розглядається як можливість особи самостійно вживати певних дій для захисту своїх прав та інтересів без звернення до компетентних органів, що передбачено Цивільний кодекс України. Водночас у кримінальному праві подібний інститут проявляється у формі необхідної оборони, коли особа має право захищати себе або інших від суспільно небезпечного посягання, що закріплено у Кримінальний кодекс України. Таким чином, хоча обидва поняття пов'язані із захистом прав особи, їх правова природа, підстави застосування та межі реалізації мають суттєві відмінності, які потребують окремого аналізу.

У контексті сучасного політико-правового розвитку особливе значення має право на захист, закріплене в статті 55 Конституції України, оскільки нормальне функціонування цивільного обороту передбачає наявність ефективного механізму захисту [1]. Згідно зі статтею 19 Цивільного кодексу України, кожна особа має право на самозахист свого цивільного права та прав іншої особи від протиправних посягань [2]. Сучасна юридична наука наголошує на тому, що дієвість захисних механізмів значною мірою залежить від їх оперативності. Самозахист цивільних прав виступає як неюрисдикційна форма захисту, коли учасник правовідносин може діяти без звернення до суду або інших компетентних органів.

Інститут самозахисту є відносно новим у правовій системі України, тому він досліджувався багатьма науковцями, серед яких Є. О. Харитонов, О. О. Підпригора, О. С. Йоффе, Ю. Г. Басін, Г. А. Сverdлик та З. В. Ромовська. Основна суть самозахисту полягає у тому, що особа самостійно, власними діями, забезпечує захист своїх цивільних прав та інтересів без звернення до суду або державних органів.

Виділяють дві форми захисту: юрисдикційну та неюрисдикційну. Якщо перша здійснюється через суд або інші органи влади, то неюрисдикційна передбачає безпосередні дії самої особи. Самозахист слід розуміти не як спосіб, а як форму реалізації права, що дозволяє особі застосовувати законні засоби протидії порушенню її прав. Ознаки самозахисту включають:

1) Застосування лише у випадку наявного або триваючого порушення права;

2) Дії здійснюються без участі органів влади чи посадових осіб;

3) Неможливість позбавлення особи права на самозахист;

4) Заходи самозахисту повинні відповідати необхідним межам для припинення порушення [4, с.101-105].

Науковці зазначають, що питання щодо суб'єктів, об'єктів, заходів самозахисту, підстав його виникнення та меж застосування є дискусійними. Часто спостерігається плутанина між самозахистом, самоуправством та самосудом. Самоуправство характеризується свавільними діями особи всупереч закону чи договору, а самосуд – це протиправне застосування фізичної сили до порушника, що саме по собі є правопорушенням. На відміну від них, дії, передбачені статтею 19 ЦК, є правомірними [2].

При цьому чинне законодавство визначає, що шкода, спричинена самозахистом, не тягне відповідальності (ст.1169 ЦК), що створює певні ризики зловживання правом. Тому важливим є чітке визначення меж самозахисту, щоб він не перетворювався на порушення прав інших осіб. Право на самозахист є природним правом людини та новелою українського законодавства. Норми, що регулюють самозахист, потребують удосконалення як з теоретичної, так і з практичної точки зору.

На мою думку, дуже важливо розуміти, де закінчується самозахист і починається самоуправство або самосуд. Ці поняття іноді легко плутають.

Самоуправство – це коли людина діє на власний розсуд, всупереч закону або договору, проявляючи особисте свавілля. Такі дії не можна вважати законним самозахистом [5, с.91].

Самосуд ще більш радикальний – це коли порушника карають самостійно, застосовуючи фізичну силу або самочинні методи покарання. Людина, яка вдається до самосуду, сама стає порушником закону, тому такі дії теж не можна вважати самозахистом. На відміну від цього, дії, передбачені статтею 19 ЦК, є законними і правомірними [2].

Також важливо, що самозахист не тягне відповідальності за шкоду, заподіяну у процесі захисту, якщо вона була необхідною для припинення порушення (ст.1169 ЦК) [2]. Проте закон зараз трохи надає перевагу самозахисту, бо створює умови, коли самостійні дії людини можуть інколи переходити межу і перетворюватися на зловживання правом.

Тому важливо чітко визначати межі самозахисту. Це право дозволяє людині захищати своє цивільне право чи інтерес законними способами, не порушуючи права інших і не суперечачи моральним нормам суспільства. Самозахист – це природне право людини, новація в українському законодавстві, але його норми ще потребують уточнення, особливо щодо визначення меж допустимих дій. Аналіз наукових праць свідчить, що на сучасному етапі законодавство потребує вдосконалення як з практичної, так і з теоретичної точки зору.

ЛІТЕРАТУРА:

1. Конституція України від 28.06.1996 року № 30.
2. Цивільний кодекс України від 16.01.2003 року № 435-IV.
3. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III.
4. Харитонов Є.О., Старцев О.В. Цивільне право України. Підручник. Вид. 2, перероб. і доп. К. : Істина, 2007. 816 с.
5. Ромовська З. В. Українське цивільне право. Загальна частина. Академічний курс: підручник. Київ: Атіка, 2015. 560 с

Крупеня Вероніка Олегівна

*студ. 2 курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., проф. Зубар В.М.*

ПОРУШЕННЯ АВТОРСЬКИХ ПРАВ У СОЦІАЛЬНИХ МЕРЕЖАХ: ЦИВІЛЬНО-ПРАВОВИЙ АСПЕКТ

Сучасний розвиток цифрових технологій та соціальних мереж (Instagram, Facebook, TikTok, YouTube) радикально змінив способи створення, поширення та споживання контенту. За даними Центру спостереження ІР-офісу, щодня мільйони користувачів

завантажують фото, відео, музику та тексти без отримання дозволу правовласників, що призводить до масових порушень авторських прав [1]. З позиції цивільного права це є порушенням особистих немайнових та майнових прав суб'єктів інтелектуальної власності, яке розглядається як делікт [2, с. 154–155]. Порушенням авторського права визнається будь-яке використання твору без дозволу правовласника, крім випадків, прямо передбачених законом (вільне використання). Такі дії можуть включати відтворення, розповсюдження, публічний показ, доведення до загального відома та інші способи використання твору. Актуальність теми зумовлена необхідністю ефективного цивільно-правового захисту в умовах цифровізації, адже соціальні мережі стали основним каналом комунікації, де порушення відбуваються миттєво та часто анонімно.

Авторське право в Україні виникає автоматично з моменту створення твору в об'єктивній формі та не потребує реєстрації. Об'єктами захисту є твори науки, літератури і мистецтва, зокрема фотографії, аудіовізуальні твори, музичні композиції, тексти, комп'ютерні програми. У соціальних мережах найпоширенішими порушеннями є: незаконне відтворення та розповсюдження чужих фотографій і відео (зокрема у форматах сторіз та коротких відео), використання музики без належної ліцензії, репост контенту без зазначення автора, а також інтернет-піратство. Під останнім розуміються будь-які дії з використанням мережі Інтернет, що порушують виключні права суб'єктів авторського права [1].

Цивільно-правова відповідальність за такі порушення передбачена ст. 431 Цивільного кодексу України: порушення права інтелектуальної власності тягне відповідальність, встановлену Кодексом, іншим законом чи договором. Як цивільне правопорушення, порушення авторських прав включає такі елементи: протиправну поведінку (незаконне використання твору), шкоду (майнову або немайнову), причинний зв'язок між діями порушника та шкодою, а також вину. Українське законодавство гарантує авторам право на захист своїх інтересів. Зокрема, можливими є вимоги про визнання права, припинення порушення, відновлення становища,

що існувало до порушення, відшкодування матеріальних збитків та упущеної вигоди, стягнення доходів порушника, а також компенсації та моральної шкоди. Судова практика підтверджує, що навіть одноразове неправомірне використання контенту може бути підставою для відповідальності (наприклад, справа № 750/602/25, компенсація 6 056 грн за розміщення фото в соціальній мережі) [5].

Особливості захисту авторських прав у соціальних мережах пов'язані з процедурою «повідомлення та видалення» (notice and takedown). Правовласник може направити платформі обґрунтовану заяву про порушення, після чого відповідний контент підлягає блокуванню або видаленню протягом розумного строку [1]. Водночас соціальні мережі мають власні внутрішні правила та політики щодо захисту авторських прав, однак їх застосування не звільняє порушника від цивільно-правової відповідальності за законодавством України [4, с. 213]. Суттєвими проблемами правозастосування є складність фіксації доказів (зокрема необхідність використання скріншотів або нотаріального посвідчення веб-сторінок), анонімність користувачів, транскордонний характер правопорушень, а також недостатня правова визначеність щодо контенту, створеного із застосуванням штучного інтелекту [1; 4, с. 342–343]. Особливої уваги потребує питання правового статусу такого контенту, оскільки відсутність чіткого регулювання ускладнює визначення авторства та притягнення до відповідальності. Водночас важливим є забезпечення балансу між правами авторів і суспільними інтересами, зокрема правом на доступ до інформації, цитування, використання творів у навчальних цілях та створення похідного контенту (меми, ремікси тощо).

Науковці зазначають, що цивільно-правова відповідальність у мережі Інтернет потребує подальшого вдосконалення, зокрема шляхом гармонізації з правом Європейського Союзу (Директива ЄС про авторське право в цифровому єдиному ринку) [3, с. 160–161]. Ефективність захисту значною мірою залежить від активної позиції правовласника, який може як звернутися до суду, так і використовувати досудові механізми захисту.

Таким чином, порушення авторських прав у соціальних мережах є поширеним цивільно-правовим деліктом, що потребує комплексного підходу до захисту. Доцільним є вдосконалення механізмів ідентифікації порушників, спрощення процедури фіксації доказів та подальша адаптація національного законодавства до європейських стандартів. Це сприятиме забезпеченню ефективного захисту прав авторів та встановленню балансу інтересів у цифровому середовищі.

ЛІТЕРАТУРА:

1. Про авторське право і суміжні права: Закон України від 01.12.2022 № 2811-IX.
2. Цивільний кодекс України від 16 січня 2003 року № 435-IV.
3. Кирилюк А. В. Цивільно-правова відповідальність за порушення авторських прав у мережі Інтернет. *Актуальні проблеми держави і права*. 2014. Вип. 72. С. 154–161.
4. Колб О. С. Аспекти захисту авторського права в мережі інтернет. *Науковий вісник Ужгородського національного університету*. 2025. № 1. С. 342–213.
5. Судова практика: рішення Деснянського районного суду Чернігова від 04.12.2025 у справі № 750/602/25.

Лашин Костянтин Анатолійович

*студ. 2 курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., проф. Зубар В.М.*

ДОКАЗУВАННЯ У СПРАВАХ ПРО ВИТРЕБУВАННЯ МАЙНА З ЧУЖОГО НЕЗАКОННОГО ВОЛОДІННЯ

Для розуміння проблематики поставленого питання, вважаю за доцільним коротко пройти по Віндикації.

Віндикація є одним із найдавніших способів речово-правового захисту права власності суб'єкта, даний спосіб використовується в певному випадку, а саме коли особа є володільцем і його право власності зберігається, але суб'єкт не може його здійснювати, бо річ вибула з його користування і знаходиться на час вибуття у особи яка незаконно заволоділа, тоді вже власник подає позов,

слід зазначити, що предметом позову є індивідуально-визначена річ, що на реальний час подання існує в натурі. Відповідно до ст.387 Цивільного Кодексу України «Власник має право витребувати своє майно від особи, яка незаконно, без відповідної правової підстави заволоділа ним.»[1]. Таким чином законодавець прописує про право яке особа може захистити, а самі інструменти захисту знаходяться в Главі 3 ЦКУ в ст 16. Основною метою є відновлення становища об'єкта та повернення його до власника

Позивачами у віндикаційному позові є: фізична особа, юридична особа, держава, територіальна громада.

Слід зазначити цікавий момент стосовно віднімаційного позову, що «Водночас законодавство надає право звертатися з вимогами про витребування майна з чужого незаконного володіння не лише власникам, а й іншим особам, у яких майно власника перебувало у законному володінні за відповідною правовою підставою («титолом»).»[6, с. 229], а також слід згадати питання про добросовісного набувача, це особа яка набула майно у суб'єкта яка не мала як такого права його відторгати, однак, у добросовісного набувача специфічна позиція, тобто, в окремих випадках встановленими законодавцем закон може захистити добросовісного набувача так званім віндикаційним імунітетом, який ми можемо простежити відповідно до ч 2 ст. ст 388,389 ЦКУ, також Касаційний цивільний суд у складі Верховного Суду у постанові дає такий коментар «Завдяки «віндикаційному імунітету», який передбачений парламентом для майна проданого чи переданого в порядку виконання судового рішення, досягається охорона прав добросовісної особи, яка набула майно, що було відчужене чи передане на виконання судового рішення і стабільність цивільного обороту.»[3]

Слід пам'ятати, що віндикаційний позов входить до загальної позовної давності, а саме 3 роки, тобто, після спливу цього строку буде вже проблематично або неможливо подати віндикаційний позов.[5]

Особливості у справах про витребування майна необхідно розглядати докази у контексті загальних принципів доказування

у цивільному судочинстві успішний захист права власності шляхом віндикації можливий лише за умови доведення позивачем сукупності юридичних фактів, що утворюють предмет доказування, доказування це питання факту.

Відповідно до ст 76 Цивільного Процесуального Кодексу України «Доказами є будь-які дані, на підставі яких суд встановлює наявність або відсутність обставин (фактів), що обґрунтовують вимоги і заперечення учасників справи, та інших обставин, які мають значення для вирішення справи.»[2], такими доказами виступають: письмовими, речовими і електронними доказами, висновками експертів, показаннями свідків.

Відповідно до ч.1 ст 81 ЦПК України «Кожна сторона повинна довести ті обставини, на які вона посилається як на підставу своїх вимог або заперечень, крім випадків, встановлених цим Кодексом.»[2] Тобто у справах обов'язок на доказ покладається на позивача.

Предметом доказування є: Наявність у позивача права власності на дане майно, фактичне вибуття з володіння особи позивача, факт незаконного привласнення майна відповідачем в момент звернення до суду, наявність вираження індивідуальної-речі.

Для підтвердження права власності позивач має надати суду правовстановлюючі документи, одну з ключових ролей відіграє постулат реєстраційного підтвердження володіння цього майна.

Велика Палата Верховного Суду «Відомості державного реєстру прав на нерухомість презюмуються правильними, доки не доведено протилежне, тобто державна реєстрація права за певною особою не є безспірним підтвердженням наявності в цієї особи права, але створює спростовувану презумпцію права такої особи»[4] правовстановлюючі документи, витяги з реєстрів. До прикладу, витяг з Державний реєстр речових прав на нерухоме майно або з Єдиного державного реєстру транспортних засобів може підтвердити, чи перебуває майно за держреєстрацією на позивачі чи відповідачі, для рухомих речей такими доказами є технічні паспорти, реєстраційні документи на транспортні засоби, договори тощо.

Розвиток нового століття створює нові можливості та виклики цифрових технологій зростає значення електронних доказів, що фіксують факт перебування майна у відповідача, користування ним, вчинення дій щодо майна так можна ще в категорію доказів ввести фото-відео фіксація факту перебування майна у відповідача або вчинення конкретних дій відповідача.

Важливу роль у доказовій базі створюють свідки: сусіди, колишніх співробітників, знайомих або експертів, а вони, можуть свідчити про обставини появи майна у володінні відповідача. До прикладу, сусіди можуть підтвердити, що будинок та\або автомобіль давно належить позивачу, а потім «проданий без дозволу та участі власника». Нотаріус як свідок може підтвердити факт чинності чи недійсності правочину, який став підставою набуття майна.

Важливим елементом доказів є клопотання про огляд доказів за їх місцезнаходженням відповідно до ЦПК України статті 84, припустимо, що об'єкт знаходиться у відповідача і дана процедура, допомагає посвідчити факт дійсного знаходження майна у власності відповідача, так-то треба конкретика який саме доказ, обставини і підстави релевантності даного доказу, а також створює заборону на відчужування на підставі статті 150 ЦПК України.

Кожен з вищезазначених доказів має бути послідовно засвідченим та відповідати дійсності, бо інакше вони будуть нікчемними та їх юридична сила втратить всяку значимість у справі з приводу віндикації.

Виходячи з вищепереліченого види доказів є різноманітними та дає простір для сильної доказової бази в суді, кожен з яких має специфічне значення для підтвердження окремих важливих фактів предмету доказування залежно від обставин справи, а сам збір доказів має бути послідовним та систематизованим з чіткою стратегією та розумінням свої подальших дій.

Основним завданням позивача є доведення права власності на майно, факту його вибуття з володіння власника, перебування майна у відповідача та індивідуальної визначеності речі.

Судова практика Верховного Суду відіграє важливу роль у формуванні підходів до визначення предмета доказування у справах цієї категорії.

Належне визначення предмета доказування та правильне застосування норм цивільного та цивільного процесуального законодавства є необхідною умовою ефективного захисту права власності.

ЛІТЕРАТУРА:

1. Цивільний кодекс України : Закон України від 16.01.2003 № 435-IV. *Відомості Верховної Ради України*. 2003. № 40-44. Ст. 356.
2. Цивільний процесуальний кодекс України : Закон України від 18 березня 2004 р. № 1618-IV. *Відомості Верховної Ради України*. 2004. № 40–41, № 42. Ст. 492.
3. Віндикація та імунітет права власності : презентаційні матеріали Верховного Суду. Київ : Верховний Суд, 2025. 28 с.
4. Власов Ю.Л. Віндикаційний та негативний позови у практиці Верховного Суду : презентаційні матеріали. Київ : Верховний Суд, 2023. 32 с.
5. Крат В.І. Строки. Позовна давність: практика Верховного Суду: презентаційні матеріали. Київ : Верховний Суд, 2022. 35 с.
6. Дзера І.О. Захист права власності, віндикаційний позов. *Велика українська юридична енциклопедія*. Харків: Право, 2023. Т. 9. С. 228–231.

Лук'яненко Валерія Станіславівна

*студ. 2 курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., проф. Зубар В.М.*

ОПІКА ТА ПІКЛУВАННЯ В УКРАЇНІ: ПРАВОВА БАЗА ЧИ РЕАЛЬНА ДОПОМОГА ПІДОПІЧНИМ?

Інститут опіки та піклування виступає одним із основних інструментів, що забезпечують захист прав людей, які через свій вік, стан здоров'я або психофізичні особливості не можуть самостійно повною мірою реалізовувати власні права та інтереси [1]. В Україні ця сфера регулюється Цивільним кодексом, Сімейним кодексом та підзаконними актами, які визначають порядок встановлення опіки й піклування, а також права та обов'язки опікунів і піклувальників [2].

