

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

Кафедра цивільного права

ІТ-ПРАВО ТА КІБЕРБЕЗПЕКА В УМОВАХ ГІБРИДНОЇ ВІЙНИ

**МАТЕРІАЛИ
Всеукраїнського круглого столу**

Одеса,
12 квітня 2025 року

Одеса
Фенікс
2025

УДК 342.95 : 343.32 (477): 351.863
I-52

За загальною редакцією

доктора юридичних наук, професора **Є. Харитонова**,
кандидатки юридичних наук, доцентки **Ю. Кривенко**.

Упорядники-укладачі:

Кривенко Юлія – к.ю.н., доцентка кафедри цивільного права Національного університету «Одеська юридична академія», доцентка;

Лешкова Єлизавета – лаборантка кафедри цивільного права Національного університету «Одеська юридична академія».

ІТ-право та кібербезпека в умовах гібридної війни :
I-52 матеріали Всеукр. круглого столу (м. Одеса, 12 квіт. 2025 р.) / за заг. ред.: Є. О. Харитонова, Ю. Кривенко ; кафедра цив. права НУ «Одес. юрид. академія». – Одеса : Фенікс, 2025. – 138 с. – Режим доступу:

ISBN 978-617-8430-57-3

Збірник містить матеріали доповідей з теоретичних, історичних і методологічних проблем ІТ-права та кібербезпеки, які були оприлюднені на Всеукраїнському круглому столі «ІТ-право та кібербезпека в умовах гібридної війни» 12 квітня 2025 у Національному університеті «Одеська юридична академія».

Збірник спрямований на ознайомлення громадськості з дослідженнями науковців у сфері ІТ-права та кібербезпеки і може бути корисний як у навчальному процесі, так і в практичній діяльності.

УДК 342.95 : 343.32 (477): 351.863

*Матеріали видано в авторській редакції.
Повну відповідальність за достовірність та якість поданого матеріалу несуть
учасники конференції, їхні наукові керівники, рецензенти,
які рекомендували ці матеріали до друку.*

ISBN 978-617-8430-57-3

© Колектив авторів, 2025

© НУ «Одеська юридична академія»,
2025

Голова оргкомітету:

Харитонов Євгеній – завідувач кафедри цивільного права, професор, д.ю.н.

Заступник голови оргкомітету:

Матійко Микола – доцент кафедри цивільного права, доцент, к.ю.н.

Члени оргкомітету:

Харитонova Олена – завідувачка кафедри права інтелектуальної власності і патентної юстиції, професорка, д.ю.н.;

Давидова Ірина – професорка кафедри цивільного права, професорка, д.ю.н.;

Сафончик Оксана – професорка кафедри цивільного права, професорка, д.ю.н.;

Токарева Віра – доцентка кафедри цивільного права, доцентка, к.ю.н.;

Павлова Вікторія – доцентка кафедри цивільного права, доцентка, к.ю.н.;

Шамота Олександр – асистент кафедри цивільного права;

Лешкова Єлизавета – лаборантка кафедри цивільного права.

ПЕРЕДМОВА

Однією з найдинамічніших глобальних тенденцій поточного десятиліття є цифровізація. Тотальне її проникнення у життя сучасного суспільства сформувало нову реальність, особливості якої полягають у використанні цифрових технологій у всіх сферах життєдіяльності людини, що, своєю чергою, сприяє активному розвитку людського капіталу, модернізації економіки, трансформації державних та громадських інститутів та, відповідно, покращенню умов повсякденного життя громадян.

Процеси цифровізації змінюють предмет правового регулювання суспільних відносин, розширюючи його межі та зміст. З появою нових правовідносин виникає безліч правових проблем, які часто вирішуються методом спроб та помилок через відсутність готових правових доктрин. Законодавець не завжди здатний оперативно та точно врегулювати нові явища.

Сучасна глобальна стратегія розвитку суспільства орієнтована на цифрову трансформацію всіх сфер життя, що, в свою чергу, актуалізує питання кібербезпеки. Розвиток цифрових технологій породжує нові правові явища: нові суб'єкти і об'єкти права, цифрові права, електронні підписи, смарт-контракти тощо.

Інформаційні технології проникають в усі галузі – від економіки та державного управління до оборони і безпеки. Створення кіберпростору та розвиток технологій, таких як блокчейн, вимагають нового підходу до правового регулювання.

Інтернет став ареною нових ризиків: питання захисту персональних даних, боротьби з кіберзлочинністю та регулювання інтелектуальної власності потребують комплексного перегляду законодавства.

Змінився також і характер ведення бойових дій: війни стали мережевими, де інформація відіграє вирішальну роль. Гібридна війна передбачає маніпуляцію свідомістю людей через інформацій-

ні технології, що має глобальні наслідки, адже Інтернет не обмежується державними кордонами.

З початку XXI століття інформаційні технології міцно укорінилися не тільки на рівні звичайних соціальних відносин, а й стали одним із методів ведення гібридних воєн. Інформація стала сильним чинником світової політики, надаючи значний вплив на формування відносин між державами.

Інформаційний чинник є однією з ключових складових гібридної війни. Війни такого типу супроводжуються використанням масових маніпулятивних технологій, спрямованого інформаційного впливу на свідомість людей з урахуванням їх психологічних, вікових, гендерних та інших особливостей. Оскільки Інтернет є мережею без державних кордонів, «інформаційні війни» не обмежуються певними територіями, а охоплюють увесь світ.

Цифровізація та гібридні війни як нові виклики сучасному праву вимагають від юристів, науковців та законодавців швидкої адаптації та розробки нових правових механізмів і норм, що сприятимуть захисту прав людини та забезпеченню стійкості суспільства у нових умовах.

Відповідно до актуальності окреслених проблем і завдань, була проведена наукова конференція, матеріали якої вміщено у даному збірнику. Вони відображають сучасний стан досліджень у сфері ІТ права в умовах гібридної війни та пропонують шляхи вдосконалення правового регулювання у цій сфері.

Євген Харитонов

*доктор юридичних наук, професор,
член-кореспондент НАПрН України*

Юлія Кривенко

кандидатка юридичних наук, доцентка

Харитонов Євген Олегович,
*доктор юридичних наук, професор, член-кореспондент НАПрН України,
зав. кафедри цивільного права Національного університету
«Одеська юридична академія»*

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ: ПРАВОВІ ПРОБЛЕМИ

Сутність російсько-українського конфлікту як «гібридної» війни охарактеризована у позиції Міністерства закордонних справ України наступним чином: «Збройна агресія є лише одним з елементів гібридної війни Росії проти України. Іншими елементами стали: 1) пропаганда, що базується на брехні та підміні понять; 2) торговельно-економічний тиск; 3) енергетична блокада; 4) терор і залякування громадян України; 5) кібератаки; 6) категоричне заперечення самого факту війни попри наявність безлічі неспростовних доказів; 7) використання у своїх інтересах проросійських сил та держав-сателітів; 8) звинувачення іншої сторони у власних злочинах» [1].