Актуальність теми зумовлена сучасними викликами у сфері захисту прав людини та потребою оцінити ефективність існуючих законодавчих механізмів на практиці. Попри чітке нормативно-правове регулювання, наявний розрив між прописаними положеннями та фактичною підтримкою осіб під опікою ставить під сумнів реальність забезпечення їхніх прав. Саме тому дослідження взаємозв'язку між правовою базою і реальною допомогою має важливе значення – як для наукових досліджень, так і для практичного розвитку правової та соціальної роботи [4].

Опіка та піклування є видами юридичного представництва для осіб, які частково або повністю позбавлені дієздатності. Відповідно до положень Цивільного кодексу України [2]:

Опіка встановлюється для малолітніх осіб, а також для тих, кого суд визнав недієздатними. Опікун відповідає за фізичне, психологічне та соціальне благополуччя підопічного, а також за належне управління його майном.

Піклування передбачає опіку над неповнолітніми та обмежено дієздатними особами, які частково можуть здійснювати свої права, але потребують підтримки при прийнятті юридично значущих рішень [5].

Основне призначення інституту полягає в забезпеченні балансу між захистом підопічного і збереженням його особистої автономії. Важливим аспектом сучасної практики є не лише формальне представництво, а й надання можливості підопічному брати участь у прийнятті рішень, які стосуються його життя та майна [6].

Державне регулювання здійснюється через органи опіки та піклування при органах місцевого самоврядування, під координацією Міністерство соціальної політики України [7].

Основними функціями органів опіки є:

- установа опіки та піклування над особами, які цього потребують;
- здійснення нагляду за діяльністю опікунів і піклувальників;

- захист майнових і немайнових прав осіб, які перебувають під опікою;
- участь у судових процесах, спрямованих на захист інтересів підопічних.

Держава виконує роль не лише регулятора, але й гаранта дотримання прав соціально вразливих категорій населення. Однак ефективність цього механізму нерідко обмежується недостатністю фінансових та людських ресурсів, низьким рівнем підготовки спеціалістів і впливом бюрократичних бар'єрів. Ці фактори створюють можливі загрози для забезпечення прав і інтересів осіб, що перебувають під опікою [8].

Ключовим елементом ефективності інституту є тристороння взаємодія:

Держава та опікун визначають рамки функціонування, здійснюють контроль над діяльністю і встановлюють обмеження щодо розпорядження майном, яке належить підопічному [7].

Опікун у співпраці з підопічним забезпечує повсякденний догляд, представляє його інтереси у правових аспектах та приймає рішення, що стосуються освіти, медичного забезпечення та майнових питань [5].

Держава разом із підопічним гарантує реалізацію прав через законодавчі механізми, а також надає соціальні й юридичні послуги.

Однак ключова проблема полягає в тому, що підопічного часто позбавляють реальної можливості впливати на процес прийняття рішень. Це суперечить сучасним стандартам прав людини і принципам Конвенції ООН про права осіб з інвалідністю [9].

Незважаючи на існування детальної нормативної бази, в реальному житті виникають наступні проблеми:

- Формальний характер контролю з боку державних органів, що не забезпечує належного нагляду за діяльністю опікунів.
- Обмежена свобода дій підопічних, зокрема тих, хто здатен частково приймати рішення самостійно.

- Ризик неправомірного використання майна підопічних через недостатність суворого контролю.
- Брак професійної підготовки опікунів та відсутність необхідної психологічної підтримки для підопічних.

Дані фактори вказують на існування розриву між встановленими правовими нормами та фактичною реалізацією захисту прав людини. Сучасні європейські та міжнародні стандарти, зокрема рекомендації Організації Об'єднаних Націй, пропонують поступовий перехід від моделі повного представництва до моделі підтриманого прийняття рішень.

Цей підхід передбачає максимальне залучення особи, яка потребує підтримки, до процесу ухвалення рішень, з акцентом на збереження її автономії, забезпечення права на власний голос, а також надання необхідної консультативної та правової допомоги.

Для запровадження цих стандартів в Україні необхідно здійснити реформування законодавства та модернізувати існуючу систему моніторингу і контролю.

Інститут опіки та піклування в Україні має досить розвинену нормативно-правову базу, проте його ефективність залишається обмеженою через розрив між законодавчими положеннями та практичною підтримкою.

Основними проблемами є слабкий контроль за діяльністю опікунів, обмежена автономія підопічних, а також існування ризику зловживань з боку державних органів. Перспективним шляхом розвитку цього інституту може стати впровадження міжнародних стандартів щодо підтриманого прийняття рішень, що передбачає забезпечення дійсної допомоги для підопічних. Це вимагає посилення контролю за діяльністю опікунів, покращення їх професійної підготовки та надання їм психологічної підтримки, а також активного залучення підопічних до процесу ухвалення рішень. Інститут опіки в Україні має значний потенціал для перетворення на дієвий механізм захисту прав людини, але для цього необхідні комплексні реформи та адаптація до сучасних підходів у галузі прав людини та соціальної роботи.

ЛІТЕРАТУРА

1. Головка О.І. Соціально-правовий захист неповнолітніх та осіб з обмеженою дієздатністю в Україні. *Юридична думка*. 2019..
2. Цивільний кодекс України. *Верховна Рада України*. 2003. Ст. 315–330.
3. Сидоренко В.М. Проблеми реалізації опіки та піклування в сучасній Україні. *Соціальні студії*. 2020. № 2. С. 12–22.
4. Коваленко Т.В. Інститут опіки та піклування: правова та соціальна перспектива. *Право і суспільство*. 2018. № 4. С. 67-75.
5. Климчук О.С. Юридичне представництво осіб з обмеженою дієздатністю. *Права людини*. 2021. С. 58.
6. Петрова Н.В. Автономія підопічного та інститут опіки в Україні. *Науковий вісник*. 2019. № 6. С. 44–53.
7. Міністерство соціальної політики України. Організація опіки та піклування. Київ, 2022.
8. Шевченко І.П. Соціальний нагляд за правами підопічних: проблеми та перспективи. *Соціальна робота*. 2018. № 2. С. 33–42.
9. United Nations. Convention on the Rights of Persons with Disabilities. New York, 2006. 28 p., p. 12.

Мазниця Дарина Сергіївна

*студ. 2 курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., проф. Зубар В.М.*

ПОНЯТТЯ ТА ВИДИ ЦИФРОВИХ РЕЧЕЙ

З приходом нових технологій, в світі стрімко з'являються інформаційні технології, та формується нова категорія в праві – цифрові речі, без яких жодна людина в сьогоденні не може обійтись. Їх виникнення зумовлене цифровізацією суспільних відносин та розвитком віртуального простору, що спричиняє потребу правового регулювання подібних об'єктів.

Предметами є – речі, гроші, цінні папери, майнові права, результати робіт, послуги, також матеріальні й нематеріальні блага [1, ст 177 ЦКУ]. Цифрові речі закріплені в ЦКУ, і вони можуть сприйматися як різновид нематеріальних благ або як окрема група цивільних прав, що існують у цифровому просторі та мають економічну вартість.

Цифрові речі – це благо, що твориться та живе виключно у цифровому середовищі та має майнову вартість [2, ст 179-1 ЦКУ].

Віртуальними об'єктами є цифрові активи, цифровий контент та інші цінності, стосовно яких діють положення частини першої цього тексту. У ЄС чітке й уніфіковане визначення «digital thing» або «digital object» – відсутнє. В юридичних документах ЄС частіше вживаються терміни на кшталт «digital content» (цифровий вміст) та «digital service» (цифрова служба), зокрема у Директиві (ЄС) 2019/770 про договори надання цифрового вмісту та цифрових послуг. [3, с. 38].

Нормативне врегулювання цифрових об'єктів частково здійснюється крізь приписи, що стосуються відомостей [ЗУ «Про інформацію», електронних паперів [ЗУ «Про електронні документи та електронний документообіг»] та віртуальних активів [ЗУ «Про віртуальні активи»]. Згідно з нормами цього закону, віртуальний актив тлумачиться як не фізичне благо, що є предметом цивільних прав та має цінність.

Види цифрових речей класифікують за такими ознаками:

- віртуальні активи
- цифровий контент

Цифровий контент є об'єктом права інтелектуальної власності, а отже підпадає під дію ст. 433 ЦК України, ЗУ «Про авторське право і суміжні права».

По правовому статусу цифрові об'єкти можна розділити на ті, що знаходяться у володінні особи (наприклад, віртуальні активи), та ті, що надаються в оренду на підставі дозволу (наприклад, електронний контент у потокових сервісах).

За методом обігу виділяють обертові цифрові речі, які можуть безперешкодно передаватися, та з обмеженим обігом, застосування яких підпорядковується особливим нормам чи умовам платформи.

Правовий уклад цифрових предметів передбачає, що власник цифрового доробку має право на його застосування, розпорядження та переказ, проте зобов'язаний додержуватись припи-

сів платформи, ліцензійних угод та законодавчих засад. Також законодавство передбачає змогу тимчасового звуження доступу до цифрових доробок у разі недотримання умов вжитку або задля оберегу прав інших сторін.

На мою думку, цифрові активи вимагають чіткого та системного закріплення в цивільному законодавстві України як окремої категорії суб'єктів цивільних прав. Їх правова природа не може цілком ототожнюватися ані з традиційними предметами, ані винятково з нематеріальними благами, адже вони містять риси обох: з одного боку – відсутність фізичної форми, а з іншого – здатність до економічного обігу, відчуження та володіння.

Тому цифрові предмети є відносно новим, проте надзвичайно значущим розрядом цивільних правооб'єктів, виникнення якого спричинене швидким прогресом інформаційних технологій та діджиталізацією суспільства. Попри відсутність їх чіткої фіксації в актуальному законодавстві України, вони вже фактично займають істотне місце у цивільному обігу та мають фінансову вартість.

Розгляд національних та європейських поглядів вказує на уривчастість правового упорядкування цифрових об'єктів, що вимагає їхньої уніфікації та нормативного доопрацювання. З'ясування юридичної сутності цифрових речей, їх категоризація та визначення особливостей правового статусу є ключовими кроками для гарантування дієвого захисту інтересів суб'єктів цивільних взаємин.

ЛІТЕРАТУРА

1. Цивільний кодекс України : Закон України від 16.01.2003 № 435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>^{[P]_{SEP}}
2. Цивільний кодекс України. Станом на 01 січня 2023 р.: наук.-практ. Коментар. За заг. ред. проф. Харитонova Є.О., доц. Калітенко О.М. Київ: Норма права, 2023. 1424 с.^{[P]_{SEP}}
3. Савчин Р.В. Поняття та ознаки цифрових речей. URL: <https://previous.scientia.report/index.php/archive/article/download/2980/3012>
4. Директива (ЄС) 2019/770 Європейського парламенту і Ради від 20 травня 2019 року про договори надання цифрового контенту та цифрових послуг.
5. Про інформацію: Закон України від 02.10.1992 № 2657-XII. Відомості Верховної Ради України. № 48. Ст. 28.

6. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. URL: <https://zakon.rada.gov.ua/laws/show/851-15>

7. Про віртуальні активи: Закон України від 17 лютого 2022 року № 2074-IX. URL: <https://zakon.rada.gov.ua/laws/show/2074-20>

Мінько Ірина Василівна

*студ. 2 курсу факультету прокуратури та слідства
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., доц. Калітенко О.М.*

ЦИВІЛЬНО-ПРАВОВІ АСПЕКТИ ЗАХИСТУ ПРИВАТНОСТІ В УМОВАХ ЦИФРОВІЗАЦІЇ СУСПІЛЬСТВА

Актуальність теми дослідження зумовлена стрімким розвитком цифрових технологій та активним впровадженням електронних сервісів у всі сфери суспільного життя. У таких умовах питання захисту приватності набуває особливого значення, оскільки персональні дані особи стають об'єктом широкого обігу. Цифровізація сприяє підвищенню ефективності управління та комунікацій, однак водночас створює нові ризики порушення права на приватне життя. Особливо актуальним є питання забезпечення цивільно-правового захисту особи від незаконного втручання у її приватну сферу. Недостатність правових механізмів та складність їх реалізації у цифровому середовищі обумовлюють необхідність наукового дослідження цієї проблематики. Саме тому аналіз цивільно-правових аспектів захисту приватності в умовах цифровізації суспільства є важливим і своєчасним.

В міру розвитку цифрових трансформацій зростає значення цивільно-правового захисту приватності особи, виникають і розвиваються нові форми втручання у приватне життя, що потребують удосконалення правових механізмів їх регулювання та захисту (1 абзац тексту) [1]. Кузьменко О.В. у своєму дослідженні зазначила, що використання електронних реєстрів та цифрових сервісів у сфері сімейних правовідносин супроводжується ризиками порушення конфіденційності персональних даних дітей і батьків [1]. Автор наголошує, що неналежний рівень захисту ін-

формації може призвести до її несанкціонованого поширення, що негативно впливає на реалізацію права на приватність.

Степаненко Н.В. та Величко Д.С. у своєму дослідженні розглянули судові способи захисту права на особисте життя та зазначили, що цивільне законодавство України передбачає можливість відшкодування моральної шкоди, спростування недостовірної інформації та припинення дій, що порушують право на приватність [2]. Автори підкреслюють, що судовий захист є ключовим механізмом відновлення порушених прав, однак його ефективність залежить від належного доказування та правозастосовної практики.

Коломоєць Ю.О. у своєму дослідженні зазначив, що цифровізація системи публічного управління створює як нові можливості, так і ризики для забезпечення прав і свобод людини [3]. Автор вважає, що обробка великих масивів даних державними органами потребує чітких правових гарантій захисту персональної інформації, оскільки існує загроза її зловживання або витоку. Це актуалізує необхідність удосконалення цивільно-правових механізмів захисту приватності.

Вавженчук С.Я. у своєму дослідженні розглянув проблеми цивільно-правового захисту права на зображення особи та зазначив, що в умовах цифровізації особливої актуальності набуває питання використання зображень без згоди особи [4]. Автор підкреслює, що поширення фотографій та відео у мережі Інтернет без дозволу може порушувати особисті немайнові права та потребує належного правового реагування.

Малюга Л.Ю. та Шкрібляк К.П. у своєму дослідженні вважають, що захист персональних даних у процесі цифровізації трудових відносин є важливою складовою забезпечення права на приватність [5]. Автори зазначають, що роботодавці повинні дотримуватися принципів законності, пропорційності та конфіденційності при обробці даних працівників. Це сприяє формуванню належного рівня захисту прав особи у цифровому середовищі.

Таким чином, цивільно-правовий захист приватності в умовах цифровізації суспільства потребує комплексного підходу, що

включає вдосконалення законодавства, розвиток судової практики та підвищення правової культури учасників правовідносин [1–5].

Захист приватності в умовах цифровізації є одним із ключових завдань сучасного цивільного права. Розвиток цифрових технологій створює нові виклики для забезпечення особистих немайнових прав. Існуючі правові механізми потребують адаптації до умов цифрового середовища. Важливим є поєднання правових, технічних та організаційних заходів захисту. Подальший розвиток цивільно-правового регулювання сприятиме ефективнішому забезпеченню права на приватність.

ЛІТЕРАТУРА:

1. Кузьменко О.В. Електронні реєстри та цифрові сервіси у сфері сімейних правовідносин: проблеми захисту персональних даних дітей і батьків. URL: <https://journal-app.uzhnu.edu.ua/article/view/352607/339318>
2. Степаненко Н.В., Величко Д.С. Судові способи захисту права на особисте життя в цивільному праві України. URL: <https://ppdnz.com.ua/index.php/home/article/view/510/408>
3. Коломоєць Ю.О. Проблеми забезпечення прав і свобод людини в умовах цифровізації системи публічного управління. URL: <https://dspace.dsau.dp.ua/server/api/core/bitstreams/98e8e5e8-efe6-42d7-8130-554b3579e087/content>
4. Вавженчук С.Я. Проблеми цивільно-правового захисту права на зображення пацієнта в умовах цифровізації системи охорони здоров'я. URL: <https://pravo.cusu.edu.ua/index.php/pravo/article/view/625/651>
5. Малюга Л.Ю., Шкрібляк К.П. Особливості захисту персональних даних у процесі цифровізації трудових відносин: теоретико-правовий аналіз. URL: <https://visnyk-pravo.uzhnu.edu.ua/article/view/343816/331603>

Носалюк Данійл Артемович

*студ. 2 курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., проф. Зубар В.М.*

РЕЧІ ЯК ОСНОВНИЙ ОБ'ЄКТ ЦИВІЛЬНИХ ПРАВ

Категорія «об'єкт цивільних правовідносин» виступає ключовим елементом у структурі цивільних правовідносин. У науковій літературі з цивільного права існує кілька підходів до визначення цього поняття. Згідно з першим підходом, об'єктом цивільних

прав вважається те, на що спрямовані права та обов'язки учасників цивільних правовідносин. Другий підхід передбачає, що об'єктом є те, з приводу чого виникають такі правовідносини. Третій підхід акцентує увагу на тому, що об'єкт – це те, на що можна безпосередньо впливати. У сучасній юридичній доктрині більшість фахівців у галузі права визначають об'єкт цивільних прав за допомогою терміна «благо». Цей підхід пояснюється тим, що сфера цивільного права охоплює не лише матеріальні цінності, а й такі нематеріальні, як честь, гідність, інформація, а також результати інтелектуальної та творчої діяльності.

Згідно з дослідженнями у галузі римського приватного права, можна зробити висновок, що в античному римському суспільстві речі (*res*) розглядалося як єдиний елемент усіх цивільних правовідносин.

Річ (*res*) – це елемент природи, незалежно від того, чи вона жива або нежива, який може бути просторово або фізично відокремлений, або залишатися нерозривно пов'язаним з іншими частинами природи, і водночас виступати об'єктом юридичного володіння особи. Такий елемент природи може бути відокремленим (наприклад, раби, будівля), або ж залишатися невіддільним від навколишнього середовища (наприклад, вода, земельна ділянка чи ліси). При цьому не має значення, чи є природа живою чи неживою. У римському праві речами вважалося все, що оточувало людину, могло бути предметом речового права та мало певну цінність. Однак наявність цих ознак не була обов'язковою для того, щоб певний об'єкт визнавався річчю.

Слід підкреслити, що всі речі поділялися на дві основні групи: речі, які належали до сакрального права, і ті, що належали до людського права. Речі людського права, у свою чергу, класифікувалися на приватні та публічні. Важливо зазначити, що певні речі у римському праві – так звані публічні речі – не могли бути об'єктами приватного права чи предметом договорів. Такі речі вважалися вилученими з цивільного обігу і позначалися терміном *res extra commercium*. На противагу їм, існували речі, які не були вилучені з обігу, і їх найменували обороздатними (*res in commercio*).

У правовій системі Стародавнього Риму норми приватного права охоплювали виключно майнові відносини, які, як відомо, стосуються об'єктів власності. Проте сам термін «майно» не був знайомий римському приватному праву. Його роль виконував термін «річ» (res). Виходячи з цього, можна зробити висновок, що поняття «річ» (res) у римському приватному праві відповідає сучасному терміну «майно» в українському цивільному законодавстві [3, с.75].

Законодавець дав визначення поняття речей у ст. 177 ЦКУ, згідно з яким «річчю є предмет матеріального світу, щодо якого можуть виникати цивільні права та обов'язки» [1]. Предметом цивільно-правових договорів є речі, які мають велике значення не лише через свої фізичні властивості, але й через здатність задовольняти потреби учасників цивільного обороту. Правові норми враховують цю особливість, надаючи можливість одній стороні вимагати від іншої виконання чи утримання від певних дій щодо конкретних речей. До таких речей належать також види енергії, оскільки вони є матеріальними благами, які можуть забезпечувати майнові інтереси учасників цивільних правовідносин.

Правовий режим речей є ключовою основою для їх класифікації, що дозволяє визначити обсяг і зміст прав та обов'язків учасників цивільних правовідносин. Якщо брати до уваги особливості правового режиму окремих речей або їх груп, а також інших критеріїв, відбувається поділ речей на різні категорії.

Відповідно до ст. 181 ЦК речі поділяються на нерухомі та рухомі. Як зазначається у частині 1 цієї статті «до нерухомих речей (нерухоме майно, нерухомість) належать земельні ділянки, а також об'єкти, розташовані на земельній ділянці, переміщення яких є неможливим без їх знецінення та зміни їх призначення.» [1]. Також «режим нерухомої речі може бути поширений законом на повітряні та морські судна, судна внутрішнього плавання, космічні об'єкти, а також інші речі, права на які підлягають державній реєстрації.» [1].

Під час аналізу чинного цивільного законодавства можна дійти висновку, що публічний характер режиму нерухомого май-

на закріпленій у Цивільному кодексі України. Так, відповідно до «ст. 182 ЦК України право власності та інші речові права на нерухомі речі, обмеження цих прав, їх виникнення, перехід і припинення підлягають державній реєстрації» [1]. Так, у ст. 5 Закону України «Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень» визначені об'єкти, які підлягають під державну реєстрацію: «житлові будинки, будівлі, споруди, а також їх окремі частини, квартири, житлові та нежитлові приміщення, земельні ділянки»[2]. Стосовно рухомих речей, то це ті, які можна вільно переміщувати у просторі, як зазначається у ч.2 ст. 181 ЦК. Рухомим майном є речі, такі як гроші та цінні папери, які не належать до категорії нерухомість згідно з Цивільним кодексом та іншими законами.

Наступний поділ речей це подільні і неподільні. Значення цих видів речей закріплено у ст. 183 ЦК, відповідно до якої подільні це речі, які можна поділити без втрати їхньої первісної функціональності, призначення. До таких можна віднести продукти харчування, нафта, вода та ін. До неподільних належать такі складні речі, що складаються з окремих самостійних предметів, об'єднаних спільним призначенням. Тобто, у разі поділу вони не матимуть того ж призначення, яке мали до поділу. Це можуть бути витвори мистецтва, до прикладу картини або скульптури, також меблі, техніка(телевізор, телефон).

Класифікація речей на подільні та неподільні має юридичне значення як у правовідносинах власності, так і в зобов'язальних правовідносинах. При розподілі майна, яке перебуває у спільній власності, неподільна річ не може бути розділена фізично. Замість цього така річ може бути продана, а отримані гроші будуть розподілені між власниками. Альтернативно, вона може залишитися у власності одного з них, при умові надання відповідної грошової або іншої компенсації іншим учасникам спільної власності.

Також, як зазначено у ст. 184 ЦК, є речі, визначені індивідуальними ознаками або родовими. Речі, визначені індивідуальними ознаками, характеризуються унікальними властивостями, які дозволяють їх розрізняти серед інших подібних і несхожих речей(кар-

тина «Мона Ліза»). Такі речі є незамінними, тому їхнє випадкове знищення звільняє боржника від обов'язку передачі їх уповноваженій особі. Тоді як, речі, визначені родовими ознаками, можуть бути замінені іншими речами того ж типу, оскільки вони мають спільні характеристики і можуть бути виміряні кількістю, вагою чи мірою (різні крупы, картопля та ін.). Ця особливість підкреслюється виразом давньоримських юристів «*Generis non pereunt*», яка означає, що речі родового типу не зникають, оскільки можуть бути замінені іншими подібними речами того ж роду.

Далі, відповідно до ст. 185 Цивільного кодексу України є речі споживні і неспоживні. Споживні речі це ті, які під час використання втрачають свою фізичну сутність повністю або частково або трансформуються в інший продукт (наприклад, приготування тістечка з борошна). Однак їх не слід плутати з предметами споживання, які призначені для задоволення споживчих потреб. З іншого боку, неспоживні речі це ті, які під час використання поступово втрачають свої споживчі властивості протягом довгого періоду часу (наприклад, технічне обладнання). Інакше кажучи, неспоживні речі призначені для багаторазового використання і зберігають свій первісний вигляд протягом тривалого часу.

Варто наостанок зазначити про такі категорії, як продукція, плоди та доходи. Відповідно до статті 189 Цивільного Кодексу, під продукцією, плодами та доходами розуміється будь-яка річ, яка створюється, добувається або одержується з неї. Ця норма не містить конкретних ознак цих понять, які частково визначаються цивілістичною доктриною. Продукцією вважається все, що виникає внаслідок господарської діяльності та матеріалізується у вигляді нової речі (наприклад, виробництво машин, спорудження будинків, переробка нафти на бензин). Плоди являють собою результат органічного розвитку самої речі (наприклад, приплід худоби, урожай). Доходи включають усе, що річ приносить під час визискування та цивільного обороту, наприклад, плата за оренду.

Відповідно до частини 2 статті 189 Цивільного кодексу України «продукція, плоди і доходи належать власникові речі, якщо інше не встановлено законом чи окремим договором між власни-

ком і іншою особою» [1]. Ця норма має диспозитивний характер, що дозволяє сторонам домовлятися про інші умови в договорах, наприклад, у договорі застави можна передбачити, що плоди та приплід тварин залишаються у заставодержателя та будуть зараховані як виконання зобов'язання.

Отже, об'єкти цивільних правовідносин є ключовим елементом цивільного права, що охоплює як матеріальні, так і нематеріальні блага. Історично поняття «речі» у римському праві стало фундаментом для сучасного розуміння майна. У Цивільному кодексі України речі отримали чітке визначення та багаторівневу класифікацію (нерухомі й рухомі, подільні й неподільні, індивідуально визначені й родові, споживні й неспоживні), що дозволяє ефективно врегульовувати цивільний оборот. Таким чином, сучасне право, спираючись на римську традицію, забезпечує системний підхід до визначення та використання речей як основних об'єктів цивільних правовідносин.

ЛІТЕРАТУРА:

1. Цивільний кодекс України : Закон України від 16 січня 2003 р. № 435-IV. *Відомості Верховної Ради України*. 2003. № 40–44. Ст. 356.
2. Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень : Закон України від 01.07.2004 № 1952-IV. *Відомості Верховної Ради України*. 2004. № 51. Ст. 553.
3. Основи римського приватного права: Підручник. За заг. ред. В. І. Борисової та Л. М. Баранової. Х.: Право, 2008. 224 с.
4. Цивільне право. Загальна частина: навчальний посібник. Харків: ХНУВС, 2022. 332 с

Одинська Юлія Дмитрівна

*студ. 2 курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: д.ю.н., проф. Харитонов Є.О.*

ЗАПОВІТ ЯК ОДНОСТОРОННІЙ ПРАВОЧИН

Заповіт є ключовим елементом спадкового права та одним із основних способів розпорядження майном у разі смерті. Його важливість полягає в тому, що він надає особі можливість самостійно вирішувати подальшу долю свого майна після смерті, що

сприяє реалізації принципу свободи волі, закріпленого в цивільному праві.

Відповідно до Цивільного кодексу України, заповіт є особистим розпорядженням фізичної особи на випадок її смерті [1, ст. 1233]. Таке визначення підкреслює, що заповіт представляє собою акт волевиявлення конкретної людини, який спрямований на визначення правових наслідків у майбутньому. Він займає важливе місце у системі цивільного права, оскільки регулює відносини, що стосуються переходу прав і обов'язків після смерті особи.

Особливо важливо зосередитися на питанні, чому заповіт класифікується як односторонній правочин. Це обумовлено його юридичною природою та специфікою формування волевиявлення. Одностороннім правочином вважається дія, для здійснення якої достатньо волі лише однієї особи[1, ст. 202]. Така характеристика повністю відповідає складанню заповіту, де рішення ухвалюється виключно однією стороною.

Перш за все, заповіт складається виключно за бажанням заповідача. Жодна інша особа не може брати участь у визначенні його змісту або впливати на прийняття відповідного рішення. Саме заповідач вирішує, хто стане спадкоємцем, який обсяг майна буде передано, а також встановлює всі інші умови [3]. Таким чином, його волевиявлення має одноосібний характер і не потребує узгодження з будь-якими іншими особами.

По-друге, для чинності заповіту не потрібна згода спадкоємців або будь-яких інших осіб [1, ст. 1236]. Вони можуть навіть не здогадуватися про його існування аж до моменту відкриття спадщини. Проте після смерті заповідача в них автоматично виникають відповідні права та зобов'язання. Це відображає головну особливість одностороннього правочину, адже правові наслідки виникають незалежно від бажання чи волі інших учасників.

По-третє, заповіт має суто особистий характер [1, ст.1234]. Його не можна укласти через представника, що вкотре підкреслює односторонню природу цього акту. У такому разі воля заповідача повинна бути висловлена безпосередньо, що забезпечує її автентичність і добровільність.

Також слід зазначити, що однією з ключових характеристик заповіту є його здатність до вільної зміни або скасування. Заповідач зберігає право в будь-який час змінити зміст документа або повністю анулювати його, не потребуючи при цьому схвалення з боку інших осіб [1, ст.1254]. Ця особливість підкреслює односторонній характер заповіту, що базується виключно на волевиявленні однієї сторони.

Розглядаючи заповіт як односторонній правочин, слід не лише виокремити його характерні ознаки, але й проаналізувати їх практичне застосування. Завдяки своїм унікальним властивостям заповіт займає окреме місце серед інших правочинів у межах цивільного права.

Однією з фундаментальних особливостей заповіту є його відкладений правовий наслідок. На відміну від переважної більшості інших правочинів, юридичні наслідки заповіту не настають безпосередньо після його складання. Заповіт набирає чинності лише після смерті особи, яка його склала, що забезпечує його особливу роль у системі правового регулювання [2]. До моменту смерті заповідача цей правочин фактично не викликає змін у правовому статусі інших осіб, чим підкреслюється його специфічний характер як засобу правового регулювання.

Однією з ключових особливостей є нестабільність заповіту до моменту відкриття спадщини. Заповідач має право необмежено змінювати або скасовувати свій заповіт стільки разів, скільки вважає за потрібне. При цьому кожен новий заповіт може як повністю, так і частково змінювати чи замінювати попередній [4]. Це лише підкреслює, що даний правочин цілком залежить від волевиявлення однієї особи.

На практиці це означає, що навіть за умови знання спадкоємцями про існування заповіту, вони не можуть бути впевнені у його остаточному змісті до моменту смерті заповідача. Така ситуація створює певну правову невизначеність, яка властива саме заповітам як одностороннім правочинам.

Також варто приділити увагу формі заповіту та її значущості. У цьому випадку форма виконує як формальну функцію, так і за-

безпечує захист інтересів заповідача. Наявність письмової форми та нотаріального посвідчення дає змогу підтвердити справжність волевиявлення і запобігти можливим подальшим конфліктним ситуаціям. Саме через це недотримання встановлених вимог до форми стає однією з найпоширеніших підстав для визнання заповіту недійсним [4].

Важливе практичне значення має також зміст заповіту. Заповідач отримує можливість не лише визначити спадкоємців, але й додатково висунути певні розпорядження: наприклад, покласти на спадкоємців конкретні обов'язки чи створити певні умови отримання спадщини [2, с. 576]. Це підкреслює, що заповіт є універсальним правовим інструментом, який дозволяє максимально точно реалізувати волю особи.

Разом з тим, варто також зазначити щодо одного з ключових аспектів спадкового права – обмеження свободи заповіту. Хоча заповідач має повне право самостійно розпоряджатися своїм майном, ця свобода не є необмеженою. Законодавство передбачає особливі гарантії для певних категорій осіб, які не можуть бути повністю позбавлені спадщини навіть за умов існування заповіту. Йдеться насамперед про тих, хто має право на обов'язкову частку у спадщині. Це означає, що навіть у разі відсутності згадки про таких осіб у заповіті або прямого позбавлення їх права на спадщину, вони все одно мають законне право на отримання певної частини майна [2, с. 568].

Таке регулювання з боку держави спрямоване на захист найбільш соціально вразливих категорій громадян, наприклад, неповнолітніх дітей чи непрацездатних членів родини. З точки зору практики, це виглядає так: людина може скласти заповіт, у якому передасть усе своє майно іншій особі, наприклад, другові або знайомому. Проте після її смерті частина цього майна обов'язково має бути виділена тим, хто володіє правом на обов'язкову частку. Подібні ситуації нерідко стають причиною спадкових конфліктів, адже фактичний розподіл майна може значно відрізнитися від початкового бажання заповідача.

ЛІТЕРАТУРА:

1. Цивільний кодекс України : Закон України від 16.01.2003 № 435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>
2. Харитонов, Є.О., Саніахметова, Н.О. Цивільне право України. К.: Істина, 2003- 238 с.
3. Поняття та юридична природа заповіді. Західне міжрегіональне управління Міністерства юстиції України. URL: <https://pzmrujust.gov.ua/napriamy-diialnosti/144-yurydychni-konsultatsii/1729-poniattia-ta-iurydychna-pryroda-zapovitu-05112018>
4. Васирина Н.В. Право на заповіт та окремі питання його реалізації. 2014.

Олійник Катерина Дмитрівна

*студ. 2 курсу факультету прокуратури та слідства
(кримінальної юстиції)*

*Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., доц. Калітенко О.М.*

СОЦІАЛЬНІ МЕРЕЖІ ТА ПРАВО: МЕЖІ СВОБОДИ СЛОВА

У сучасному світі соціальні мережі стали ключовим інструментом реалізації права на свободу слова. Вони забезпечують миттєве поширення інформації, участь громадян у публічному дискурсі та формування громадської думки. Водночас їх розвиток породжує деякі правові проблеми, такі як визначення меж свободи слова, відповідальність за контент або баланс між правами людини і публічними інтересами.

Свобода слова є фундаментальним правом, закріпленим як на національному, так і міжнародному рівнях. Але свобода слова в соціальних мережах не є абсолютною. В Україні це питання регулюється статтею 34 Конституції України, де зазначається, що кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розго-

лошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя [1]. Відповідно до Закону України “Про інформацію” який наголошує на тому, що інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини [2].

На міжнародному рівні це питання регулюється Резолюцією ООН «Про сприяння, захист та здійснення прав людини в інтернеті». На зустрічі в Сан-Паулу 2014 року була визнана необхідність того, щоб права людини лежали в основі управління Інтернетом, і що права людей, які є в офлайн-середовищі, повинні також захищатися в онлайн-середовищі [3].

Незважаючи на широкий спектр захисту прав людини в Інтернеті, соціальні мережі створюють ризики, такі як: поширення дезінформації, мова ворожнечі, маніпуляцій громадською думкою.

Хоча й дозволено вільно висловлюватися в Інтернеті та мати доступ до інформації, поглядів і висловлювань інших осіб, до яких належать політичні заяви, релігійні переконання, погляди і висловлювання, що сприймаються прихильно або вважаються не образливими, так і такі, що можуть завдавати образу, шокувати або виводити інших осіб зі стану рівноваги. Тож необхідно приділяти належну увагу репутації та правам інших осіб, зокрема їхньому праву на приватне життя [4]. Проте, можуть накладатися обмеження на такі висловлювання, в яких містяться заклики до дискримінації, ненависті або насильства. Такі обмеження повинні бути правомірними, цілеспрямованими і запроваджуватися під контролем суду.

Україна зіткнулася зі значною проблемою поширення дезінформації в соціальних мережах, мовою ворожнечі та розповсюдженням закликів до насильства у 2014 році під час збройної агресії, яка отримала назву “Антитерористичної операції” на сході країни. В той період ця проблема не мала таких широких обертів,

аж до моменту настання широкомасштабного вторгнення у 2022 році. Наразі це питання залишається досі актуальним. Тому в умовах воєнного стану держава вимушена застосовувати обмеження на поширення деякої інформації з метою захисту національної безпеки та запобігання операціям ворога в інформаційній війні. Ці обмеження відповідають Конституції України, як вже зазначалось раніше, і є обґрунтованими в умовах збройної агресії. Однак, із настанням мирного часу влада має переглянути такі обмеження для забезпечення принципу пропорційності.

Органи державної влади зобов'язані поважати і захищати свободу вираження поглядів та свободу інформації. Будь-які обмеження цієї свободи не повинні бути свавільними та мають переслідувати законну мету. Крім того, згідно з принципом юридичної визначеності, такі обмеження мають бути чітко викладені в законодавчих актах та доступні до ознайомлення користувачами мережі Інтернет.

Можна зробити висновок, що незважаючи на всі плюси використання соціальних мереж, які виступають у формі свободи слова, свободи вираження поглядів, доступу до інформації, поширення інформації, законодавчих ініціативах, контролі за прийняттям рішень, зокрема, підписання петицій та участі в розробці політики, пов'язаної з управлінням Інтернетом та сприянні взаємодії між людьми різних сфер діяльності, потрібно враховувати, що соціальні мережі та всесвітня мережа несуть в собі і низку ризиків, такі як порушення права на приватність, кібербулінг, кіберзлочинність, дезінформація, пропаганда, заохочення до використання мови ворожнечі чи маніпуляції.

Соціальні мережі стають все більш ефективнішим інструментом для боротьби за забезпечення та реалізацію прав людини в Інтернет-просторі, проте використання соціальних мереж та медіа потребує свідомого та відповідального ставлення як і з боку користувачів Інтернету так і з боку держави, міжнародної спільноти та з боку самих платформ, що надають доступ до використання таких мереж. Важливо розуміти та вивчати баланс між захистом

прав людини та захистом від зловживань, встановленню етичних чи нормативних кордонів, які будуть забезпечувати такий баланс.

Соціальні мережі мають вкрай вагомий потенціал для розвитку та можуть як і якісно так і негативно впливати на реалізацію прав людини в мережі. Проте, це потребує зусиль з боку держав, міжнародної спільноти, громадських організацій та самих користувачів задля утворення безпечного та сприятливого середовища в контексті використання соціальних мереж та Інтернет-мережі в цілому.