Слід нагадати, що Мирослав Попович ще у 2010 році у передмові до книги Володимира Горбуліна «Без права на покаєння» наголошував на тому, що: «майбутні конфлікти потребують насамперед високоточної зброї й розвиненої системи інформаційних технологій» [2, с. 5].

Інформаційні технології відіграють величезну роль у сучасних збройних конфліктах. При цьому Сенгер зазнач, що коли «десять років тому лише три-чотири країни володіли ефективною кіберзброєю, то зараз таких уже понад тридцять. Крива обсягу виробництва кіберзброї за останні десять років загалом нагадує траєкторію злету бойового літака. Нову зброю вже застосовували багато разів, навіть якщо результати були неоднозначні... США були одними з перших – створили так звані «Сили кібероперацій» ... Сучасні збройні сили будь-якої країни не можуть функціонувати без кіберарсеналу так само, як після 1918 року годі було уявити військо без літаків. Сьогодні, як і тоді, неможливо передбачити, наскільки цей винахід змінить застосування державних сил» [3, с. 19].

«Ми всі живемо в страху, що нашу залежність від цифрових технологій обернуть проти нас інші держави, які за останнє десятиліття знайшли нові способи продовжити давнє протистояння. Ми вже знаємо, що перед кіберзброєю, як і перед ядерною, усі рівні. І в нас є всі підстави непокоїтися, що через кілька років ця зброя вкупі зі штучним інтелектом діятиме настільки швидко, що люди не встигнуть ні усвідомити загрози, ні запобігти їй – тож атаки відбудуться і призведуть до ескалації конфлікту» [3, с. 21].

Отже зафіксуємо цю обставину, що зумовлює вищий ступінь загрози – такий, що може вийти з-під влади людини: поєднання кіберзброї зі штучним інтелектом. Цей випадок є головною гібридною загрозою, а відтак потребує адекватної /гібридної відповіді, зокрема, за допомогою юридичних заходів.

Ці юридичні заходи мають забезпечити «кібербезпеку» – стан захищеності кіберпростору від кібератак, за якого забезпечується його сталий розвиток, а також своєчасне виявлення, запобігання і нейтралізація реальних та потенційних функціонуванню його елементів» [4, с. 189]. «Кібербезпека» відповідно до положень Закону України «Про основні засади забезпечення кібербезпеки України» є захищеністю життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [5].

Стратегія національної безпеки України сучасними загрозами для національної безпеки України в інформаційній сфері визначила: 1) стрімкі технологічні зміни та зростання ролі інформаційних технологій у всіх сферах суспільного життя; 2) застосування росією інформаційної «зброї» у поєднанні з енергетичною для зміцнення позицій у Європі, її намагання впливати на внутрішню ситуацію у європейських державах, підживлення триваючих конфліктів, збільшення військової присутності у Східній Європі; 3) продовження російською федерацією гібридної війни проти України

шляхом системного застосування інформаційно-психологічних, кібернетичних, політичних, економічних і воєнних засобів для відновлення свого впливу на неї; 4) внутрішню і зовнішню деструктивну пропаганду, що розпалює ворожнечу, провокує конфлікти, підриває суспільну єдність, використовуючи суспільні суперечності в умовах відсутності цілісної інформаційної політики держави, слабкості системи стратегічних комунікацій; 5) недостатню ефективність державних органів, що ускладнює вироблення і реалізацію державною ефективною політики (зокрема в інформаційній сфері), є джерелом загроз незалежності України, її суверенітету і демократії; 6) посилення загроз для критичної інформаційної інфраструктури, пов'язаних із погіршенням її технічного стану, відсутністю інвестицій в її оновлення та розвиток, несанкціонованим втручанням у її функціонування, зокрема фізичним і кібернетичним, триваючими бойовими діями, а також тимчасовою окупацією частини території України.

Істотну кіберзагрозу становлять кібератаки – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [5].

Після повномасштабного вторгнення росії в Україну кількість кібератак на державні інформаційні системи та об'єкти критичної інформаційної інфраструктури України зросла втричі. 90% атак здійснюють військові хакери рф та білорусі, діяльність яких

фінансується владою. Основна ціль російських хакерів – цивільна інфраструктура. Вони намагаються завдати якомога більше шкоди звичайним людям шляхом як ракетних та інших обстрілів, так і кібератак [6].

Після початку повномасштабного російського вторгнення в Україні також значно зросла кількість випадків кібершахрайства. Про це повідомили учасники спільного прес-брифінгу РНБО, НБУ та «Київстар», який пройшов у Нацбанку 15 лютого 2023 року. Найпопулярнішим методом кібершахраїв під час війни став фішинг – збір персональної інформації громадян, у тому числі необхідної для доступу до фінансових акаунтів і облікових записів [7].

Використання кібератак у гібридних війнах ставить під сумнів спроможність ідеї самовпорядкування ІТ-сфери на сучасному етапі її розвитку. Можливо, це стане реальністю після того як штучний інтелект стане дужчим інтелекту людського і сформує свій ідеальний віртуальний світ.

Отже, загрози інформаційній безпеці не подолати лише за допомогою технічних засобів, оскільки останні можуть впливати лише на технічну складову ІТ-сфери, залишаючи поза увагою «соціальний елемент» яким є учасники відносин, що виникають у ІТ-сфері (у тому числі, програмісти, провайдери, користувачі тощо). Це не можна визнати виправданим, оскільки на даному етапі розвитку ІТ саме соціальний елемент є головним чинником порушення інформаційної безпеки.

У залежності від виду і джерел походження кіберзагрози для її попередження та ліквідації наслідків державою можуть бути використані різноманітні профілактичні, організаційні та правові засоби, нормативним підґрунтям визначення яких є Доктрина інформаційної безпеки України, ухвалена у грудні 2016 р. РНБО і введена в дію 25 лютого 2017 р. Указом Президента України. Ї хоча деякі експерти вважають, що Доктрина це лише декларація [8], однак слід визнати, що вона встановила достатньо чіткі орієнтири діяльності у цій галузі. Доповнив Доктрину Закон України «Про основні засади забезпечення кібербезпеки України», який визначив основні шляхи функціонування національної системи кібербезпеки.

Україна визнає загрози кібербезпеки як важливий аспект національної безпеки. Запровадження ефективних механізмів захисту від кібератак, підвищення кіберсвідомості людей та ефективна координація усіх суб'єктів кібербезпеки є пріоритетами.