ЛІТЕРАТУРА:

1. Конституція України. *Відомості Верховної Ради України*. 1996. № 30. ст. 34.
2. Про інформацію: Закон України від 02.10.1992 № 2657-XII. *Відомості Верховної Ради України*. № 48. Ст. 28.
3. Резолюції ООН «Про сприяння, захист та здійснення прав людини в інтернеті». URL: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf
4. Рекомендація CM/Rec(2014)6 Комітету міністрів Ради Європи державам-членам щодо посібника з прав людини для Інтернет-користувачів та пояснювальний меморандум.

Оліярчик Аліна Віталіївна

*студ. 2 курсу факультету прокуратури
та слідства (кримінальної юстиції)*

*Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., доц. Калітенко О.М.*

КІБЕРБУЛІНГ ЯК НОВИЙ ВИКЛИК ДЛЯ ЗАХИСТУ ПРАВ ПРИВАТНОЇ ОСОБИ У ЦИФРОВОМУ СЕРЕДОВИЩІ

Стрімка цифровізація всіх сфер суспільного життя спричинила глибокі трансформації в комунікативних практиках, способах самореалізації та здійсненні прав. Інтернет, соціальні мережі та цифрові платформи створили безпрецедентні можливості для обміну інформацією та доступу до знань. Однак віртуальний простір став ареною для нових форм насильства та посягань на права особи. Особливе місце серед таких загроз посідає кібербулінг –

цькування з використанням цифрових технологій. Як слушно зазначають дослідники, віртуальне середовище через анонімність, відсутність фізичного контакту та здатність миттєво охоплювати необмежену аудиторію створює сприятливі умови для агресивної поведінки. В умовах, коли приватне життя дедалі більше переміщується в онлайн, захист недоторканності приватного життя, честі, гідності та особистої безпеки стикається з новітніми викликами.

Особливої актуальності ця проблема набуває в Україні в умовах воєнного стану. Активне використання цифрових технологій для доступу до критичних послуг супроводжується збільшенням часу, проведеного в інтернеті, зростанням соціальної напруги та поширенням ворожих наративів, що створює підґрунтя для ескалації кіберагресії. Вимушене переміщення громадян призводить до розриву соціальних зв'язків, роблячи людей більш вразливими до онлайн-переслідувань. Аналіз кібербулінгу як загрози правам приватної особи та пошук механізмів його запобігання є нагальним завданням для юридичної науки та правозастосовної практики в Україні [5, с. 135].

Кібербулінг становить специфічну форму посягання на особисті немайнові права, що здійснюється з використанням електронних комунікацій. На відміну від традиційних форм цькування, він характеризується анонімністю правопорушника, можливістю миттєвого охоплення необмеженої аудиторії та тривалістю впливу – шкідливий контент може зберігатися в мережі необмежений час. З теоретико-правової точки зору кібербулінг розглядається як грубе втручання у право на приватність, яке сьогодні включає недоторканність особистого життя, захист честі та гідності, а також право на контроль над цифровою ідентичністю. Цифрова приватність є фундаментом безпеки особи, оскільки її порушення відкриває шлях до подальшої агресії [2, с. 357].

Ефективна протидія кібербулінгу неможлива без захисту персональних даних, оскільки більшість сценаріїв цифрового цькування розпочинаються з доксингу – незаконного збору та опри-

люднення приватної інформації. В Україні правовий фундамент складають Закони «Про захист персональних даних» та «Про основні засади забезпечення кібербезпеки України». Проте правозастосовна практика свідчить про складнощі в ідентифікації агресорів, які використовують інструменти анонізації або зарубіжні платформи, що не реагують на запити в прийнятні строки. Захист прав приватної особи вимагає гармонізації українських норм із європейським GDPR, який посилює відповідальність володільців даних та надає громадянам право на забуття [4].

Важливим аспектом у контексті захисту прав приватної особи є також міжнародне співробітництво у сфері кібербезпеки. Кібербулінг, маючи транскордонний характер, потребує скоординованих дій на рівні держав, оскільки жертва та кривдник можуть перебувати в різних юрисдикціях, а серверне обладнання соціальних мереж – у третіх країнах. Участь України в Будапештській конвенції про кіберзлочинність створює правову основу для міжнародної взаємодії, однак потребує розвитку механізмів оперативного обміну інформацією між правоохоронними органами різних держав. Лише за умови ефективної міжнародної кооперації можливе своєчасне блокування шкідливого контенту, ідентифікація анонімних агресорів та притягнення їх до відповідальності незалежно від місця їхнього перебування.

Сучасне українське законодавство зробило крок уперед із введенням статті 173–4 КУпАП, яка встановлює відповідальність за булінг учасника освітнього процесу. Однак її застосування до кібербулінгу обмежене: суб'єктний склад обмежений освітнім середовищем. Водночас кібербулінг часто переростає у кримінальні правопорушення, передбачені статтею 182 КК України (порушення недоторканності приватного життя), статтею 163 (порушення таємниці кореспонденції), а в тяжких випадках – статтями 129 (погроза вбивством) або 115 (умисне вбивство). Правозастосовна практика ускладнена через недостатню обізнаність правоохоронців із цифровими інструментами фіксації доказів.

Основними викликами залишаються транскордонний характер соціальних мереж та складність процесуального закріплення

цифрових доказів. Платформи часто мають сервери в іноземних юрисдикціях, що ускладнює отримання відомостей про агресорів. Цифрові докази потребують належного оформлення, оскільки їх достовірність може бути оскаржена. Відсутність уніфікованого підходу до електронних доказів та недостатня технічна оснащеність правоохоронних органів знижують ефективність притягнення кривдників до відповідальності. Для подолання цих викликів необхідне впровадження механізмів швидкої взаємодії між правоохоронними органами та адміністраторами цифрових платформ, а також приведення законодавства до європейських стандартів [1, с. 86].

Освітній компонент відіграє ключову роль у формуванні культури безпечної поведінки в цифровому середовищі. Впровадження у шкільну програму курсів з цифрової грамотності, медіаосвіти та кібергігієни дозволяє з раннього віку формувати у дітей навички розпізнавання маніпуляцій, критичного оцінювання інформації та відповідального ставлення до власних персональних даних. Важливим є також навчання педагогічних працівників методів виявлення випадків кібербулінгу та алгоритмів реагування на них. Залучення батьків до просвітницьких заходів сприяє створенню єдиного безпечового простору, де дитина може отримати підтримку як у реальному, так і у віртуальному житті.

Захист прав приватної особи має ґрунтуватися не лише на репресивних заходах, але й на принципі цифрової гігієни, правової просвіти та невідворотності покарання. Цифрова гігієна передбачає формування навичок безпечної поведінки в мережі: обережність при оприлюдненні персональної інформації, використання налаштувань приватності. Правова просвіта має роз'яснювати права жертв та відповідальність кривдників. Ключовим є принцип невідворотності покарання: навіть якщо юридична відповідальність ускладнена, суспільство має давати однозначну оцінку таких дій як неприпустимих. Кібербулінг є складним викликом, що потребує системного підходу до захисту прав людини. Подальше вдосконалення законодавства, адаптація до європейських норм,

посилення спроможностей кіберполіції та підвищення цифрової грамотності населення є ключовими кроками на шляху до мінімізації загроз кібербулінгу та забезпечення надійного захисту прав приватної особи у цифровому середовищі [3, с. 129].

ЛІТЕРАТУРА:

1. Бахаєва А. С. Інформаційно-комунікаційні технології: спосіб вчинення чи підстава для виокремлення окремої форми домашнього насильства? *Вісник Харківського національного університету внутрішніх справ*. 2025. Т. 110. № 3. С. 82–90.
2. Малець М. Р., Даниляк В. І. Кібербулінг і правові механізми захисту жертв. *Аналітично-порівняльне правознавство*. 2025. № 6. С. 355–360.
3. Петренко С. Негативні впливи в онлайн-середовищі: ефективні стратегії та заходи протидії. *Visegrad Journal on Human Rights*. 2025. № 2. С. 125–130.
4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.
5. Сперкач Н. А., Ковбасюк В. С. Напрями запобігання кіберзлочинності та вдосконалення правового регулювання захисту прав людини в кіберпросторі. *Аналітично-порівняльне правознавство*. 2024. № 6. С. 131–137.

Півторак Анастасія Олександрівна

студ. 2 курсу факультету прокуратури та слідства
(кримінальної юстиції)

Національного університету «Одеська юридична академія»

Науковий керівник: к.ю.н., доц. Калітенко О.М.

ЦИФРОВІ ПРАВА ЛЮДИНИ У КІБЕРПРОСТОРІ: СУЧАСНІ ВИКЛИКИ ПРАВОВОГО РЕГУЛЮВАННЯ

В умовах активного розвитку передових технологій, коли життя вже важко уявити без електронних систем, мережі Інтернет, соцмереж або електронних послуг в режимі онлайн, особливо загострюється питання втручання, контролю та регуляції зазначених систем державними законодавчими механізмами. Тож важливо враховувати інтеграцію даних систем в економічний, політичний та соціальний простір, а також розвиток суспільних відносин

у вказаних галузях із використанням результатів технологічного розвитку. Наведене безпосередньо пов'язано із законодавчими механізмами забезпечення правопорядку, у зв'язку з чим аналіз правового регулювання цифрових прав є напрямком, що потребує дискусії.

Наразі поняття «цифрові права» на міжнародному та національному законодавчих рівнях не визначається, проте формується доктринально як комплексна категорія в межах загального розуміння прав людини у цифровому просторі, що розробляється законодавцями та вченими. Зазначене зумовлює застосування комплексного підходу до розуміння «цифрових прав», які становлять сукупність прав особи, що реалізуються у цифровому просторі та гарантують захист свободи, особистого життя і доступу до інформації [2, с. 112].

Цифрові права в Україні мають похідний характер і формуються через конституційні гарантії права на інформацію та приватність, а ні як самостійна системна категорія. Тому зазначене призводить до їх фрагментарного нормативного закріплення та неоднорідну практику застосування [1, с. 270].

Слід звернути увагу на те, що інформаційне право утворюється з кількох взаємопов'язаних складових. Передусім ідеться про право на доступ до Інтернету, яким передбачено позбавлений дискримінації доступ до мережі, свободу вибору провайдера та можливість користування відповідною інфраструктурою. Наступною складовою є право на приватність і захист персональних даних, що забезпечує особам контроль над власною інформацією, зокрема можливість вільного доступу, її виправлення, видалення та, за потреби, заперечення щодо обробки. Окремо зазначається право на інформаційну самовизначеність, яким передбачено отримання відомостей про процедури прийняття рішень автоматизованими системами, право вимагати пояснення та оскаржувати алгоритмічні рішення. Не менш значущим є право на свободу вираження поглядів, що гарантує вільний обмін думками та інформацією із позбавленням від необґрунтованого втручання держави чи при-

ватних структур. Додатково виокремлюється право на участь в електронній демократії, яким передбачено доступ до електронного урядування, онлайн-консультацій, електронного голосування та подання електронних петицій. Завершальною складовою є право на креативність та інтелектуальну власність, останнє включає захист авторських прав на цифровий контент і можливість його законного поширення, зокрема за відкритими ліцензіями [1, с. 271].

На сьогодні правовою регламентацією цифрових прав визначається комплекс міжнародних і національних нормативно-правових актів та рекомендацій, з яких формується фундамент для правового регулювання кіберпростору. До основних міжнародних правових актів слід віднести Генеральну Окінавську хартію глобального інформаційного суспільства прийняту у 2000 році, останньою закріплюється необхідність забезпечення прав людини в умовах цифровізації та визнається Інтернет глобальним простором, що має відповідати міжнародним стандартам, зокрема щодо захисту приватності [5, с. 307]. Вагоме значення посягає Загальний регламент з захисту даних (GDPR), яким встановлено “високі” стандарти обробки персональних даних, зокрема принципи законності, прозорості, цільового обмеження та мінімізації даних, а також гарантує суб’єктам даних широкий спектр прав, включаючи право на доступ, виправлення, стирання, тобто «право на забуття» і обмеження обробки. Крім того, значною мірою має вплив на правову регуляцію Європейська Конвенція з прав людини (ECHR), що зазначає необхідність дотримання універсальних прав людини в умовах цифровізації, зокрема щодо недопущення цифрової дискримінації, забезпечення доступу до інформації та захисту від “надмірного” втручання в приватне життя [3, с. 231].

У працях вчених неодноразово наголошується на тому, що національне правове регулювання цифрових прав перебуває у процесі постійного вдосконалення законодавчими механізмами та взаємоузгодження з європейськими стандартами. Основоположним актом у зазначеному напрямку стає Закон України «Про захист персональних даних» датований 2010 р., яким закріплюють-

ся правові засади обробки персональних даних, встановлюються права суб'єктів даних і обов'язки власників та розпорядників інформації. Додатково набуває перспектив проєкт закону «Про цифрову доступність в Україні» №14278, 2025 року, що спрямований на комплексне врегулювання прав людини в цифровому просторі, включаючи право на доступ до Інтернету, цифрову ідентичність, захист від алгоритмічної дискримінації та гарантії прозорості цифрових сервісів. У сукупності зазначені акти та ініціативи формують нормативну основу для подальшого розвитку інституту цифрових прав, сприяючи забезпеченню рівноваги між технологічним прогресом і дотриманням основоположних прав і свобод людини [4, с. 62].

Однак сучасний етап розвитку цифрових прав супроводжується низкою системних викликів, що ускладнюють їх повноцінну реалізацію та потребують належного правового реагування. Зосереджено значну увагу в науковому просторі цифровому розриву, виражений у нерівномірному доступі до цифрових технологій і мережевих ресурсів між міським і сільським населенням, а також між різними соціально-економічними групами, що, у свою чергу, обмежує можливості реалізації базових прав, зокрема права на інформацію, освіту та участь у цифровому врядуванні. Не менш значущим викликом є тенденція до розширення практик масового спостереження та контролю за інформаційним простором, що потенційно може призводити до непропорційного втручання у приватне життя, обмеження свободи вираження поглядів і формування ризиків зловживання владними повноваженнями як з боку держави, так і з боку приватних суб'єктів [5, с. 307].

Окремої дискусії потребують недоліки у забезпеченні алгоритмічної справедливості, оскільки використання автоматизованих систем прийняття рішень нерідко супроводжується проявами алгоритмічної упередженості, що виникає внаслідок некоректних або нерепрезентативних даних, закладених моделей чи непрозорості алгоритмів, і може призводити до дискримінаційних наслідків для окремих осіб або груп. У вказаному контексті особливо зосе-

реджена увага на необхідність запровадження механізмів аудиту, роз'яснення та підзвітності алгоритмічних систем. Додатково суттєвим викликом залишається забезпечення кібербезпеки, зокрема захисту критичної інформаційної інфраструктури, оскільки зростання кількості та складності кібератак ініціює ризики для функціонування державних інституцій, економічної стабільності та безпеки громадян, що зумовлює потребу у формуванні комплексної системи правових, організаційних і технічних заходів протидії вищезазначеним загрозам [6, с. 211].

Отже, цифрові права на сучасному етапі розвитку суспільства розглядаються як динамічна та комплексна правова категорія, що формується під впливом стрімкої цифровізації та потребує системного нормативного закріплення. Науковцями наголошується на їх похідному характері у національному праві, фрагментарність регулювання та неоднорідність правозастосовної практики, що свідчать про необхідність подальшого концептуального осмислення і кодифікації. Також інтеграція міжнародних стандартів, зокрема європейських підходів до захисту персональних даних, інформаційної самовизначеності та забезпечення прозорості цифрових процесів, стають основоположними для формування цілісної моделі правового регулювання у кіберпросторі. Перспективи розвитку цифрових прав на національному рівні пов'язані з прийняттям спеціалізованого законодавства, нормативне взаємоузгодження з правом Європейського Союзу, інституційним посиленням механізмів контролю та нагляду, а також впровадженням результативних інструментів забезпечення алгоритмічної справедливості та кібербезпеки. Не менш важливим зазначається подолання цифрового розриву та забезпечення рівного доступу до цифрових ресурсів як передумови реалізації основоположних прав і свобод. У даному контексті подальші наукові дослідження орієнтовані на розроблення теоретико-правової моделі цифрових прав, визначення їх місця в системі прав людини та обґрунтування ефективних механізмів їх гарантування в умовах цифрової трансформації суспільства.

ЛІТЕРАТУРА:

1. Захарчук І.В. Цифрові права громадян України: конституційно-правове закріплення та механізми реалізації. *Науковий вісник Ужгородського Національного Університету*. 2025. Вип. 90: ч. 1. С. 286-273.
2. Белов Д.М., Переш, І.Є., Покорба І. Цифрові права людини: доктринальні засади. *Аналітично-порівняльне правознавство*. 2024. Вип. № 2. С. 111-115.
3. Бочковой В.О., Бааджи Н.А. Цифрові права людини їх обмеження в умовах сучасних правових викликів. *Науковий вісник Ужгородського Національного Університету*. 2024. Вип. 84: ч.4. С. 228-233.
4. Дідух Х.В. Цифрові права: український та європейський досвід. *Науковий вісник Ужгородського національного університету*. 2024. Вип. 85: ч. 1. С. 59–65.
5. Сіленко А. Цифрова нерівність у політико-правовому вимірі. *Вісник Прикарпатського університету*. 2026. Вип. № 22. С. 36–49.
6. Лабик А. Р. Право на пояснення алгоритмічних рішень у системі цифрових прав людини. *Науковий вісник Ужгородського національного університету*. 2025. Вип. 92: ч. 5. С. 29–41.

Подцерковна Поліна Олегівна

*студ. 2 курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., проф. Зубар В.М.*

ПРАВИЛА INCOTERMS ЯК ДЖЕРЕЛО ЦИВІЛЬНОГО ПРАВА

У сучасному цивільному обігу, що характеризується динамічністю та транскордонним характером, особливого значення набуває уніфікація правового регулювання. Відмінності у національних правових системах щодо тлумачення торговельних термінів нерідко зумовлюють правову невизначеність та ускладнюють реалізацію прав і обов'язків сторін договору. За таких умов застосування уніфікованих міжнародних правил виступає необхідним інструментом забезпечення стабільності цивільних правовідносин, оскільки сприяє однаковому розумінню змісту договірних умов незалежно від юрисдикції.

У цьому контексті важливу роль відіграють Incoterms (Інкотермс) – правила інтерпретації комерційних термінів. У сучасній

доктрині цивільного права питання визначення місця Інкотермс у системі джерел правового регулювання залишається дискусійним, оскільки ці правила, розроблені Міжнародною торговою палатою (МТП), не є нормативно-правовими актами у класичному розумінні, проте становлять ядро сучасного *lex mercatoria*. В українському правовому полі статус Інкотермс визначається крізь призму статті 7 Цивільного кодексу України, яка визнає звичай джерелом права, а також через спеціальне законодавство, зокрема Закон України «Про зовнішньоекономічну діяльність», що прямо вказує на можливість застосування міжнародних торговельних звичаїв.

Складність правової кваліфікації Інкотермс полягає в їхній дуальній природі: з одного боку, вони виступають як усталені торговельні звичаї, що відображають світову практику, з іншого – стають обов'язковими для сторін передусім у силу принципу автономії волі та свободи договору, закріплених у статті 6 Цивільного кодексу України. У контексті транскордонних операцій правова вага Інкотермс підсилюється положеннями Закону України «Про міжнародне приватне право», де звичаї визнаються допоміжним регулятором у разі відсутності прямих законодавчих приписів.

Окремим дискусійним аспектом у доктрині міжнародного приватного права є те, що текст Інкотермс захищений авторським правом МТП. Це створює суперечність: інтелектуальна власність – це приватна справа, а правовий звичай має бути загальнодоступним. Дехто вважає, що коли приватна організація володіє текстом правил, це суперечить самій суті звичаю, який зазвичай виникає природним шляхом, а не створюється конкретним автором. Проте такий контроль з боку МТП є необхідним, оскільки він гарантує, що правила будуть однаковими для всіх. Саме авторський нагляд дозволяє зберегти стабільність і єдине тлумачення термінів у всьому світі, не допускаючи їх викривлення чи роздроблення у практиці різних держав.

Варто зазначити, що застосування Інкотермс обмежується імперативними нормами національного законодавства, які мають пріоритет у разі їх суперечності. Це підтверджується сталою прак-

тикою Верховного Суду, де правила Інкотермс розглядаються як інструмент для визначення змісту волевиявлення сторін, зокрема щодо моменту переходу ризиків. Таким чином, визнання Інкотермс джерелом цивільного права свідчить про поступову еволюцію правової системи у напрямі більшої децентралізації регулювання, коли недержавні стандарти ефективно доповнюють законодавство та забезпечують гнучкість сучасного комерційного обігу.

ЛІТЕРАТУРА:

1. Цивільний кодекс України : прийнятий 16 січня 2003 року. *Відомості Верховної Ради України*. 2003. №40-44. Ст. 7.
2. Закон України «Про зовнішньоекономічну діяльність» від 16.04.1991 № 959-XII. Ст. 6.
3. Інкотермс. Офіційні правила тлумачення торговельних термінів Міжнародної торгової палати (редакція 2000 року) : Правила МТП від 01.01.2000 № 988_007. URL: https://zakon.rada.gov.ua/laws/show/988_007#Text.
4. Лешанич Л. Правила Інкотермс у регулюванні відносин міжнародних перевезень. *Підприємництво, господарство і право*. 2017. № 12. С. 48–49.
5. Барановська В. М. Практика застосування INCOTERMS 2020 в зовнішньоекономічних договорах. *Науковий вісник Ужгородського національного університету*. 2025. Вип. 87. Ч. 4. С. 188–192.

Прокончук Вікторія Сергіївна

*студ. 2 курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., проф. Зубар В.М.*

ПРАВОВИЙ СТАТУС КУЛЬТУРНИХ ЦІННОСТЕЙ У ЦИВІЛЬНОМУ ОБОРОТІ

Культурні цінності є особливими об'єктами цивільного права, які мають значне історичне, художнє та духовне значення. Їх правовий статус в Україні регулюється як загальними нормами законодавства, в тому числі і цивільного, так і спеціальними законами, що забезпечують охорону національної спадщини. Особливості правового режиму культурних цінностей обумовлюють їхню специфіку як об'єктів цивільного обороту, а також встановлюють певні обмеження у використанні та відчуженні.

Перш за все слід зазначити, що у Цивільному кодексі поняття “культурні цінності” прямо не вживається, проте зробивши аналіз законодавства України можна сказати, що законодавець визначає культурні цінності як об’єкти матеріальної та духовної культури, що мають художнє, історичне, етнографічне або наукове значення. Відповідно до Закону України «Про вивезення, ввезення та повернення культурних цінностей», до цієї категорії належать твори мистецтва (живопис, скульптура), археологічні знахідки, рідкісні рукописи, архівні документи тощо[1]. Важливим аспектом є те, що культурні цінності можуть бути приватною власністю, але їх використання регулюється державою для збереження національного надбання.

Культурні цінності виступають об’єктами таких цивільних правовідносин, як договірні зобов’язання(частіш за все це договір купівлі – продажу), право власності, спадкові[2, с.138]. Наприклад, передача культурних цінностей у спадок регулюється загальними нормами Цивільного кодексу України. Але тут слід зауважити на тому, що для окремих категорій таких об’єктів (зокрема тих, що входять до Державного реєстру національного культурного надбання) існують додаткові вимоги щодо реєстрації або погодження з державними органами.

Одним із ключових аспектів правового статусу культурних цінностей є регулювання їх експорту за межі території України. Згідно із Законом України «Про вивезення, ввезення та повернення культурних цінностей» встановлено суворі правила щодо переміщення таких об’єктів через митний кордон. До прикладу, заборонено вивозити за межі країни:

- Об’єкти з Державного реєстру національного культурного надбання;
- Експонати Музейного фонду України;
- Документи Національного архівного фонду [3, с.29].

Проте, законодавством передбачена можливість тимчасового вивезення культурних цінностей з метою їх участі у міжнародних виставках чи проведення реставраційних робіт. У таких випадках власник зобов’язаний отримати свідоцтво про право на тимчасове

вивезення від Міністерства культури України. Це свідоцтво видається лише за умови страхування об'єкта та гарантій його може кваліфікуватися як контрабанда і каратися відповідно до статті 201 Кримінального кодексу України[4].

До того ж існують певні обмеження щодо відчуження культурних цінностей через цивільні угоди. Наприклад, продаж або дарування таких об'єктів можливе лише для тих категорій, які не входять до охоронних переліків. У разі дарування чи передачі в спадщину культурних цінностей власник або спадкоємець зобов'язаний зареєструвати ці об'єкти в державному реєстрі або передати їх до музеїв чи архівів[5, с.35].

Окремо слід виділити питання повернення незаконно вивезених за кордон культурних цінностей. У разі виявлення таких об'єктів Україна має право вимагати їх повернення на підставі міжнародних договорів, зокрема Гаазької конвенції 1954 року, або шляхом переговорів із відповідними державами. У деяких випадках можливе викуп таких об'єктів державою для забезпечення їхнього повернення.

У своїй роботі “Цивільно – правова охорона прав на культурні цінності та їх оборотоздатність”, Дуденко Т. В. підбиваючи підсумки зазначає, що правовий режим культурних цінностей передбачає встановлення особливих юридичних вимог, які спрямовані на забезпечення їх належного збереження, охорони і використання[6, с.168]. У першу чергу це стосується обмежень у користуванні та розпорядженні такими об'єктами, які закріплені законодавством. Власники культурних цінностей несуть підвищену відповідальність за дотримання правил поведження з ними, а також зобов'язані виконувати низку обов'язків, задля збереження цих об'єктів для майбутніх поколінь.

Одним із ключових елементів цього режиму є вимогу щодо утримання об'єктів культурної спадщини в належному стані. Це означає, що власник мусить забезпечити їх своєчасний поточний та капітальний ремонт, а також створити належні умови їх зберігання задля запобігання їх пошкодження, руйнування або знищення. Це все має здійснюватися не лише з урахуванням за-

гальних норм цивільного законодавства, а й згідно з вимогами спеціального законодавства у відповідній сфері.

Отже, культурні цінності відносяться до особливого правового режиму, який не лише визнає за власником традиційні цивільні права, а саме володіння, користування і розпорядження, а й суттєво обмежує їх. Це обмеження полягає у встановленні конкретних охоронних обов'язків. Попри правовий характер, ці обов'язки виділяються і соціально – культурним характером, бо спрямовані вони на збереження національного культурного надбання України.

ЛІТЕРАТУРА:

1. Про вивезення, ввезення та повернення культурних цінностей: Закон України від 21.09.1999 №1068- XIV. *Відомості Верховної Ради*. 1999. № 48. Ст.405.
2. Зверховська В.Ф. Становлення та розвиток правового регулювання цивільного обігу культурних цінностей. 2020. С. 138.
3. Ангеловська О.С. Порядок переміщення через митний кордон України культурних цінностей. *Юридичний науковий електронний журнал*. 2020. № 3. С. 72–79.
4. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III (зі змінами і доповненнями). *Відомості Верховної Ради України*. Ст. 201.
5. Дуденко Т. В. Культурні цінності в цивільному обороті України. *Проблеми законності*. 2008. С. 33–38..
6. Дуденко Т. В. Система засобів охорони прав на культурні цінності. *Державне будівництво та місцеве самоврядування*. 2016. № 32. С. 159–171

Рижук Єлизавета Вікторівна

*студ. 2 курсу факультету прокуратури та слідства
(кримінальна юстиція)*

*Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., доц. Калітенко О.М.*

ЕЛЕКТРОННІ ДОГОВОРИ: ПРОБЛЕМИ ДОКАЗУВАННЯ ТА ПРАВОВОГО РЕГУЛЮВАННЯ

У сучасному світі все більше правовідносин переходить в електронну форму, що пов'язано з розвитком Інтернету та цифрових технологій. Зараз люди часто укладають договори онлайн,

наприклад при купівлі товарів, замовленні послуг або використанні різних сервісів. Тому електронні договори стали звичайним явищем у цивільному обороті. На мою думку, це значно спрощує життя, але водночас створює певні юридичні проблеми, особливо коли виникають спори між сторонами [1].

Відповідно до цивільного законодавства України, договір – це домовленість сторін, яка спрямована на встановлення, зміну або припинення цивільних прав і обов'язків [2]. Електронний договір по суті нічим не відрізняється від звичайного, крім форми його укладення. Згідно із Законом України «Про електронну комерцію», він укладається в електронній формі і має таку ж юридичну силу, як і письмовий договір [3]. Це означає, що права і обов'язки сторін є однаковими незалежно від того, укладено договір на папері чи через Інтернет.

Електронні договори можуть укладатися різними способами. Наприклад, це може бути обмін електронними листами або прийняття умов договору на сайті шляхом натискання кнопки «Погоджуюсь». Такі дії вважаються акцептом оферти [3]. Проте саме така спрощена форма часто і створює проблеми, тому що не завжди зрозуміло, чи особа дійсно ознайомилась з умовами договору.

Правове регулювання електронних договорів здійснюється кількома нормативно-правовими актами. Основними є Цивільний кодекс України, Закон України «Про електронну комерцію», Закон України «Про електронні довірчі послуги» та Закон України «Про електронні документи та електронний документообіг» [2–5]. Вони визначають загальні правила укладення договорів, вимоги до електронних документів та використання електронного підпису. Зокрема, закон передбачає, що електронний підпис може прирівнюватися до звичайного підпису, якщо він відповідає встановленим вимогам [4].

Разом з тим, на практиці не всі електронні договори укладаються із застосуванням електронного підпису. Дуже часто достатньо просто зареєструватися на сайті або підтвердити дію кодом з телефону. У таких випадках виникає питання, чи можна вважати,

що договір дійсно укладений саме цією особою. На мою думку, це є однією з основних проблем, тому що довести це у суді може бути складно.

Ще однією важливою проблемою є доказування факту укладення електронного договору. Якщо у звичайному договорі є підпис сторін, то в електронному середовищі потрібно використовувати інші докази. Це можуть бути електронні листи, дані з сайту, історія замовлень або навіть скріншоти [6]. Але проблема в тому, що такі докази можна підробити або змінити, і тому суди не завжди ставляться до них однаково.

Також існує проблема збереження електронних доказів. Інформація в електронному вигляді може бути втрачена або видалена. Закон України «Про електронні документи та електронний документообіг» передбачає, що електронний документ має юридичну силу, якщо збережена його цілісність [5]. Але на практиці це не завжди легко забезпечити, особливо якщо пройшло багато часу.

Окремо варто зазначити проблему оцінки доказів судом. Суд оцінює всі докази за своїм внутрішнім переконанням, але чітких правил щодо електронних доказів немає. Через це в одних випадках суд може прийняти, наприклад, скріншот як доказ, а в інших – ні [7]. Це створює певну невизначеність і ускладнює захист прав сторін.

Крім цього, існують і проблеми самого правового регулювання. Хоча в Україні вже є спеціальні закони, вони не повністю враховують сучасні технології. Наприклад, недостатньо врегульовані питання смарт-контрактів або використання нових цифрових інструментів. На мою думку, законодавство в цій сфері ще буде розвиватися, тому що технології змінюються дуже швидко.

Отже, електронні договори є важливою частиною сучасного цивільного обороту і значно спрощують укладення правочинів. Але разом з цим виникають проблеми, пов'язані з доказуванням, ідентифікацією сторін та недосконалістю законодавства. Тому необхідно вдосконалювати правове регулювання та виробляти єдину практику застосування електронних доказів, щоб забезпечити належний захист прав учасників правовідносин.

ЛІТЕРАТУРА:

1. Конституція України від 28.06.1996 р. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр>
2. Цивільний кодекс України від 16.01.2003 р. URL: <https://zakon.rada.gov.ua/laws/show/435-15>
3. Про електронну комерцію: Закон України від 03.09.2015 р. URL: <https://zakon.rada.gov.ua/laws/show/675-19>
4. Про електронні довірчі послуги: Закон України від 05.10.2017 р. URL: <https://zakon.rada.gov.ua/laws/show/2155-19>
5. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. URL: <https://zakon.rada.gov.ua/laws/show/851-15>
6. Дзера О.В. Цивільне право України: підручник. Київ: Юрінком Інтер, 2019. 848 с.

Стефанський Михайло Андрійович

*студ. 2 курсу факультету прокуратури та слідства
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., доц. Калітенко О.М.*

ЦИФРОВІ ДОКАЗИ У СУДОВОМУ ПРОЦЕСІ: ПРОБЛЕМИ ВИКОРИСТАННЯ ТА ПРАВОВОГО РЕГУЛЮВАННЯ

Цифрові докази стають дедалі важливішими у сучасному судочинстві, оскільки значна частина злочинів пов'язана з використанням інформаційних технологій та цифрових платформ. Актуальність цієї теми зумовлена швидким розвитком електронного документообігу, мережових комунікацій та онлайн-сервісів, що створюють нові виклики для кримінального та цивільного процесу. Проблеми використання цифрових доказів охоплюють як технічні аспекти їх збереження та автентичності, так і правові питання щодо допустимості та оцінки таких доказів у суді. Крім того, відсутність єдиних стандартів їх збору та обробки ускладнює ефективне розслідування та забезпечення принципу справедливого суду. У міжнародному контексті спостерігається активний розвиток методів цифрової експертизи та регламентів щодо доказів, що стимулює необхідність адаптації національного законодавства. Тема є особливо актуальною для України, де використання

цифрових доказів у судовій практиці перебуває на стадії формування та потребує системного наукового підходу.

У своєму дослідженні Авдєєва Г. зазначила, що цифрові докази мають низку специфічних характеристик, що відрізняють їх від традиційних доказів у кримінальному процесі. Вона розглянула питання автентичності, цілісності та доказової сили електронної інформації, підкресливши, що без належного технічного забезпечення та стандартизованих процедур цифрові докази можуть бути оскаржені у суді [1]. Ураховуючи роботу Авдєєвої, можна констатувати, що на практиці часто виникає проблема відтворення ланцюжка зберігання цифрового доказу, що ставить під сумнів його достовірність. Цей аспект особливо важливий при розгляді злочинів, пов'язаних з комп'ютерними системами або великими масивами даних, де будь-яке порушення процедури збору може призвести до виключення доказу з процесу.

З погляду Гарасимів О., Марко С. та Ряшко О., основними проблемними питаннями є визначення правового статусу цифрових доказів та методологія їх оцінки у суді. Вони підкреслюють, що сучасне кримінальне законодавство часто не враховує специфіку електронних даних, що ускладнює їх використання для встановлення фактичних обставин справи [2]. Аналізуючи їхні роботи, слід зазначити, що відсутність єдиних критеріїв допустимості та стандартизованих процедур експертизи створює ризик різного трактування цифрових доказів різними суддями, що порушує принцип рівності сторін у процесі та принцип справедливого суду. Водночас автори відзначають позитивну тенденцію до запровадження електронних систем контролю та процедур цифрової експертизи, що поступово підвищує надійність таких доказів.

Аналізуючи роботу Фоміної Т.Г., можна виділити питання технічної безпеки та захисту цифрових доказів від маніпуляцій або знищення. Фоміна зазначає, що електронні докази потребують спеціалізованого програмного забезпечення для фіксації, збереження та перевірки цілісності [3]. У міру розвитку інформаційних технологій та засобів криптографічного захисту можна очікувати

підвищення рівня достовірності електронних доказів. Однак авторка підкреслює, що національне законодавство ще не завжди відповідає технічним вимогам, що призводить до колізій у процесі судового розгляду та до сумнівів щодо допустимості цифрових доказів у суді.

Петренко В.С. у своїй роботі розглянув проблеми використання цифрових доказів у цивільному судочинстві, зазначивши, що подібні питання актуальні не лише для кримінального процесу, а й для цивільних справ, пов'язаних з інтелектуальною власністю та корпоративними правовідносинами [5]. Він наголошує на необхідності впровадження єдиних правил і стандартів оцінки цифрових доказів у цивільному процесі, а також на важливості підготовки суддів і адвокатів до роботи з такими доказами. Ураховуючи його висновки, стає очевидним, що відсутність правового регулювання та стандартизованих процедур створює загрозу ефективності судового процесу та захисту прав сторін.

Цивільний кодекс України визначає загальні принципи доказування та регулює правові відносини щодо документів і електронних даних, що можуть бути використані як докази у цивільному судочинстві [4]. Його норми закладають базу для формування правил допустимості цифрових доказів, але вони потребують деталізації та адаптації під сучасні цифрові технології. У міру розвитку цифрової економіки та масового використання електронних платформ законодавець має забезпечити гармонізацію кодексу з міжнародними стандартами та практиками.

В цілому, проведений аналіз свідчить, що цифрові докази є важливим інструментом для встановлення фактів та підтримки доказової бази у судовому процесі, але їх використання супроводжується численними проблемами. Основними з них є відсутність правового статусу, проблеми автентичності та цілісності, технічна складність збору та зберігання, а також недостатня підготовка суддів та адвокатів до роботи з цифровими даними. Для вирішення цих проблем необхідне удосконалення національного законодавства, розробка стандартів цифрової експертизи та підготовка

професійних кадрів. Крім того, слід враховувати досвід міжнародних практик та застосовувати їхні методи оцінки та контролю цифрових доказів.