ЛІТЕРАТУРА:

1. 10 фактів про збройну агресію Росії проти України. Опубліковано 09 грудня 2019 року о 14:10. URL: <https://mfa.gov.ua/10-faktiv-pro-zbroynu-agresiyu-rosiyi-proti-ukrayini>
2. Горбулін В. П. Без права на покаєння. Харків: Фоліо, 2010. 383 с.
3. Сенгер, Девід Е. Досконала зброя. Війна, саботаж і страх у кіберполюсі. пер. з англ. Вікторія Дедик: факт.ред.укр.вид Олександр Дедик і Олег Фешовець. Львів: Астролябія, 2022. 496 с.
4. Попова Т. В., Ліпкан В. А. Стратегічні комунікації. Словник. / за заг. ред. В. А. Ліпкана. К.: ФОП О. С. Ліпкан. 2016. 416 с.
5. Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. *Відомості Верховної Ради*. 2017. № 45. ст. 403. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
6. Вимоги до захисту інформації в інформаційних системах у воєнний час: роз'яснення Держспецзв'язку | Кабінет Міністрів України (kmu.gov.ua)
7. Бабенко М. Фейки, фішинг, крадіжка грошей із карт: у кібершахрайства в Україні російське коріння. URL: Кіберзлочини під час війни. Що таке і як працює фішинг (focus.ua)
8. Доктрина інформаційної безпеки України – це лише декларація – експерти. URL: <https://www.radiosvoboda.org/a/28336852.html>

Булеца Сібілла Богданівна,

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

ЦИФРОВІ АВАТАРИ: ОБ'ЄКТИ ЧИ СУБ'ЄКТИ ПРИВАТНОГО ПРАВА

Аватар у цифровому контексті – це віртуальне втілення особи у віртуальному середовищі, тобто її цифрова проекція. При цьому аватар може бути схожим на користувача або ж відрізнятися від нього. [1, с.18] Спочатку слово аватар мало переважно релігійне або духовне підґрунтя та зміст і означало сходження божества на землю, згідно з індуїзмом [2, с.72–73]. Свого сучасного значен-

ня слово «аватар» набуло приблизно з 1985 року, коли було створено Habitat – комп’ютерну рольову гру від Lucasfilm [3, с.28–29]. Зараз найпоширенішим є розуміння аватара як графічного зображення, пов’язаного з профілем користувача, яке використовується в онлайн-форумах, відеоіграх, програмах обміну миттєвими повідомленнями тощо.

На сьогодні використання аватарів у Метавсесвіті та його віртуальних онлайн-платформах окремо не врегульовано, тому визначити їх правовий режим за допомогою існуючих правових стандартів складно. Найбільше дискусій викликають питання їх правової природи, ідентичності та автономії [4, с.117–118]. З точки зору приватного права, ключове питання зосереджується на тому, чи слід розглядати аватари як речі (цифрові речі, цифровий контент, продукт або об’єкт інтелектуальної власності) чи їх слід вважати автономними особами з власним набором прав і обов’язків? Тож у науковій літературі продовжуються дискусії навколо основних підходів до визначення правового статусу аватарів:

1. *Аватари як цифрові речі* характеризуються наявністю стабільної (фіксованої) цифрової комбінації, що складається з унікальної послідовності нулів і одиниць, які можуть зберігатися на фізичному носії. Ця характеристика дозволяє аватарам підпорядковуватися існуючим законам, що регулюють права власності та авторські права, подібно до традиційних фізичних об’єктів. Такий підхід значно спрощує захист власності та прав інтелектуальної власності в цифровому просторі, пропонуючи чіткі та перевірені механізми правового захисту. Відмінності аватара як «цифрової речі» від «електронного контенту» полягають у можливостях трансформації та фіксації, що впливає на життєвий цикл аватара як інформаційного продукту. Ця динаміка вимагає адаптації правових норм, спрямованих на регулювання електронного контенту, щоб враховувати унікальні аспекти цифрової ідентифікації та власності [5, с.3].

2. *Аватари як продукти*. Іншим можливим підходом до встановлення правового режиму для аватарів (зокрема щодо цивільної

відповідальності) є визначення їх як продуктів. Згідно з даними Європейської комісії [6, с.27] така точка зору є переважаючою точкою зору, яку підтримують вчені-юристи щодо питання збитків, заподіяних роботами, оснащеними штучним інтелектом. Європейська комісія пропонує поширити цей вид відповідальності (за дефектні продукти та їх компоненти, навіть якщо вони в цифровій формі) на нові цифрові технології. Однак, складно узгодити концепцію аватара з концепцією «продукту», оскільки останній наразі визначається як рухоме майно, яке здебільшого стосується матеріальних благ (ст. 2 Директиви 85/374/CEE – Директива про відповідальність за продукт [7]). Крім цього, еволюція Метавсесвіту в бік децентралізації значно зменшує ймовірність ефективного пред'явлення претензії будь-кому, кого ми можемо визначити як виробника (тобто виробника чи імпортера аватара). Ідея класифікації аватарів як продуктів викликає серйозні занепокоєння також і щодо анонімності та захисту персональних даних, які онлайн-платформи наразі мають гарантувати своїм користувачам [4, с. 122].

3. *Аватари як цифрові проксі-сервери*, тобто розширення користувачів (людей, організацій чи систем штучного інтелекту, які ними керують), що не мають незалежного правового статусу. З цієї точки зору аватари підпадають під дію законодавства про інтелектуальну власність як твори їхніх користувачів, а будь-які юридичні претензії чи захист зрештою стосуватимуться людини чи юридичної особи, що стоїть за аватаром, а не самого аватару [8, с.4]. Наявність ознак оригінальності та об'єктивної форми дає змогу розглядати аватар як нетиповий об'єкт авторського права. При цьому правова охорона аватара може здійснюватися за двома правовими режимами: авторсько-правової охорони та інституту прав особливого роду (*sui generis*) [9, с.43].

4. *Аватари як цифрові активи*. Той факт, що аватар може бути цифровим активом у Метавсесвіті, створюючи таким чином унікальну та сумісну форму ідентифікації для користувачів, уже встановлено вченими-технологами. Аватар справді може функціонувати як невзаємозамінний токен (NFT), досягаючи сертифіко-

ваної унікальності та стаючи предметом ексклюзивного контролю, наданого користувачам, які є їхніми власниками. При цьому, якщо користувачі не вживають дій, які розкривають їхню особу в реальному світі під час придбання чи роботи з цифровим активом, наприклад, аватаром, їх анонімність зберігається, адже публічно відома лише адреса їх цифрового гаманця [4, с.123].

5. *Аватари як юридичні особи.* У Метавсесвіті майбутнього, ймовірно доцільно буде надати аватарам окрему правосуб'єктність. Зокрема якщо аватари у віртуальному світі зможуть функціонувати незалежно (до прикладу, аватар володітиме можливостями штучного інтелекту, постійно навчаючись), і в результаті самостійно прийматимуть рішення, то їх можна наділити статусом юридичної особи. Цю правосуб'єктність можна надати через процес реєстрації [10, с.472].