Таким чином, можна зробити висновки, що цифрові докази є незамінним елементом сучасного судового процесу, але їх ефективне використання потребує комплексного підходу, що поєднує технічну надійність та правову визначеність. Важливо запровадити чіткі стандарти збору, зберігання та оцінки таких доказів, щоб забезпечити їхню допустимість і достовірність у суді. Розвиток цифрових технологій зумовлює необхідність адаптації законодавства та методик експертизи. Судді та адвокати мають отримувати спеціальну підготовку для роботи з електронними доказами. Врешті-решт, гармонізація національного та міжнародного законодавства дозволить підвищити ефективність судового процесу та гарантувати захист прав сторін.

ЛІТЕРАТУРА:

1. Авдєєва Г. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. *Теорія та практика кримінального процесу*. 2023. № 1. С. 45–57.
2. Гарасимів О., Марко С., Ряшко О. Цифрові докази: деякі проблемні питання щодо їх поняття та використання у кримінальному судочинстві. *Науковий вісник Ужгородського національного університету*. 2023. Том 2, № 75. С. 120–132.
3. Фоміна Т.Г. Електронні докази у кримінальному процесі: проблемні питання теорії та практики. *Кримінальний процес та криміналістика: матеріали наук.-практ. конф.* 2023. С. 88–101.
4. Цивільний кодекс України: Закон України від 16.01.2003 № 435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15>.
5. Петренко В.С. Проблеми використання електронних доказів у цивільному судочинстві. *Наукові записки Національного університету «Одеська юридична академія»*. 2023. Вип. 78. С. 55–70.

Сухомлин Владислава Вітлайівна
*студ. 2 курсу факультету прокуратури та слідства
(кримінальної юстиції) Національного університету
“Одеська юридична академія”*
Науковий керівник: к.ю.н., проф. Калітенко О.М.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ: СУЧАСНИЙ СТАН ТА ПРОБЛЕМИ

У сучасному інформаційному суспільстві персональні дані набувають статусу одного з найцінніших ресурсів, що активно використовується у державному управлінні, бізнесі та повсякденному житті громадян. Цифровізація практично всіх сфер суспільних відносин, розвиток електронного урядування, впровадження онлайн-сервісів та масове використання соціальних мереж сприяють безпрецедентному зростанню обсягів збирання, обробки та зберігання інформації про фізичних осіб. У таких умовах проблема забезпечення належного рівня захисту персональних даних набуває не лише правового, а й соціального значення.

Поняття «персональні дані» – «...будь-яка інформація, яка стосується ідентифікованої особи або особи, яка може бути ідентифікованою» [1, с.20].

В Україні питання захисту персональних даних є особливо актуальним у зв'язку з євроінтеграційними процесами, необхідністю гармонізації національного законодавства із правом Європейського Союзу, а також з огляду на виклики, пов'язані з гібридною війною та зростанням кіберзагроз.

«Саме Європейський Союз сьогодні став локомотивом розвитку правового регулювання у сфері захисту персональних даних. Ключове місце права на приватність серед спільних європейських цінностей було підтверджено і в Хартії основних прав ЄС від 7 грудня 2000 року» [1, с.13].

Правову основу захисту персональних даних в Україні становлять конституційні гарантії права на невтручання в особисте і сімейне життя, а також спеціальне законодавство. Закон України «Про захист персональних даних» визначає основні засади обробки інформації про фізичну особу, включаючи принципи законно-

сті, цільового призначення, адекватності та безпеки, але водночас це – «...рамковий документ. Його положення регулюють правові відносини, пов'язані із захистом та обробкою персональних даних у величезній кількості сфер суспільного життя. З цих же причин Закон не може детально визначати порядок та процедуру обробки персональних даних у всіх вказаних сферах» [1, с.19].

Порівняння українського законодавства із Загальним регламентом Європейського Союзу про захист даних свідчить про наявність суттєвих відмінностей. Європейський підхід передбачає більш жорсткі вимоги до обробки персональних даних, включаючи обов'язок отримання чіткої та однозначної згоди суб'єкта даних, забезпечення прозорості процесів обробки та встановлення значних санкцій за порушення. В Україні ж механізми контролю та відповідальності залишаються недостатньо ефективними, що знижує рівень захисту.

Важливу роль у формуванні практики захисту персональних даних відіграють судові органи. Аналіз судових рішень дозволяє виявити основні проблеми правозастосування та визначити тенденції розвитку відповідної практики. Суди розглядають широкий спектр справ, пов'язаних із порушенням права на приватність, незаконним поширенням інформації, використанням персональних даних без згоди особи та іншими порушеннями.

В Україні судові рішення публікуються у відкритому доступі (наприклад, у Єдиному державному реєстрі судових рішень). Це забезпечує прозорість судової влади, але водночас створює ризик розголошення персональних даних учасників процесу.

Головна ідея підходу судді Верховного Суду Яна Берназюка щодо даної проблеми – поєднання двох принципів: публічність судових рішень (для довіри до суду) та захист приватного життя людини. Тому судові рішення повинні бути відкритими, але без розкриття зайвої персональної інформації [2].

Особливу складність становлять справи, у яких захист персональних даних поєднується з іншими правовими інститутами, зокрема захистом честі, гідності та ділової репутації, а також

правом інтелектуальної власності. У таких випадках суди змушені враховувати баланс між різними правами та інтересами, що ускладнює процес прийняття рішень.

Впровадження штучного інтелекту у сферу правосуддя створює як нові можливості, так і нові ризики. З одного боку, такі технології можуть підвищити ефективність роботи судів, з іншого – вони пов'язані з обробкою великих масивів персональних даних, що потребує належного правового регулювання та технічного захисту.

«...для безпечного опрацювання матеріалів справ потрібен суверенний ШІ. Як альтернативу експерти розглядають використання моделей із відкритим кодом, розгорнутих на автономному обладнанні без доступу до мережі «Інтернет». Це дозволило б забезпечити конфіденційність, проте на сьогодні такі рішення ще не набули широкого практичного застосування» [2].

Необхідно також відзначити недостатній рівень правової культури у сфері захисту персональних даних. Багато суб'єктів господарювання не приділяють належної уваги дотриманню вимог законодавства, що призводить до численних порушень. Громадяни, у свою чергу, часто не усвідомлюють своїх прав або не знають механізмів їх захисту.

Захист персональних даних в умовах воєнного стану в Україні – це система правових, організаційних і технічних заходів, спрямованих на забезпечення конфіденційності та безпеки інформації про фізичну особу, навіть у період збройного конфлікту. «...воєнний стан в Україні змінив звичайний правовий режим суспільного життя, зокрема він вплинув і на захист персональних даних, перетворивши його на один із ключових елементів національної безпеки» [5, с.426].

Державні органи, військове командування та військові адміністрації можуть обробляти персональні дані без згоди особи, якщо це необхідно для: забезпечення оборони держави; проведення оперативно-розшукової діяльності; боротьби з тероризмом; виконання повноважень органів влади.

В умовах війни поширились кібератаки, які були безпосередньо пов'язані з атаками на державні реєстри, що містять персональні дані. Досвід України щодо захисту персональних даних в умовах війни підкреслює, що ця проблема має комплексний і системний характер. Виявилося, що важливим аспектом є як міжвідомча координація між Держспецзв'язку, Службою безпеки України, Міністерством юстиції України, так і міжнародна співпраця щодо обміну досвідом захисту персональних даних та отримання новітніх інноваційних технологій у сфері захисту даних. Водночас війна актуалізувала потребу у швидкому реагуванні та адаптації національної правової системи до міжнародних стандартів.

«...у надзвичайних умовах захист персональних даних має бути посиленим. Доцільною є розробка особливої системи захисту персональних даних, яка може включати такі елементи: роз'яснення населенню ризиків використання персональних даних; підвищення кваліфікації фахівців; створення спеціалізованих підрозділів для захисту персональних даних; розробку та впровадження стратегії кібербезпеки, а також міжнародне співробітництво й обмін досвідом» [5, с. 430].

Таким чином, сучасний стан захисту персональних даних в Україні характеризується складним поєднанням позитивних і негативних тенденцій. З одного боку, існує нормативна база та формується судова практика, з іншого – наявні суттєві проблеми, пов'язані з недосконалістю законодавства, складністю правозастосування та зростанням кіберзагроз. Подальший розвиток цієї сфери потребує комплексного підходу, що включає вдосконалення законодавства, гармонізацію з європейськими стандартами, розвиток судової практики, підвищення ефективності контролю та формування належного рівня правової культури.

Захист персональних даних під час воєнного стану має особливий правовий режим. Держава може розширювати повноваження щодо обробки інформації з метою національної безпеки, однак такі обмеження повинні бути тимчасовими, законними та пропорційними, а право людини на приватність залишається фундаментальною конституційною гарантією.

«...системи захисту персональних даних формуються з урахуванням рівня технічного оснащення інформаційних систем, особливостей національного законодавства, правової обізнаності громадян та дієвості механізмів контролю. Реалізація захисту персональних даних може відбуватися у звичайному і надзвичайному правовому режимі» [5, с.432].

ЛІТЕРАТУРА:

1. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: правове регулювання та практичні аспекти: навч.-практ. посібник. Київ: К.I.C., 2015. 220 с.
2. Берназюк Я. Захист персональних даних при опублікуванні судових рішень: доповідь. 2026. URL: https://court.gov.ua/storage/portal/supreme/prezent2026/179_Privacy_Rights_in_AI_Justice_bernaziuk.pdf
3. Брижко В. М. Захист персональних даних: реалії та практика сучасності. *Інформація і право*. 2013. № 3 (9).
4. Сфремова К. В. Технології цифрової економіки та фінансова безпека. *Право та інновації*. 2023. № 2 (42). С. 7–11.
5. Пальчик М. Л., Шкрібляк К. П., Березецький Ю. М. Актуальні проблеми захисту персональних даних як напряду забезпечення національної безпеки України в умовах війни. *Аналітично-порівняльне правознавство* 2025. Вип. 6. Частина 2. С. 425-434.
6. Савченко В. В., Биков О. М. Захист персональних даних у сучасному законодавстві. *Legal Bulletin*. 2024. № 4 (14). С. 67-72.

Татарінцева Дарина Ігорівна

*студ. 2 курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., проф. Зубар В.М.*

ЦИВІЛЬНО-ПРОВА ХАРАКТЕРИСТИКА СУПЕРФІЦІЮ: СУЧАСНІ ВИКЛИКИ ПРАВЗАСТОСУВАННЯ

У контексті сучасних трансформацій приватного права України особливої актуальності набуває дослідження обмежених речових прав на чуже майно. Одним із таких інститутів є суперфіцій – право користування чужою земельною ділянкою для забудови.

Право користування чужою земельною ділянкою для забудови (суперфіцій) визначається як довгострокове, відчужуване та

успадковане право користування земельною ділянкою, передачею власником іншій особі за плату або безоплатно для будівництва та експлуатації на ній будівель і споруд, право власності на які належить користувачу [1]. За своєю правовою природою суперфіцій є речовим (абсолютним) правом, що забезпечує безпосередній вплив на річ та захищається від порушень з боку невизначеного кола осіб [2, с. 363].

Інститут суперфіцію є фундаментальною правовою конструкцією, що дозволяє ефективно розмежовувати повноваження власника та користувача земельної ділянки. Його значення особливо зростає в умовах земельної реформи, оскільки він створює правовий механізм залучення земельних ресурсів до економічного обороту без відчуження права власності. Водночас, незважаючи на нормативне закріплення, українська правозастосовна практика свідчить, що ефективне функціонування гальмується низкою нормативних, процедурних та практичних проблем, які потребують наукового осмислення та законодавчого вдосконалення.

Правове регулювання суперфіцію здійснюється, насамперед, нормами Цивільного кодексу України (глава 34), а також положеннями Земельного кодексу України. М.Я. Ващишин вважає, що суперфіцій – це право користування чужою земельною ділянкою для будівництва промислових, побутових, соціально-культурних, житлових та інших споруд і будівель, що характеризується довгостроковістю, платністю, відчужуваністю та успадкованістю [3, с. 127].

Суперфіцій як обмежене речове право має низку характерних ознак, що виокремлюють суперфіцій з поміж інших речових прав. По-перше, він є похідним від права власності на земельну ділянку, однак не зводиться до нього. По-друге, суперфіцій має самостійний об'єкт – право забудови, що відрізняє його від оренди. По-третє, він може бути предметом цивільного обороту, зокрема відчужуватися та передаватися у спадщину. Крім того, на нього поширюються способи абсолютного захисту, аналогічні захисту права власності [4, с. 186].

Водночас правова природа суперфіцію має складний, комплексний характер. Він поєднує ознаки речового права (абсолютність, слідування, публічність) та зобов'язального елементу (договірна основа виникнення та визначення умов користування). Така дуалістична природа обумовлює складність його правозастосування та спричиняє низку колізій.

Насамперед, спостерігається невизначеність у розмежуванні суперфіцію та оренди земельної ділянки. Судова практика Верховного Суду свідчить про відсутність єдиного підходу до розмежування суперфіцію та оренди земельної ділянки. Показовою у контексті розмежування суперфіцію та оренди земельної ділянки є справа № 922/1626/23, у якій Верховний Суд дійшов висновку про неможливість застосування до орендних правовідносин підходів, характерних для суперфіцію [5]. Суд відмовив у застосуванні положень, характерних для суперфіцію, визнавши правовідносини орендними, незважаючи на наявність ознак забудови. Суд зазначив, що відсутність забудови земельної ділянки не може розглядатися як порушення умов договору оренди, якщо обов'язок забудови прямо не передбачений договором.

Таким чином, було підтверджено, що визначальним критерієм розмежування цих інститутів є зміст правовідносин, а не їх формальне або фактичне сприйняття сторонами. Це підтверджує тенденцію до оцінки фактичного змісту правовідносин, що, однак, призводить до неоднакової правової кваліфікації аналогічних ситуацій.

Другою проблемою є відсутність чіткого правового режиму об'єктів нерухомості, створених на підставі суперфіцію. Неврегульованість питання про належність таких об'єктів після припинення права користування створює правову невизначеність і підвищує ризик виникнення спорів.

Третьою проблемою є колізійність норм цивільного та земельного законодавства. Відсутність належної координації між ЦК України та Земельним кодексом України ускладнює застосування норм і знижує ефективність правового регулювання.

Крім того, слід відзначити недосконалість механізмів державної реєстрації права суперфіцію, що негативно впливає на забезпечення принципу публічності речових прав.

У судовій практиці суперфіцій найчастіше стає предметом спорів у зв'язку з невикористанням земельної ділянки для забудови протягом встановленого строку (зокрема відповідно до ст. 416 ЦК України), припиненням договору, визначенням правового режиму збудованих об'єктів, а також вимогами щодо знесення будівель або викупу земельної ділянки.

Проект нового ЦК України передбачає системне оновлення інституту речових прав, зокрема шляхом їх чіткішої класифікації, посилення принципу публічності та удосконалення механізмів державної реєстрації. Простежується також орієнтація на європейські моделі регулювання прав на чужі речі, що розглядають суперфіцій як ефективний інструмент забудови.

Водночас аналіз положень проекту свідчить, що він не усуває повною мірою існуючих проблем. Зокрема, зберігається недостатня конкретизація змісту суперфіцію, що не дозволяє остаточно відмежувати його від оренди. Також недостатньо врегульовано наслідки припинення суперфіцію, особливо щодо об'єктів нерухомості.

Отже, суперфіцій як інститут цивільного права України перебуває на етапі становлення та потребує подальшого вдосконалення. Чинне законодавство містить низку прогалин і колізій, що ускладнюють його ефективне застосування.

Проект нового Цивільного кодексу України від 22.01.2026 створює передумови для модернізації правового регулювання суперфіцію, однак не усуває всіх наявних проблем. У зв'язку з цим доцільним є:

- чітке нормативне розмежування суперфіцію та оренди;
- визначення правового режиму об'єктів забудови;
- узгодження норм цивільного та земельного законодавства;
- удосконалення інституту державної реєстрації речових прав.

Реалізація зазначених напрямів сприятиме підвищенню ефективності правового регулювання, забезпеченню стабільності цивільного обороту та гармонізації національного законодавства з європейськими стандартами.

ЛІТЕРАТУРА:

1. Цивільний кодекс України : прийнятий 16 січня 2003 року. *Відомості Верховної Ради України*. 2003. №40-44. Ст. 356.
2. Харитонов Є.О., Харитонova О.І., Старцев О.В. Цивільне право України: Підручник. Вид. 3, перероб. і доп. Київ: Істина, 2013. С. 808.
3. Ващишин М.Я. Юридичні факти у правовідносинах суперфікцію. *Науковий вісник Львівського державного університету внутрішніх справ*. 2013. № 3. С.126–135.
4. Мaляр С.А., Грищенко Л.В. Правова природа користування чужим майном у контексті модернізації цивільного кодексу України. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2021. № 4. С. 184-194.
5. Справа № 922/1626/23: Судова справа за позовом керівника Шевченківської окружної прокуратури міста Харкова в інтересах держави, в особі Харківської міської ради, м. Харків до Приватного підприємства «Геюр+», м. Харків про розірвання договору оренди землі та повернення земельної ділянки. *Єдиний державний реєстр судових рішень*. URL: <https://reyestr.court.gov.ua/>

Толкачова Тетяна Андріївна

*студ. 2-го курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., проф. Зубар В.М.*

ПОНЯТТЯ МАЙНА У ЦИВІЛЬНОМУ ПРАВІ

Поняття майна у цивільному праві є однією з основних категорій, через яку визначається зміст більшості цивільних правовідносин. Саме майно виступає основним об'єктом права власності, зобов'язальних відносин, спадкування та інших інститутів цивільного права. Від правильного визначення поняття майна залежить застосування норм законодавства, визначення правового режиму речей та майнових прав, а також можливість їх участі у цивільному обороті.

У законодавстві України поняття майна використовується у різних значеннях. У деяких випадках під майном розуміють лише речі, а в інших – також майнові права та обов’язки. Таке різноманіття підходів пояснюється складністю даної правової категорії та її широким застосуванням у цивільному праві.

У різних нормах поняття майна використовується у різному значенні. У деяких випадках під майном розуміють певні речі або їх сукупність, а в інших – майнові права та обов’язки. Відповідно до ст. 177 Цивільного кодексу України об’єктами цивільних прав є речі, у тому числі гроші та цінні папери, інше майно, майнові права, результати робіт і послуг, а також інші матеріальні та нематеріальні блага. Водночас згідно зі ст. 190 ЦК України майном як особливим об’єктом цивільних прав визнається окрема річ, сукупність речей, а також майнові права та обов’язки. Отже, законодавець закріплює широке розуміння майна, що включає як матеріальні, так і нематеріальні елементи. [1]

У науковій літературі пропонується розглядати поняття майна у широкому та вузькому значенні. У широкому розумінні майном є всі блага, які мають економічну цінність і можуть бути об’єктом цивільних правовідносин, а у вузькому – речі, майнові права та обов’язки. У цивільному праві важливо відмежовувати майнові та немайнові блага. До майнових благ належать речі, результати робіт, послуги, майнові права та обов’язки, які можуть бути оцінені у грошовій формі.

Нематеріальні блага – це результати думок людини, інформація та інші об’єкти, які не мають фізичної форми. До особистих немайнових благ належать життя, здоров’я, честь, гідність, ім’я, репутація, свобода творчості та інші цінності, які захищає закон.

Речі – найпоширеніший вид майна у цивільному праві. Речами називаються предмети з матеріального світу, які можуть задовольнити потреби людини та бути продані або передані. До речей належать як природні об’єкти, так і ті, які створювалися людиною. Щоб щось вважали річчю, воно має бути обігоздатним, тобто може перейти з рук у руки через угоду, спадок або інші законні способи. [2, с.143]

Речі поділяються за обігоздатністю на три групи: речі, які обігають, речі, які вилучили з обігу, і речі, обмежені в обігу. Речі, які вилучили з обігу, не можуть належати особі, наприклад, зброя, вибухові речовини, бойова техніка, наркотики і тому подібне. Речі, обмежені в обігу, можуть належати особі лише після отримання спеціального дозволу [2].

У цивільному праві речі можна поділити за різними ознаками.

1. Рухомі і нерухомі речі. Нерухомі речі – це земельні ділянки, будівлі, споруди тощо, які неможливо переміщати без знецінення. Рухомі – всі інші речі. Для нерухомого майна встановлено особливий порядок передачі, який вимагає державної реєстрації.
2. Індивідуально визначені та родові речі. Індивідуальні речі мають унікальні ознаки, родові – визначаються кількістю, вагою або мірою. Якщо втрачається індивідуальна річ, боржник повинен відшкодувати її вартість, а якщо – родова, то передає іншу річ такого самого роду.
3. Подільні і неподільні речі. Подільні – це речі, які можна поділити, не знищуючи їх призначення. Неподільні – не можна ділити без зниження їх вартості.
4. Споживні і неспоживні речі. Споживні речі зникають при використанні, наприклад, харчові продукти. Неспоживні речі зберігають свої властивості довго.
5. Головні і приналежні речі. Головна річ має самостійне призначення, а приналежна – щоб її обслуговувати. Якщо головна річ втрачається, то приналежна теж втрачається, якщо це не передбачено законом або угодою.

Хочу також зазначити, що до об'єктів цивільних прав належать також гроші, плоди, доходи та продукція. Гроші є особливим видом майна і виступають загальним еквівалентом вартості. Вони можуть бути самостійним об'єктом правовідносин, а також засобом для виконання зобов'язань. Плоди – це речі, які утворюються природним шляхом з іншої речі, а доходи – це грошові або

інші надходження від використання майна. Загальним правилом є те, що плоди та доходи належать власникові речі, якщо іншого не встановлено законом або договором.

Поняття майна важливе для всієї системи цивільного права. Воно використовується для визначення об'єктів власності, змісту зобов'язань, складу спадщини, відповідальності за шкоду, а також при підписанні цивільно-правових договорів. Саме з розуміння майна залежить поділ цивільного права на речове і зобов'язальне, а також встановлюється правовий режим різних об'єктів цивільних правовідносин.[3]

Можна зробити такий висновок, що поняття майна в цивільному праві – це складна і різноманітна категорія, яка включає речі, гроші, цінні папери, майнові права та обов'язки. Законодавство України застосовує це поняття як у широкому, так і у вузькому смислі, оскільки норми цивільного права використовуються в різних сферах. Основним типом майна є речі, які можна продавати або передавати у власність і мають певні законні правила. Дуже важливо визначати, які саме речі є, бо це допомагає правильно застосовувати закони про те, як з ними можна виставляти на продаж, передавати або захищати. Отже, поняття майна дуже важливе для всього цивільного права, бо через нього ставляться до об'єктів правових відносин, визначається зміст прав і обов'язків учасників, а також способи захисту їхніх інтересів.

ЛІТЕРАТУРА:

1. Цивільний кодекс України від 16 січня 2003 р. № 435-IV. *Відомості Верховної Ради України*. 2003. № 40-44. Ст. 356
2. Бірюков І.А., Заїка Ю.О. Цивільне право України. Загальна частина: навчальний посібник. К.: КНТ, 2006. 480 с.
3. Дзера О.В. Цивільне право України: підручник. Київ: Юрінком Інтер, 2019.

Чурсова Таїсія Миколаївна
*студ. 2 курсу факультету прокуратури та слідства
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., доц. Калітенко О.М*

КІБЕРБУЛІНГ ЯК НОВИЙ ВИКЛИК ДЛЯ ЗАХИСТУ ПРАВ ПРИВАТНОЇ ОСОБИ У ЦИФРОВОМУ СЕРЕДОВИЩІ

Актуальність теми дослідження зумовлена стрімким розвитком цифрових технологій та зростанням ролі інтернет-комунікацій у повсякденному житті людини. Разом із позитивними аспектами цифровізації з'являються нові загрози для прав і свобод особи, зокрема кібербулінг. Особливо вразливими до цього явища є діти та підлітки, однак жертвами можуть ставати й дорослі. Кібербулінг створює серйозні ризики для психічного здоров'я, честі, гідності та приватного життя особи. Водночас існують проблеми правового регулювання та практичного захисту прав постраждалих у цифровому середовищі. Саме тому дослідження кібербулінгу як нового виклику для захисту прав приватної особи є надзвичайно актуальним.

В міру розвитку цифрового середовища зростає значення забезпечення прав людини у сфері інформаційних відносин, виникають і розвиваються нові форми посягання на честь, гідність і приватність особи, серед яких особливе місце займає кібербулінг як форма психологічного насильства в мережі Інтернет (1 абзац тексту) [1]. Денисюк М.М. у своєму дослідженні зазначає, що насильство в освітньому середовищі дедалі частіше переходить у цифрову площину, де проявляється у формі образ, переслідування, поширення неправдивої інформації та приниження гідності особи [1]. Автор підкреслює, що кібербулінг має більш тривалий і масштабний вплив порівняно з традиційними формами насильства через швидкість поширення інформації та її доступність широкому колу осіб.

Серебряк С.В. у своєму дослідженні розглянув особливості правового регулювання цифрових прав людини та зазначив, що сучасне законодавство повинно враховувати нові виклики, пов'яза-

ні з розвитком цифрового середовища [2]. Автор вважає, що право на приватність, захист персональних даних та свободу вираження поглядів потребують додаткових гарантій у кіберпросторі. Водночас відсутність чітких механізмів реагування на випадки кібербулінгу ускладнює ефективний захист прав постраждалих осіб.

Ломачинський Б.Г. у своєму дослідженні зазначив, що цифрова доба формує нові світоглядні виклики, пов'язані з трансформацією соціальних відносин та комунікацій [3]. Автор наголошує, що анонімність та відсутність безпосереднього контакту між учасниками комунікації сприяють зростанню агресивної поведінки в мережі. Це створює додаткові труднощі для ідентифікації правопорушників та притягнення їх до відповідальності.

Сперкач Н.А. та Ковбасюк В.С. у своєму дослідженні розглянули напрями запобігання кіберзлочинності та вдосконалення правового регулювання захисту прав людини у кіберпросторі [4, с. 785–790]. Автори зазначають, що ефективна протидія кібербулінгу потребує комплексного підходу, який включає як правові, так і організаційні заходи. Вони підкреслюють необхідність удосконалення законодавства, підвищення рівня цифрової грамотності населення та розвитку міжнародного співробітництва у сфері кібербезпеки.

Важливу роль у забезпеченні захисту прав особи у цифровому середовищі відіграє законодавство України, зокрема Закон України «Про захист персональних даних», який визначає правові засади обробки та захисту інформації про фізичну особу [5]. Зазначений нормативно-правовий акт встановлює обов'язки суб'єктів, що здійснюють обробку персональних даних, а також гарантує право особи на захист від незаконного втручання у її приватне життя. Проте на практиці застосування цього закону у випадках кібербулінгу залишається недостатньо ефективним, що свідчить про необхідність його вдосконалення.

Таким чином, кібербулінг є складним соціально-правовим явищем, яке потребує комплексного підходу до його розуміння та подолання, а також вдосконалення механізмів захисту прав приватної особи у цифровому середовищі [1–5].

Висновки. Кібербулінг є одним із найбільш актуальних викликів сучасного цифрового суспільства. Його поширення негативно впливає на реалізацію прав людини, зокрема права на повагу до честі, гідності та приватного життя. Існуючі механізми правового захисту потребують удосконалення та адаптації до нових умов цифрового середовища. Важливим є поєднання правових, освітніх та технічних заходів для ефективної протидії цьому явищу. Подальший розвиток законодавства та практики його застосування сприятиме підвищенню рівня захисту прав особи у кіберпросторі.

ЛІТЕРАТУРА:

1. Закон України «Про захист персональних даних». URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
2. Денисюк М.М. Насильство в шкільному середовищі. 2025. URL: <https://lpnu.ua/sites/default/files/2025/radaphd/31098/disertaciya-denisyuk-mm-versiya-sayt.pdf>
3. Серебряк С.В. Особливості правового регулювання цифрових прав людини. URL: <https://journals.snu.edu.ua/index.php/app/article/view/1081/1039>
4. Ломачинський Б.Г. Світоглядні виклики цифрової доби. 2025. URL: https://elibrary.kubg.edu.ua/id/eprint/52399/1/B_Lomachynskyi_FSHN_2025.pdf
5. Сперкач Н.А., Ковбасюк В.С. Напрями запобігання кіберзлочинності та вдосконалення правового регулювання захисту прав людини у кіберпросторі. *Аналітично-порівняльне правознавство*. 2024. № 6. С. 785–790.

Шарко Світлана Василівна

*студ. 2-го курсу факультету прокуратури та слідства
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., доц. Калітенко О.М*

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ КІБЕРБЕЗПЕКИ: ПРАВОВІ РИЗИКИ ТА ПЕРСПЕКТИВИ

У сучасному цифровому суспільстві кібербезпека являється однією з ключових складових національної та глобальної безпеки. Захист інформаційного простору є пріоритетним завданням

для сучасних інституцій, оскільки концентрація значних масивів конфіденційних даних створює передумови для масштабних кібератак. Стрімкий розвиток інформаційних технологій, зростання обсягів даних ускладнення кіберзагроз обумовлюють необхідність застосування новітніх інструментів захисту. Одним із таких інструментів є штучний інтелект, який відкриває нові можливості для виявлення, аналізу та запобігання кіберзлочинам.

Для українського законодавства термін «штучний інтелект» є відносно новим, і на сьогодні відсутні спеціалізовані нормативно-правові акти, що регулюють цю сферу, проте, у 2020 році розпорядженням Кабінету Міністрів України було затверджено Концепцію розвитку штучного інтелекту, у якій, серед інших понять, подано й визначення ШІ. Відповідно до даної Концепції, штучний інтелект – це впорядкована система інформаційних технологій, що дає змогу виконувати складні завдання завдяки застосуванню наукових методів і алгоритмів обробки інформації, яка отримується або генерується під час функціонування системи, а також дозволяє створювати й використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з даними та визначати шляхи досягнення поставлених цілей[1]. Водночас, в Україні правове регулювання ШІ залишається недостатнім. Зокрема, чинний Закон України «Про захист персональних даних» не враховує особливостей обробки великих масивів інформації із застосуванням машинного навчання, що створює прогалини у сфері приватності та безпеки [2, с. 578]. Крім того, відсутні чіткі норми щодо перевірки алгоритмів, оцінювання ризиків і забезпечення прозорості їх використання державними органами. Міжнародне та національне право наразі характеризуються обережним і фрагментарним підходом до визначення правового статусу штучного інтелекту. У межах євроінтеграційного курсу Україна повинна поступово узгоджувати своє законодавство зі стандартами Європейського Союзу, зокрема щодо підзвітності алгоритмічних рішень, відкритості критеріїв та недискримінації. Водночас впровадження ШІ повинно супроводжуватися визначенням відповідальності, забезпечен-

ням людського контролю та можливістю оскарження автоматизованих рішень [2, с. 578].

З урахуванням значних обсягів інформації, яку необхідно обробляти в сучасних умовах, більшість організацій і установ, у тому числі в оборонному та безпековому секторах, вже використовують можливості штучного інтелекту задля забезпечення кібербезпеки[3, с. 95]. Інтелектуальний аналіз великих обсягів текстових, графічних, аудіо- та відеоданих дає змогу виявляти потенційні терористичні загрози й формувати доказову базу для запобігання правопорушенням у сфері безпеки[4, с. 86]. Варто зазначити, що яскравим прикладом застосування штучного інтелекту у сфері кібербезпеки є SIEM-системи, адже дана система являє собою складну інформаційно-аналітичну інфраструктуру, що поєднує програмне й апаратне забезпечення, мережеві технології, управлінські підходи та відповідні процеси, спрямовані на гарантування інформаційної безпеки. Основним її призначенням є збирання, обробка та аналізування подій безпеки, а також своєчасне виявлення та реагування на інциденти, що виникають у комп'ютерних системах, мережах і програмних середовищах[5, с. 202].

У сучасних умовах штучний інтелект виступає не лише допоміжним інструментом, а й невід'ємним елементом ефективної системи протидії кіберзагрозам, адже основними напрямками застосування штучного інтелекту у сфері кібербезпеки являється прогнозування загроз, що передбачає передчасне виявлення потенційних та можливих кібератак, автоматизація реагування на кіберінциденти, інтелектуальний моніторинг мереж, спрямований на аналіз мережевої активності та виявлення відхилень, що можуть свідчити про несанкціонований доступ або ж вторгнення, управління ідентифікацією та доступом, яке дозволяє посилити контроль доступу та гарантувати, що до системи мають доступ лише авторизовані користувачі, а також застосування захищених протоколів зв'язку, де використання ШІ сприяє підвищенню рівня захисту даних під час їх передавання [3, с. 96].

В умовах правового режиму воєнного стану спостерігається істотне зростання як кількості, так і складності кібератак. Вар-

то звернути увагу на те, що такі атаки, як правило, мають цілеспрямований характер і нерідко поєднуються з психологічними впливами або інформаційно-деструктивними операціями. Під час збройної агресії здійснюються кібератаки країною-агресором на державні інформаційні ресурси та об'єкти критичної інфраструктури, досить часто задля спроби несанкціонованого втручання в системи управління об'єктами енергетичної, транспортної, телекомунікаційної сфер, також є потенційна загроза проведення фішингових кампаній, орієнтованих на військовослужбовців і волонтерські спільноти, та реалізація дезінформаційних заходів із використанням соціальних мереж і чат-ботів, а також компрометація урядових облікових записів із подальшим поширенням неправдивої інформації[6, с. 453]. У таких випадках, людський фактор стає «вузьким місцем», адже спеціалісти не встигають обробляти масштабний потік даних про можливі та потенційні атаки в реальному часі, водночас як штучний інтелект дозволяє діяти на випередження, адже, системи ШІ не просто фіксують втручання, а моделюють ймовірні сценарії майбутніх атак[3, с. 97].

Таким чином, штучний інтелект практично застосовується у сфері кібербезпеки, однак його правове забезпечення значно відстає від технологічного розвитку, що створює потенційні ризики як для прав людини, так і для стабільності цифрового середовища. Отож, правове регулювання використання штучного інтелекту у сфері кібербезпеки стикається з низкою складнощів, серед яких ключове місце посідає проблема юридичної визначеності, оскільки відсутність у вітчизняному законодавстві дефініцій «електронного суб'єкта» чи «автономного агента» унеможливорює чіткий розподіл відповідальності за рішення, що порушують права і свободи людини між розробником, адміністратором та самою системою. Ця ситуація ускладнюється динамічною автономністю алгоритмів, здатних до самостійної корекції поведінки під час машинного навчання, що ставить під сумнів ефективність людського контролю та вимагає від держави формування такого наглядового механізму, який би гарантував безпеку, не стримуючи

при цьому технологічний прогрес[7, с. 62]. Системи ШІ, навчені на упереджених даних, можуть відтворювати або посилювати соціальну нерівність, що призводить до дискримінації за різними ознаками[8, с. 11]. Ситуацію ускладнює непрозорість процесів прийняття рішень і відсутність ефективних механізмів їх оскарження, а також недостатнє нормативне регулювання у сфері запобігання алгоритмічній упередженості. Слід також зазначити, що ще одним ризиком щодо впровадження ШІ є дефіцит кваліфікованих спеціалістів, здатних ефективно працювати з технологіями штучного інтелекту [4, с. 4].

Щодо перспектив використання ШІ у сфері кібербезпеки, слід наголосити, що подальше впровадження штучного інтелекту в дану сферу потребує комплексного підходу, що поєднує технології, організацію та навчання. Ключовим є створення національних платформ кіберзахисту з інтегрованими алгоритмами ШІ для виявлення та запобігання потенційним загрозам у реальному часі, автоматизації реагування та об'єднання даних із різних джерел. Тобто, штучний інтелект дозволяє швидше виявляти нові загрози, зменшувати час реагування на них та підвищувати стійкість кіберсистем державних інституцій, при цьому зберігаючи людський контроль та дотримуючись етичних і правових норм.

Отже, використання штучного інтелекту в сфері кібербезпеки є критично необхідним для запобігання цифровим загрозам, особливо в умовах воєнного стану, оскільки дозволяє автоматизувати виявлення кібератак у реальному часі. Проте нормативно-правове регулювання використання систем штучного інтелекту в Україні залишається недостатнім. Подальший розвиток даної галузі має базуватися на створенні єдиних національних платформ кіберзахисту за умови збереження пріоритету людського контролю над критичними процесами та чіткого дотримання прав людини.

ЛІТЕРАТУРА:

1. Про схвалення Концепції розвитку штучного інтелекту в Україні: розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: <https://zakon.rada.gov.ua/laws/show/1556-2020%D1%80#Tex>

2. Інтеграція систем штучного інтелекту в державне управління: ризики, правові виклики та безпекові гарантії. *Вісник кримінологічної асоціації України*. 2026. № 35(2). С. 574-585.
3. Лисецький Ю. М. Штучний інтелект у кібербезпеці. *Інформаційні системи і технології*. 2025. № 3. С. 94-97.
4. Трофименко, О. Г., Соколов, А. В., Чикунів, П. О., Ахметьєва, Г. В., Манаков С. Ю. Штучний інтелект у військовій кіберсфері. *Технології та інжиніринг*. 2024. № 4(21). С. 85–92.
5. Пантюшенко Р., Чайка Ю. Штучний інтелект у сфері кібербезпеки: інновації, виклики та перспективи розвитку. *Military Science*. 2024. С. 200-209.
6. Фединець Н.І., Сорока А.А. Використання штучного інтелекту для виявлення та реагування на кіберзагрози під час війни. *Інформаційна безпека та інформаційні технології*. 2025. С. 453.
7. Пузирний В.Ф., Захарчук І.В. Правові аспекти використання штучного інтелекту у сфері кібербезпеки: регулювання та етичні дилеми. *Науковий вісник Сіверщини*. 2025. № 3. С. 58-69.
8. Мохначук С.В., Ломака І.І. Визначення правового статусу штучного інтелекту в контексті порушення прав людини. *Інформаційне право*. 2025. DOI: <https://doi.org/10.5281/zenodo.16869109>.