6. *Аватари як окремі особи.* Цей підхід є найбільш теоретичним і застосовується переважно у футуристичних сценаріях (наприклад, при обговоренні прав цифрових двійників). При такому підході вводиться нова концепція в законодавство: аватар як третій рід, що існує десь між речами та особами. Така категоризація може призвести до створення нової правової категорії під назвою «метаособа» [8, с.5]. При такому сценарії аватари потенційно можуть володіти правами та нести юридичну відповідальність за свої дії.

Щодо останніх двох підходів Резолюція Європейського парламенту від 17 січня 2024 року про політичні наслідки розвитку віртуальних світів – питання цивільного законодавства, права компаній, комерційної та інтелектуальної власності (2023/2062(INI)) (далі Резолюція) у пункті 21 підкреслює, що аватари не мають статусу юридичної особи, тому будь-які питання щодо їх правоздатності, прав, обов'язків і відповідальності потрібно вирішувати з посиланням на фізичних або юридичних осіб, які їх використовують. В той же час Резолюція зазначає, що в міру того, як віртуальні світи розвиваються і стають все складнішими, слід розглянути доцільність надання конкретного правового статусу аватарам

[11]. Враховуючи, що аватари теоретично можуть служити єдиною формою ідентифікації в Метавесвіті, майбутнє регулювання може передбачати, наприклад, створення реєстру аватарів у Метавесвіті, щоб кожен із них міг бути юридично визнаним, якщо він пов'язаний з фізичними чи юридичними особами; можливість – у виняткових випадках – підняти корпоративну завісу (яку можна швидше назвати завісою аватара), коли аватари використовуються окремими особами в образливий або шкідливий спосіб, тобто; або навіть придбання (можливо, обов'язкового) страхування цивільної відповідальності для полегшення компенсації збитків, які можуть завдати аватари [4, с.129].

У якості підсумку зазначимо, що в сьогоденні умовах аватар логічніше характеризувати як «річ», а не як «особу». Водночас не можна оминати увагою той факт, що унікальний досвід, який аватари забезпечують своїм користувачам, ускладнює їхню правову інтерпретацію в цифровому середовищі. Це зумовлено тим, що вони створюють відчуття реальної присутності у віртуальному просторі, що часто тісно переплітається з особистісною ідентичністю та репутацією реальної людини. Із зростанням можливостей аватарів та їхньої участі в творчих і економічних процесах виникає потреба адаптації правової системи до нових форм цифрової особистості. Для цього необхідне глибоке розуміння питань ідентичності й відповідальності у віртуальному просторі, щоб свобода дій у цифрових світах не призводила до негативних наслідків у реальному житті. Забезпечення цього балансу є критично важливим для збереження безпеки та цілісності як віртуальних, так і фізичних взаємодій. Крім цього, проблема транскордонного використання Метавесвіту та аватарів породжує нагальну потребу в розробці універсальної правової бази, яка б дозволяла регулювати ці питання на міжнародному рівні.

ЛІТЕРАТУРА:

1. Charles R. Macedo, Douglas A. Miro and Thomas Hart. The Metaverse: From Science Fiction to Commercial Reality – Protecting Intellectual Property in the Virtual Landscape. *Bright Ideas* (NYSBA). 31(1): 2022. P. 13–20.

2. Lochtefeld, James G. «Avatar». In *The illustrated encyclopedia of Hinduism*, vol. 1, *Rosen Publishing*, 2001, pp. 72–73.

3. Lee, Lik-Hang, et al. «All one needs to know about metaverse», *Op Cit*, pp. 28–29.

4. Arismendy Mengual, Lorena Maria, *A Legal Status for Avatars in the Metaverse from a Private Law Perspective* (April 09, 2024). pp. 117–118. URL: <https://ssrn.com/abstract=5053316>

5. Kostenko Oleksii, Dniprov Oleksii, Zhuravlov Dmytro. *Metaverse: Ensuring Legal Recognition of Avatars and Electronic Personalities Through a Cross-Border Personalized ID-code*. *International Journal of Innovative Technologies in Social Science*. 2024. 2(42). S.3. DOI:10.31435/rsglobal_ijitss/30062024/8141

6. European Commission, Directorate-General for Justice and Consumers, *Liability for artificial intelligence and other emerging digital technologies*. 2014. P. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2020/01-09/AI-report_EN.pdf

7. Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A01985L0374-19990604494rop> B. A. (2023) 1), C. 43.

8. Raposo, V.L., *Beyond Pixels and Profiles: Unveiling the Legal Identity of Avatars in the Metaverse*. *Proceedings of the International Congress Towards a Responsible Development of the Metaverse*, Alicante, 13–14 June 2024. P. 4

9. Кройтор В.А. Правова охорона аватара як нетипового об'єкта авторського права. *Вісник Харківського національного університету внутрішніх справ*, 102(3 (Part 1), 2023.

10. Cheong, B.C. Avatars in the metaverse: potential legal issues and remedies. *Int. Cybersecur. Law Rev.* 3, 2022. P. 472. URL: <https://doi.org/10.1365/s43439-022-00056-9>

11. Policy implications of the development of virtual worlds – civil, company, commercial and intellectual property law issues – European Parliament resolution of 17 January 2024 on policy implications of the development of virtual worlds – civil, company, commercial and intellectual property law issues (2023/2062(INI)). URL: <https://eur-lex.europa.eu/eli/C/2024/5720/oj/eng>

Голубєва Неллі Юріївна,

докторка юридичних наук, професорка, зав. кафедри цивільного, нотаріального та виконавчого процесу Національного університету «Одеська юридична академія», Заслужений юрист України, адвокат

РОЗВИТОК CROSS BORDER E-COMMERCE В УКРАЇНІ

За останні роки електронна комерція стала одним із найдинамічніших секторів економіки України. Згідно з аналітичними даними, у 2024 році українці придбали товарів та послуг на суму 239 млрд гривень засобами e-commerce, що на 25% більше, ніж у 2023 році [1].

Cross Border E-commerce (трансгранична електронна комерція) – це здійснення онлайн-торгівлі товарами чи послугами між продавцями та покупцями, що знаходяться у різних країнах. Для України це означає не тільки можливість купувати за кордоном пересічним українцям, а й можливість українським підприємцям та компаніям виходити на міжнародні ринки без необхідності фізичної присутності за кордоном.

Українці стають більш відкритими до онлайн-покупок, у тому числі на закордонних платформах, та купують мільйони товарів на міжнародних торговельних майданчиках AliExpress, eBay, Amazon, Temu. В Україні гранична межа неоподатковуваних товарів у міжнародних поштових відправленнях – 150 євро, попри ініціативи деяких імпортерів, які виступають за пониження цього порогу. Якщо сумарна фактурна вартість товарів перевищує еквівалент 150 євро, але не перевищує еквівалент 10000 євро, то такі товари оподатковуються ввізним митом за ставкою 10% (ст. 374 Митного кодексу України) та податком на додану вартість за ставкою 20% (ст. 193 Податкового кодексу України). Базою оподаткування для таких товарів є частина їх сумарної фактурної вартості, що перевищує еквівалент 150 євро [2]. Покупки в інтернет-магазині за статистикою не часто перевищують ці ліміти, тому, здійснюючи транскордонні онлайн-покупки, покупець платить тільки за товар та його доставку.

Особливо Cross Border Ecommerce важливий для B2B2C (від англ. business-to-business-to-consumer – бізнес-бізнес-споживач) –

модель бізнесу, яка поєднує B2B (бізнес для бізнесу) і B2C (бізнес для споживача), в якій продаж відбувається між двома компаніями, але з урахуванням запитів кінцевого споживача чи компанія (виробник або постачальник) співпрацює з іншою компанією (посередником або партнером) для доставки своїх продуктів або послуг кінцевому споживачеві.

B2B2C є трирівневою структурою, в якій ключовою фігурою виступає посередник, що працює забезпечує логістичний зв'язок між виробником та споживачем [3]. Наприклад, маркетплейс співпрацює з продавцями (B2B), які розміщують свої товари на платформі, а кінцеві споживачі купують ці товари через маркетплейс (B2C).

Ринок транскордонного B2B2C e-commerce активно зростає з 2020 року. Основними факторами розвитку даного сегменту є глобалізація, розвиток цифрових технологій, збільшення довіри споживачів до міжнародних покупок та покращення логістичних ланцюгів. B2B2C модель дозволяє компаніям інтегрувати продажі через платформи для кінцевих споживачів, пропонуючи більший вибір товарів і послуг на міжнародному рівні. Головними перевагами для продавців на cross-border є: 1) доступ до нових закордонних ринків; 2) посилення впізнаваності власного бренду на міжнародній арені та набуття репутації; 3) збільшення можливостей для продажу (більший доступ до нових споживчих ринків). Особливо цінними міжнародні електронні платформи є для малого та середнього бізнесу в епоху панування транснаціональних корпорацій. Завдяки B2B2C платформам вони отримують нові можливості виходу на міжнародні ринки без необхідності великих інвестицій у фізичну присутність на ринку кожної з країн. Основними факторами впливу на ринок в майбутньому є технологічний прогрес, що найбільше відобразатиметься в поширенні штучного інтелекту, який вивчатиме персоналізований досвід покупок та надаватиме кращі пропозиції продуктів. Також вплив матиме поширення повної реальності, що може дозволити людям бачити продукти в реальному житті онлайн [4].

Перевагами трансграничної електронної комерції для українських компаній є: по-перше, можливість виходу на нові ринки, а саме, відкриває доступ до мільйонів споживачів у Європі, США, Азії та інших регіонах; по-друге, гнучкість та низький поріг входу – достатньо зареєструватися на міжнародному маркетплейсі (Amazon, eBay, Etsy) та організувати логістику; по-третє, підвищення конкурентоспроможності, оскільки українські виробники отримують можливість конкурувати на рівних з міжнародними брендами.

Наприклад, на американському маркетплейсі Etsy (майданчик продажу товарів ручної роботи з усього світу) за даними Statista, у червні 2020 року українські продавці посідали дев'яте місце серед усіх країн на Etsy. На початок 2025 року, за даними Forbes, понад 20 тисяч українських підприємців використовують Amazon для продажу своїх товарів. На платформі Etsy, яка має понад 92 мільйони активних покупців та 7,5 мільйона продавців зі всього світу, має понад 50 тисяч українських магазинів, а на eBay, третій за популярністю платформі серед українських продавців, працюють понад 10 тисяч підприємців з України [5].

Щоб продавати послуги на іноземних сайтах, продавець має бути зареєстрований як суб'єкт підприємницької діяльності, у випадку, якщо це систематичний продаж, тобто 2 (на думку українських податківців), чи 3 та більше разів на рік (за актуальною судовою практикою).

Звернемо увагу на проект E-Export School від Укрпошти, який вже багато років проводить вебіари для підтримки малого й середнього бізнесу та вчить слухачів як ефективно експортувати товари з України та генерувати продажі на найпопулярніших світових маркетплейсах, в тому числі випускає відповідний довідник, в якому роз'яснено, наприклад, як організувати e-Export-бізнес для фізичної особи-підприємця, вибрати систему оподаткування, підібрати види економічної діяльності, як оформити відправлення вартістю до 150 та більше 150 євро від відправника ФОП чи юридичної особи, як акредитуватися на митниці, оформити вантажну митну деклара-

цію, отримати кошти на рахунок підприємця, документально оформити отримання коштів з-за кордону, правила використання рахунків для отримання виручки за e-Export, як отримати SWIFT переказ за інвойсом чи переказ за допомогою платіжних сервісів, як відбувається контроль та фінансовий моніторинг операцій з e-Export. Важливо також пам'ятати, що згідно з вимогами Закону України «Про валюту та валютні операції», кошти на рахунку в іноземній валюті можуть бути використані підприємцем лише для конвертації в національну валюту і подальшого зняття коштів у гривнях або для переказу за кордон для виконання імпортової операції [6].

Попри позитивні тенденції, розвиток Cross Border Ecommerce в Україні стикається з низкою проблем, в тому числі із недостатньою логістичною інфраструктурою, воєнними діями, побоюваннями щодо шахрайства при оплаті, недостатньою обізнаністю про процедури у різних країнах.

При формуванні підприємцями бізнес-стратегій, можна порадити їм звернути увагу на Азійсько-Тихоокеанський регіон, який демонструє найвищі показники розвитку електронної комерції, в тому числі cross-border. Населення цих країн активно використовує онлайн-магазини, а додатковими факторами розвитку виступають поширення цифрових платежів, економічний розвиток регіонів, збільшення доступу до інтернету та загальна популяризація електронної торгівлі. В Європі основними ринками e-commerce є Німеччина, Франція та Великобританія, що пов'язано з найбільшою чисельністю населення та платоспроможністю. Китай є основним постачальником на ринок Європи. На другому місці США. Країни Європи на ринку cross-border B2B2C e-commerce переважно торгують між собою, особливо країни-сусіди. На європейському ринку дуже розвинена модель B2C [7].

Cross Border Ecommerce – це потужний драйвер розвитку української економіки, який відкриває нові можливості для бізнесу та сприяє інтеграції України у світову цифрову економіку. Подолання існуючих викликів дозволить українським компаніям ефективніше конкурувати на глобальному ринку та забезпечить сталий розвиток електронної комерції в країні.