ЗМІСТ

ПЕРЕДМОВА.....	4
<i>Берназ-Лукавецька Олена Михайлівна</i> ВИНИКНЕННЯ КРЕДИТНИХ ВІДНОСИН В УМОВАХ ВОЄННОГО СТАНУ	6
<i>Бігняк Олександр Валентинович</i> ТРАНСФОРМАЦІЯ ПРАВ УЧАСНИКІВ ТА ПРИХОВАНА ЦЕНТРАЛІЗАЦІЯ У СИСТЕМІ ВЧ ЯДУВАННЯ ДАО	9
<i>Брага Аліна Анатоліївна</i> ЦИФРОВА СПАДЩИНА, ЯК ВИКЛИК ДОКТРИНИ НЕСПАДКОВУВАНOSTІ ОСОБИСТИХ НЕМАЙНОВИХ ПРАВ	13
<i>Булеца Сибілла Богданівна</i> МІСЦЕ АНАТОМІЧНИХ МАТЕРІАЛІВ ЛЮДИНИ В МОДЕЛЬНИХ ПРАВИЛАХ РЕЧЕВОГО ПРАВА	18
<i>Вовчок Руслан Володимирович</i> КІБЕРІНЦИДЕНТИ ЯК ОБСТАВИНИ НЕПЕРЕБОРНОЇ СИЛИ В ІТ-ДОГОВОРАХ.....	26
<i>Галупова Лариса Ігорівна, Мартинюк Іван Вікторович,</i> НАВЧАЛЬНІ ДАТАСЕТИ У СИСТЕМАХ ШТУЧНОГО ІНТЕЛЕКТУ ЯК ОБ'ЄКТИ АВТОРСЬКО-ПРАВОВОЇ ОХОРОНИ	32
<i>Глиняна Катерина Михайлівна</i> ЦИФРОВА ІДЕНТИЧНІСТЬ БАТЬКІВ І ДІТЕЙ ЯК ОБ'ЄКТ ЦИВІЛЬНО-ПРАВОВОЇ ОХОРОНИ	37
<i>Голубева Неллі Юріївна</i> ПРОБЛЕМИ АВТОМАТИЗОВАНОГО УКЛАДАННЯ ДОГОВОРІВ.....	41
<i>Давидова Ірина Віталівна</i> РОЛЬ ЦИФРОВІЗАЦІЇ ПРАЦІ ПІД ЧАС ЗАХИСТУ МАЙНОВИХ І НЕМАЙНОВИХ ПРАВ НЕПОВНОЛІТНІХ	48
<i>Жорнокуй Юрій Михайлович</i> ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА ПРАВА ЛЮДИНИ: ПРОБЛЕМНІ ПИТАННЯ	54
<i>Журило Сергій Сергійович</i> ДО ПИТАННЯ ПРО ЕФЕКТИВНІСТЬ АНТИКОРУПЦІЙНОЇ ПОЛІТИКИ В СФЕРІ ПУБЛІЧНОГО УПРАВЛІННЯ	58
<i>Зубар Володимир Михайлович</i> БЛОКЧЕЙН ТА ЙОГО РОЛЬ У ТРАНСФОРМАЦІЇ КОРПОРАТИВНИХ ПРАВОВІДНОСИН.....	62
<i>Калітенко Оксана Михайлівна</i> ВРАЗЛИВІСТЬ ПРИВАТНОЇ ОСОБИ ПЕРЕД ЦИФРОВИМИ ЗАГРОЗАМИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ: ДО ФОРМУВАННЯ СУЧАСНОЇ ЦИВІЛІСТИЧНОЇ ДОКТРИНИ.....	66

<i>Кармолін Лев Маркович</i> ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПІД ЧАС ЗДІЙСНЕННЯ ПРАВСУДДЯ	71
<i>Кірсанов Олексій Володимирович, Берназ-Лукавецька Олена Михайлівна</i> ОКРЕМІ НЕСПРАВЕДЛИВІ УМОВИ КРЕДИТНОГО ДОГОВОРУ	74
<i>Кривенко Юлія Василівна</i> DEEPFAKE ЯК ПІДСТАВА ЦИВІЛЬНО-ПРАВОВОЇ ВІДПОВІДАЛЬНОСТІ: ВИКЛИКИ ГІБРИДНОЇ ВІЙНИ	77
<i>Ларіонов Владислав Сергійович</i> ПРАВОА ПРИРОДА ТА КЛАСИФІКАЦІЯ ЦИФРОВИХ РЕЧЕЙ У КОНТЕКСТІ ОНОВЛЕННЯ ЦИВІЛЬНОГО ЗАКОНОДАВСТВА УКРАЇНИ	80
<i>Маковій Віктор Петрович</i> ТРАНСФОРМАЦІЯ ПРАВОВОГО РЕГУЛЮВАННЯ ЦИФРОВОГО СЕРЕДОВИЩА З ОГЛЯДУ НА ПРОЄКТ КОДЕКСУ ПРАВА ПРИВАТНОГО	85
<i>Майданик Роман Андрійович</i> ШТУЧНИЙ ІНТЕЛЕКТ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я: АКТУАЛЬНІ ПИТАННЯ ПРАВА	90
<i>Матійко Микола Володимирович</i> ЩОДО ОКРЕМИХ АСПЕКТІВ РЕГУЛЯТИВНОГО ФУНКЦІОНУВАННЯ ЦИВІЛЬНОГО ПРАВА В СФЕРІ НАДАННЯ ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ ПОСЛУГ КІНЦЕВОМУ КОРИСТУВАЧУ	97
<i>Менджул Марія Василівна</i> ЗАХИСТ ДІТЕЙ ВІД ЦИФРОВОГО НАСИЛЬСТВА ЯКЕЛЕМЕНТ КІБЕРБЕЗПЕКИ	103
<i>Мусієнко Андрій Юрійович</i> ДО ПИТАННЯ ПРО РІЛЬ СУДОВОЇ ПРАКТИКИ В ПИТАННЯХ ЗАХИСТУ ПРАВ ВЛАСНИКІВ НЕЖИТЛОВИХ ПРИМІЩЕНЬ	107
<i>Орзіх Юрій Геннадійович</i> КРИПТОАКТИВИ ЯК ЦИФРОВА ВЛАСНІСТЬ В УМОВАХ ГІБРИДНОЇ ВІЙНИ: ПРАВО ВЛАСНОСТІ, ДОКАЗУВАННЯ КОНТРОЛЮ ТА AML/CFT-РИЗИКИ ...	111
<i>Рябченко Вікторія Олександрівна</i> ВИКОРИСТАННЯ ОНЛАЙН ІГОР ТА МЕСЕНДЖЕРІВ ЯК ІНСТРУМЕНТУ ВЕРБУВАННЯ: ВИКЛИКИ ДЛЯ ІТ-ПРАВА	116
<i>Савенко Дмитро Олександрович</i> ВИКОРИСТАННЯ OSINT ІНСТРУМЕНТІВ ДЛЯ ВИЯВЛЕННЯ ФЕЙКОВИХ НОВИН ТА ДЕЗІНФОРМАЦІЇ В УМОВАХ ГІБРИДНОЇ ВІЙНИ.	119
<i>Самойленко Георгій Валерійович</i> ВІДШКОДУВАННЯ ШКОДИ, ЗАВДАНОЇ ТЕРИТОРІАЛЬНИЙ ГРОМАДІ ЗБРОЙНОЮ АГРЕСІЄЮ РФ	122
<i>Станкевич Андрій Володимирович</i> ПРОБЛЕМИ ВИЗНАЧЕННЯ ШІ СУБ'ЄКТОМ ЕЛЕКТРОННОГО ОБІГУ ОБ'ЄКТІВ ЦИВІЛЬНОГО ПРАВА ЗА НАЦІОНАЛЬНИМ ЗАКОНОДАВСТВОМ ТА ЗАКОНОДАВСТВОМ ЄС	127
<i>Стрілець Михайло Ігорович</i> ДОВІРА ЯК ОСНОВА ФУНКЦІОНУВАННЯ ЕЛЕКТРОННОЇ КОМЕРЦІЇ	130

<i>Тітова Аліна Олексіївна</i> КЛАСИФІКАЦІЯ СПОСОБІВ МАНІПУЛЯЦІЇ ІНФОРМАЦІЄЮ	134
<i>Товт Тинде Олександрівна</i> ПРАВО НА ВІДПУСТКИ ДЛЯ НЕПОВНОЛІТНІХ ПРАЦІВНИКІВ ЗА ЗАКОНОДАВСТВОМ УКРАЇНИ ТА УГОРЩИНИ: ПОРІВНЯЛЬНИЙ АСПЕКТ	138
<i>Токарева Віра Олександрівна</i> ДО ПИТАННЯ РЕАЛІЗАЦІЇ ПРАВА НА ДОСТУП ДО ПЕРСОНАЛЬНИХ ДАНИХ.....	142
<i>Фасій Анастасія Володимирівна</i> МІЖНАРОДНІ СТАНДАРТИ ЗАХИСТУ ПСИХІЧНОГО ЗДОРОВ'Я В УМОВАХ РОЗВИТКУ ЦИФРОВИХ ТЕХНОЛОГІЙ	146
<i>Фасій Богдан Володимирович</i> САМОРЕГУЛЮВАННЯ ЯК СУЧАСНИЙ ІНСТРУМЕНТ ЦИВІЛЬНО-ПРАВОВОГО РЕГУЛЮВАННЯ	152
<i>Харитонов Євген Олегович</i> LAWFARE ШТУЧНОГО ІНТЕЛЕКТУ В УМОВАХ ГІБРИДНОЇ ВІЙНИ: ВИКЛИКИ ПРИВАТНОМУ ПРАВУ	158
<i>Харитонova Олена Іванівна</i> ПЛАТФОРМНА СПРАВЕДЛИВІСТЬ У ДОБУ ШТУЧНОГО ІНТЕЛЕКТУ: НОВІ МЕЖІ ВІДПОВІДАЛЬНОСТІ ТА ЗАХИСТУ ПРАВ КОРИСТУВАЧІВ.....	169
<i>Сівак Кристина Ігорівна</i> ЦИВІЛЬНО-ПРАВОВІ ЗАСАДИ УЧАСТІ ШТУЧНОГО ІНТЕЛЕКТУ В ПРИВАТНОПРАВОВІЙ СФЕРІ	174

НА ПОЧАТКУ НАУКОВОГО ШЛЯХУ

<i>Асцатрян Крістіна Сергіївна</i> НЕМАЙНОВІ ПРАВА ТА ОБОВ'ЯЗКИ БАТЬКІВ І ДІТЕЙ.....	178
<i>Базанова Аліна Андріївна</i> ВІДПОВІДАЛЬНІСТЬ ЗА ШКОДУ, ЗАВДАНУ СИСТЕМАМИ ШТУЧНОГО ІНТЕЛЕКТУ В УМОВАХ ВІЙНИ.....	183
<i>Балик Даша Вікторівна</i> КІБЕРБЕЗПЕКА ЯК ЕЛЕМЕНТ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ.....	186
<i>Василенко Олександра Іванівна</i> ІМ'Я ЯК ЮРИДИЧНА ІДЕНТИЧНІСТЬ ОСОБИ	188
<i>Возняк Інна Романівна</i> ПРАВА ПОДРУЖЖЯ НА ЧАСТКУ В ТОВАРИСТВІ З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ	190
<i>Гагарова Олександра Андріївна</i> ПРАВОВЕ РЕГУЛЮВАННЯ РЕКЛАМНОГО КОНТЕНТУ, СТВОРЕНОГО ГЕНЕРАТИВНИМ ШІ	194

<i>Гачук Дар'я Сергіївна</i> РЕКВІЗИЦІЯ ГРОШОВИХ КОШТІВ В УМОВАХ ВОЄННОГО СТАНУ В УКРАЇНІ	199
<i>Журило Євгенія Сергіївна</i> ПОНЯТТЯ ТА СУТЬ ЦИВІЛЬНИХ ПРАВОВІДНОСИН.....	203
<i>Заборська Ксенія Андріївна</i> ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМАХ КІБЕРРОЗВІДКИ: ПРАВОВІ ВИКЛИКИ ТА РЕГУЛЯТОРНІ ПІДХОДИ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ.....	206
<i>Казарян Ліліт Романівна</i> СПАДКУВАННЯ МАЙНА, ЩО ЗНАХОДИТЬСЯ НА ТИМЧАСОВО ОКУПОВАНИХ ТЕРИТОРІЯХ: ПРОБЛЕМИ ТА СПЕЦИФІКА	209
<i>Калова Вікторія Сергіївна</i> ЦИВІЛЬНО-ПРАВОВІ ОСОБЛИВОСТІ ДОГОВОРІВ У СФЕРІ КІБЕРБЕЗПЕКИ	212
<i>Коваленко Ростислав Русланович</i> УСУНЕННЯ ВІД ПРАВА НА СПАДКУВАННЯ	218
<i>Коцар Георгій Андрійович</i> САМОЗАХИСТ ЯК ФОРМА ЗАХИСТУ У ЦИВІЛЬНОМУ ПРАВІ	222
<i>Крупеня Вероніка Олегівна</i> ПОРУШЕННЯ АВТОРСЬКИХ ПРАВ У СОЦІАЛЬНИХ МЕРЕЖАХ: ЦИВІЛЬНО-ПРАВОВИЙ АСПЕКТ	225
<i>Лашин Костянтин Анатолійович</i> ДОКАЗУВАННЯ У СПРАВАХ ПРО ВИТРЕБУВАННЯ МАЙНА З ЧУЖОГО НЕЗАКОННОГО ВОЛОДІННЯ	228
<i>Лук'яненко Валерія Станіславівна</i> ОПІКА ТА ПІКЛУВАННЯ В УКРАЇНІ: ПРАВОВА БАЗА ЧИ РЕАЛЬНА ДОПОМОГА ПІДОПІЧНИМ?.....	232
<i>Мазниця Дарина Сергіївна</i> ПОНЯТТЯ ТА ВИДИ ЦИФРОВИХ РЕЧЕЙ.....	236
<i>Мінько Ірина Василівна</i> ЦИВІЛЬНО-ПРАВОВІ АСПЕКТИ ЗАХИСТУ ПРИВАТНОСТІ В УМОВАХ ЦИФРОВІЗАЦІЇ СУСПІЛЬСТВА	239
<i>Носалюк Даніїл Артемович</i> РЕЧІ ЯК ОСНОВНИЙ ОБ'ЄКТ ЦИВІЛЬНИХ ПРАВ	241
<i>Одинська Юлія Дмитрівна</i> ЗАПОВІТ ЯК ОДНОСТОРОННІЙ ПРАВОЧИН.....	246
<i>Олійник Катерина Дмитрівна</i> СОЦІАЛЬНІ МЕРЕЖІ ТА ПРАВО: МЕЖІ СВОБОДИ СЛОВА	250
<i>Олійарчик Аліна Віталіївна</i> КІБЕРБУЛІНГ ЯК НОВИЙ ВИКЛИК ДЛЯ ЗАХИСТУ ПРАВ ПРИВАТНОЇ ОСОБИ У ЦИФРОВОМУ СЕРЕДОВИЩІ	253

<i>Півторак Анастасія Олександрівна</i> ЦИФРОВІ ПРАВА ЛЮДИНИ У КІБЕРПРОСТОРІ: СУЧАСНІ ВИКЛИКИ ПРАВОВОГО РЕГУЛЮВАННЯ	257
<i>Подцерковна Поліна Олегівна</i> ПРАВИЛА INCOTERMS ЯК ДЖЕРЕЛО ЦИВІЛЬНОГО ПРАВА	262
<i>Прокопчук Вікторія Сергіївна</i> ПРАВОВИЙ СТАТУС КУЛЬТУРНИХ ЦІННОСТЕЙ У ЦИВІЛЬНОМУ ОБОРОТІ	264
<i>Рижук Єлизавета Вікторівна</i> ЕЛЕКТРОННІ ДОГОВОРИ: ПРОБЛЕМИ ДОКАЗУВАННЯ ТА ПРАВОВОГО РЕГУЛЮВАННЯ.....	267
<i>Стефанський Михайло Андрійович</i> ЦИФРОВІ ДОКАЗИ У СУДОВОМУ ПРОЦЕСІ: ПРОБЛЕМИ ВИКОРИСТАННЯ ТА ПРАВОВОГО РЕГУЛЮВАННЯ	270
<i>Сухомлин Владислава Вітлайівна</i> ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ: СУЧАСНИЙ СТАН ТА ПРОБЛЕМИ.....	274
<i>Татарінцева Дарина Ігорівна</i> ЦИВІЛЬНО-ПРОВА ХАРАКТЕРИСТИКА СУПЕРФІЦІО: СУЧАСНІ ВИКЛИКИ ПРАВОЗАСТОСУВАННЯ.....	278
<i>Толкачова Тетяна Андріївна</i> ПОНЯТТЯ МАЙНА У ЦИВІЛЬНОМУ ПРАВІ	282
<i>Чурсова Таїсія Миколаївна</i> КІБЕРБУЛІНГ ЯК НОВИЙ ВИКЛИК ДЛЯ ЗАХИСТУ ПРАВ ПРИВАТНОЇ ОСОБИ У ЦИФРОВОМУ СЕРЕДОВИЩІ	286
<i>Шарко Світлана Василівна</i> ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У СФЕРІ КІБЕРБЕЗПЕКИ: ПРАВОВІ РИЗИКИ ТА ПЕРСПЕКТИВИ	288

Наукове видання

ІТ-ПРАВО, КІБЕРБЕЗПЕКА ТА ШІ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

МАТЕРІАЛИ

Всеукраїнської наукової конференції

Одеса, 28 березня 2026 р.

За загальною редакцією

доктора юридичних наук, професора Є. Харитонова,
докторки юридичних наук, професорки І. Давидової

Електронне видання

Ум-друк. арк. 18,5.
Зам. № 2606-01.

Видавець ПП «Фенікс»
(Свідоцтво суб'єкта видавничої справи ДК № 1044 від 17.09.02).
Україна, м. Одеса, 65009, вул. Зоопаркова, 25.
e-mail: fenix-izd@ukr.net