ЛІТЕРАТУРА:

1. Місюкевич В. Основні тенденції розвитку інтернет-торгівлі в Україні: матеріали І Міжнародної науково-практичної конференції ПДАУ, 15 лютого 2022 року. URL: <http://dspace.puet.edu.ua/bitstream/123456789/11932/3/конференція%20ПДАУ%202022%20Місюкевич.pdf>
2. Наказ Міністерства фінансів України від 02.12.2024 № 615 «Про внесення змін до форми рішення про визначення вартості товарів, що переміщуються (пересилаються) громадянами через митний кордон України, для цілей нарахування митних платежів»
3. Що таке B2B2C і чому ця модель ведення бізнесу так добре підходить FinTech. URL: <https://psm7.com/uk/analytics/chto-takoe-b2b2c-i-pochemu-eta-model-vedeniya-biznesa-tak-xorosho-podxodit-fintech.html>
4. Аналіз ринку cross-border B2B2C e-commerce. 2024 рік. URL: <https://pro-consulting.ua/ua/issledovanie-rynka/analiz-rynka-cross-border-v2v2s-e-commerce-2024-god>
5. Тренди українського e-commerce на 2025 год. URL: <https://elit-web.ua/blog/trendy-ukrainskogo-e-commerce-na-2025-god>
6. Як розпочати бізнес з України: юридичні, податкові та митні аспекти. Покроковий довідник з рекомендаціями, 2024. URL: <https://e-export.ukrposhta.ua/wp-content/themes/custom/assets/pdf/exporter-handbook-2024.pdf>
7. Аналіз ринку cross-border B2B2C e-commerce. 2024 рік. URL: <https://pro-consulting.ua/ua/issledovanie-rynka/analiz-rynka-cross-border-v2v2s-e-commerce-2024-god>

Давидова Ірина Віталівна,

докторка юридичних наук, професорка, професорка кафедри цивільного права Національного університету «Одеська юридична академія»

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ УКЛАДАННЯ СМАРТ-КОНТРАКТІВ

Сучасні технології стрімко змінюють механізми укладення та виконання договорів. Однією з таких інновацій є смарт-контракти, тобто самовиконувані цифрові угоди, які функціонують на основі блокчейн-технологій. Інтеграція штучного інтелекту в процес розробки, аналізу й автоматизації смарт-контрактів відкриває нові горизонти для підвищення ефективності, надійності та безпеки цифрових трансакцій.

Отже, можна виділити наступні підходи до розуміння терміну «смарт-контракт»: по-перше, як програмний код, що автоматично виконується при дотриманні визначених умов (його функціонування забезпечується децентралізованою мережею блокчейну); по-друге, як цифрову угоду, яка автоматично виконує умови, закладені в її коді. Такі контракти функціонують у децентралізованих середовищах, зокрема на платформах Ethereum, Binance Smart Chain, Solana тощо. Вони є незмінними, прозорими та виконуються без посередників.

Під терміном «штучний інтелект» розуміють: по-перше, сукупність алгоритмів і методів, які дозволяють комп'ютерним системам імітувати людський інтелект, включаючи навчання, логіку, прогнозування та прийняття рішень; по-друге, галузь комп'ютерної науки, яка створює системи, здатні до самостійного навчання, прийняття рішень, розпізнавання мовлення, зображень та логічного мислення. У поєднанні з блокчейн-технологіями штучний інтелект виступає інструментом для аналізу великих обсягів даних, автоматизованої генерації коду та виявлення аномалій.

Аналізуючи питання використання штучного інтелекту для укладення смарт-контрактів, можна виділити певні етапи життєвого циклу смарт-контрактів та можливість (перспективність) застосування штучного інтелекту на кожному з виокремлених етапів. До етапів життєвого циклу смарт-контрактів віднесемо їх розробку, аналіз та верифікацію, автоматизацію укладення угод, а також виконання та моніторинг.

Отже, на етапі розробки смарт-контрактів штучний інтелект може автоматично генерувати код смарт-контракту на основі текстового опису умов угоди. Наприклад, використання великих мовних моделей, таких як GPT, дозволяє конвертувати юридичну мову в код на мовах Solidity або Vyper. Наприклад, юридична компанія Legalese розробила платформу, що дозволяє створювати смарт-контракти за допомогою інтерфейсу природної мови (користувач просто вводить умови договору, а система генерує валідний код для Ethereum).

На етапі аналізу і верифікації смарт-контрактів штучний інтелект здатен виявляти логічні помилки, вразливості та невідповідності в коді контракту. Використання методів машинного навчання дозволяє аналізувати великі обсяги даних із попередніх контрактів та прогнозувати ризики, виявити вразливості до їх розгортання в мережі. Інструменти на базі штучного інтелекту вивчають тисячі попередніх смарт-контрактів, ідентифікуючи небезпечні шаблони. Наприклад, інструмент MythX (партнер ConsenSys) використовує штучний інтелект для автоматизованого аудиту смарт-контрактів, він аналізує код Solidity, виявляє помилки безпеки та пропонує виправлення.

На етапі автоматизованого укладення угод системи на базі штучного інтелекту можуть автоматично знаходити найвигідніші умови для укладення угоди (наприклад, у сфері децентралізованих фінансів), проводити переговори та адаптувати умови контракту під потреби сторін. Також штучний інтелект може виступати як інтелектуальний агент-посередник, який веде переговори між сторонами, формує оптимальні умови та укладає угоду. Такі агенти здатні оцінювати ринкові умови, враховувати юридичні обмеження і навіть використовувати блокчейн-орекли для отримання актуальної інформації. Наприклад, у децентралізованих фінансах платформа Kleros використовує штучний інтелект для вирішення спорів між сторонами смарт-контракту, залучаючи децентралізованих арбітрів.

Наостанок, на етапі виконання контрактів та проведення моніторингу інтелектуальні агенти можуть контролювати зовнішні дані (oracles), аналізувати їх та ініціювати виконання контракту при настанні обумовлених подій. Після активації смарт-контракту штучний інтелект може контролювати зовнішні джерела даних (наприклад, ціни з бірж, погодні умови, результати матчів) та запускати виконання контракту при настанні обумовлених умов. Наприклад, у сільськогосподарському страхуванні смарт-контракт може автоматично виплатити компенсацію фермеру у разі посухи, якщо погодний API повідомляє про відсутність дощів понад 30 днів

(штучний інтелект використовується для валідації даних та фільтрації аномалій).

До переваг інтеграції штучного інтелекту в роботу із смарт-контрактами можна віднести: автоматизацію юридичних процесів і зменшення людського чинника; підвищення безпеки за рахунок виявлення вразливостей до моменту публікації контракту; оптимізацію вартості укладення угод; гнучкість та адаптивність контрактів до динамічних умов; зменшення витрат внаслідок відсутності відсутності потреби у посередниках (нотаріуси, юристи); прогнозування ризиків, адже штучний інтелект може проаналізувати історію контрагентів та виявити шахрайські дії; масштабованість; юридична прозорість, адже коди відкриті для перевірки, а історія виконання незмінна.

Окрім переваг варто виділити й певні виклики та обмеження, які існують на практиці. Зокрема, сюди варто віднести: юридичну невизначеність (смарт-контракти та штучний інтелект не завжди мають чітке правове регулювання); проблема інтерпретації (автоматизовані контракти не завжди враховують неоднозначність юридичної мови); проблеми етики та довіри до автономних рішень, що приймаються штучним інтелектом; технічна складність у забезпеченні повної прозорості та пояснюваності рішень штучного інтелекту; питання безпеки (попри аудит, існує ймовірність хакерських атак через помилки в логіці контракту або алгоритмах штучного інтелекту).

Враховуючи перспективність даного напрямку, у майбутньому варто очікувати появу повністю автономних систем, які зможуть вести переговори, укласти угоди, перевіряти дотримання умов і забезпечувати виконання контрактів без втручання людини. Особливий інтерес викликає застосування генеративного ШІ для автоматичної розробки «легальних цифрових агентів» у сфері Web3. В межах зазначеного вважаємо за необхідне роботу в таких напрямках: розробка інструментів для підвищення довіри до рішень системи; створення стандартів юридичної відповідності для смарт-контрактів у різних юрисдикціях; вдосконалення багатомов-

них моделей, які дозволяють працювати з договорами у різних правових системах; інтеграція смарт-контрактів у системи цифрової ідентичності; розробка легальних агентів. Тобто штучного інтелекту, що може виступати в суді або арбітражі в якості сторони угоди.

Підводячи підсумок варто зазначити, що інтеграція штучного інтелекту в екосистему смарт-контрактів є логічним кроком на шляху до повної автоматизації юридичних і фінансових процесів у цифровому середовищі. Хоча існують певні бар'єри, потенціал цієї синергії обіцяє значне підвищення ефективності, безпеки та доступності правових механізмів у цифровій економіці.

Інтеграція штучного інтелекту в екосистему смарт-контрактів є потужним кроком до формування «розумної економіки», де угоди укладаються без конфліктів, з мінімальною участю людини. Водночас подальше поширення таких рішень потребує оновлення правового поля, удосконалення технологій безпеки та розвитку інфраструктури пояснюваних ШІ-систем.

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

ЦИФРОВІЗАЦІЯ ЯК ІНСТРУМЕНТ РЕАЛІЗАЦІЇ ПРАВА НА ОСВІТУ ДІТЕЙ В УМОВАХ ВІЙНИ

Повномасштабна війна в Україні завдала шкоди кожному українцю, особливо вразливі діти, які страждають від втрати дому, переміщення в середині країни, виїзд закордон, втрату зв'язків із рідними та близькими. Ведеться офіційна статистика щодо постраждалих від війни дітей і станом на 10 квітня 2025 року загинуло 616 дітей, зазнали поранень 1867 дітей, зникли безвісти 2072, постраждали від сексуального насильства – 19, депортовані та примусово переміщені – 19546 дітей [1]. На жаль, триває війна і статистика постійно зростає. Більше того, важко оцінити шкоду для дітей від перешкод у здійсненні основних прав.

Ми зупинимось на проблемі реалізації права на освіту дітей в умовах війни та процесах цифровізації. Якщо діти, які є місцевими мешканцями зазнали освітніх втрат виключно під час запровадження он-лайн навчання на початку повномасштабного вторгнення та перший рік війни, під час блекаутів, запровадження карантинних обмежень, для дітей-переселенців та тих що виїхали закордон, додаються також психологічні травми через втрату домівок, звичне середовище, мовні бар'єри.

За офіційною статистикою Департаменту соціального захисту населення Закарпатської ОДА на 3 лютого 2025 р. у Закарпатській області було на обліку 125003 внутрішньо переміщені особи (ВПО) з них найбільша кількість зосереджена в Ужгородській (27871 осіб), Мукачівській (15955 осіб) та Хустській (6574 осіб) територіальних громадах. Загалом в області 36556 дітей-переселенців, з яких за даними Департаменту освіти і науки, молоді та спорту Закарпатської ОДА 28670 – шкільного віку. З вказаної кількості переселенців у розрізі громад такі показники: Ужгородська громада – 7978 дітей (шкільного віку – 6205), Мукачівська громада – 4828 (шкільного віку – 3564), Хустська громада – 1628 дітей (шкільного віку – 1290).

В Ужгороді приймальною УГСПЛ було проведено моніторинг по питанню реалізації права на освіту дітей-переселенців в Ужгородській, Мукачівській та Хустській громадах. За результатами опитування батьків було отримано такі результати: 75.8% опитаних, вказали, що діти відвідують шкільні заклади у громадах, куди вони переїхали на проживання через війну; 74.2% опитаних, вказали, що дітям забезпечується безоплатне харчування у школах; 18.9% осіб мали перешкоди та труднощі при влаштуванні дітей до дошкільних навчальних закладів, зокрема через обмеженість місць; 31.8% опитаних мали труднощі із влаштуванням дітей до шкіл, натомість 56% не мали проблем. Щодо позашкільної освіти, то тільки 56% дітей мають доступ до такого виду освітніх послуг, інші обмежені у доступі із різних причин (фінансові труднощі, брак інформації).

Водночас вказана статистика насторожує, оскільки очевидно, що не всі діти охоплені офлайн освітою за місцем нового проживан-

ня. Наприклад, в Ужгороді офіційно зареєстровано 6205 дітей-ВПО шкільного віку, а зараховано до освітніх закладах міста – 2024 дитини ВПО, що становить 32,6% від всіх дітей шкільного віку. Подібна ситуація в м. Мукачеві, так на обліку офіційно перебуває 3564 дітей шкільного віку, а в школах офлайн навчається 902 дитини із статусом ВПО, що становить 25,3% від всіх дітей шкільного віку. Ще більш гірший показник у Хустській громаді. Так, на офіційному обліку перебуває 1290 дітей шкільного віку, у школах офлайн навчається тільки 175 дітей, що становить 13,56% від всіх дітей шкільного віку. Безумовно, це не означає, що діти не навчаються, більшість із них продовжують навчання у попередніх школах онлайн, водночас виникає питання щодо якості та системності такої освіти, більше того ускладнюється процес інтеграції.

Щодо дітей, які виїхали за межі України, то по статистиці Управління Верховного комісара ООН у справах біженців наприкінці липня 2024 року у Європі на обліку не менше 6,168 млн шукачів притулку [2]. Значну частку на себе прийняли такі країни як Польща, Німеччина, Іспанія, Італія, а також інші європейські держави. Переважають серед шукачів притулку із України (80 відсотків) жінки та діти, а також люди похилого віку [3].

За таких умов процеси цифровізації у освіті мають позитивні аспекти, насамперед дозволяють заповнити прогалини та освітні втрати через безкоштовні он-лайн освітні курси, онлайн-навчальні уроки, дозволяють надавати освітні послуги навіть в умовах повітряних тривог, інших обмежень, що унеможливають офлайн освіту. З іншого боку, необхідне підвищення спеціалізації для вчителів щодо дотримання кібергігієни, гарантування кібербезпеки, вироблення відповідних навичок щодо кібергігієни у учнів. Дистанційне навчання потребує постійного контролю та гарантування якості, адже воно стало ключовим для гарантування здобуття освіти для українських дітей, що виїхали закордон. При цьому, має бути максимальне спрощення процедури ЗНО із врахуванням освітніх втрат, виїздом сотней тисяч дітей у різні європейські держави, вочевидь необхідне спрощення правих вступу до ВНЗ аби створити умови для повернення молоді в Україну.

ЛІТЕРАТУРА:

1. Діти війни (2025). URL: <https://childrenofwar.gov.ua/>
2. Ukraine: Over 6 Million Refugees Spread Across Europe. URL: <https://unric.org/en/ukraine-over-6-million-refugees-spread-across-europe/>
3. Delivering Humanitarian Cash Transfers to Ukrainian refugees in Slovakia. URL: <https://www.unicef.org/hope-hct/stories/delivering-humanitarian-cash-transfers-ukrainian-refugees-slovakia>

Самойленко Георгій Валерійович

*доктор юридичних наук, професор, професор кафедри цивільного права
Запорізького національного університету*

ДО ПИТАННЯ ВИЗНАЧЕННЯ ПРАВОВОЇ ПРИРОДИ СТАРТАПУ

В довоєнний час прискорення та інтенсифікація бізнес-процесів відбулася, здебільшого, внаслідок науково-технічного прогресу. Це пов'язане з прагненням людини до заволодіння матеріальними ресурсами, що супроводжується пошуком способів досягнення зазначеної мети. Відомо, що в умовах конкуренції це можливо різними способами, – від економії ресурсів, оптимізації виробничих процесів, до пошуку нових інноваційних продуктів, впровадження нових та перспективних бізнес-ідей та проєктів. Як модель підприємницької діяльності, яка в деяких випадках здатна забезпечити реалізацію мети швидких та великих прибутків є бізнес-модель стартапу, що можливо завдяки масштабуванню впровадження такої моделі.

Звичайно, винайдення інноваційного продукту, бізнес-рішення, технологічного рішення та ін. не обмежується ІТ сферою, про що свідчать вдалі стартап-проєкти, використані в підприємницькій діяльності окремих суб'єктів. Держава не стоїть осторонь цих процесів, вдаючись до протекціонізму та фінансової підтримки окремих суб'єктів, які винаходять чи впроваджують стартап-проєкт. Так, в епоху, яка передувала стартапам, держава вдавалася до підтримки малого та середнього бізнесу, що сприяло поживленню та інтенсифікації підприємництва. Очікуваним наслідком було поживлення економіки, створення робочих місць, сплата податків.

Розуміння того, що пошук нових ідей, рішень, продуктів та їх комерціалізація, виведення в зовнішньоекономічну сферу може сприяти вирішенню макро- та мікроекономічних завдань, зокрема, у вигляді валютних надходжень до країни, мало наслідком створення джерельної бази правового регулювання інноваційної діяльності та венчурного підприємництва. Закономірно, що наступним кроком мало стати (як наслідок прогресу) правове регулювання стартапів. Нажаль, попри очікування, лише в поодиноких актах законодавства можна знайти згадку про стартапи. До того ж, і чинних актах, які приймалися в різні періоди, вбачаються різні підходи до розуміння їхньої економічної, та, відповідно, правової природи, внаслідок чого буває не достатньо зрозуміло, коли йдеться про стартапи, – про об'єкти чи про суб'єкти правовідносин. Так, і у випадку започаткування нового бізнесу, який використовує об'єкт права інтелектуальної власності, можливо, навіть як результату венчурного підприємництва, після його реалізації шляхом створення та реєстрації суб'єкта підприємництва (йдеться про юридичну особу), доволі часто такий суб'єкт разом з його активами та правами продається як «готовий» до використання бізнес. Звичайно, може йтися як про включення до числа учасників новоствореного товариства нових учасників (додаткових чи з виходом попередніх), що сприймається, як продаж бізнесу, що має перспективи прибутковості. Тож в різних аспектах іноді доволі важко розмежувати суб'єктів та об'єкти, особливо коли йдеться про стартапи. Так, Г.М. Сітченко було визначено стартап як: 1) реципієнта венчурних інвестицій (суб'єкта інвестиційної діяльності, власника або володільця об'єкту венчурного інвестування, який, в обмін на частки (акції) у статутному капіталі, одержав від інвестора майно, майнові права й інші цінності у власність чи у користування і використовує їх у своїй підприємницькій діяльності або в спільній підприємницькій діяльності з інвестором) [1, с. 3]; 2) об'єкт венчурного інвестування інноваційної діяльності) [2, с. 349–351].

В національному законодавстві в різні періоди стартап визначався як: проект, пов'язаний зі створенням та/або використанням

винаходів, корисних моделей, промислових зразків, ноу-хау та інших результатів інтелектуальної, творчої діяльності (Наказ Міністерства економічного розвитку і торгівлі України «Про затвердження Положення щодо конкурсного відбору проектів для державного стимулювання створення і використання винаходів (корисних моделей) та промислових зразків від 12.12.2018 р. № 1879; спеціалізоване мале інноваційне підприємство (Розпорядження КМУ «Про схвалення Стратегії розвитку сфери інноваційної діяльності на період до 2030 року» від 10 липня 2019 р. № 526-р); новостворене підприємство (Постанова КМУ «Про надання фінансової державної підтримки» від № 28 від 24.01.2020 р.); суб'єкт малого, середнього підприємництва або авторський колектив, до складу якого можуть входити здобувачі освіти (наукового ступеня), наукові, науково-педагогічні працівники та інші фізичні особи, діяльність якого спрямована на розроблення, створення, впровадження та реалізацію інноваційної продукції і пошук бізнес-моделі для подальшого її масштабування та розвитку, на використання та комерціалізацію науково-технічного (прикладного) результату (Постанова КМУ «Про реалізацію експериментального проекту щодо створення на базі закладів вищої освіти, наукових установ мережі стартап-шкіл – інкубаторів-акселераторів від 23.04.2024 р. № 430).

Зупиняючись на позиції розуміння стартапу як суб'єкта, що здійснює розробку та/чи впровадження стартап проекту, виходимо, в першу чергу, з його економічного розуміння, яке має свою мету, форми, методи, інструменти, моделі, та ін. (що дає привід окремим науковцям до визначення стартапу саме як форми підприємницької діяльності певного суб'єкта, а не самого суб'єкта) та правової форми, яка має забезпечити досягнення економічної мети в поєднанні з урегульованістю відносин як зовнішніх (як самостійного суб'єкта цивільних правовідносин з іншими учасниками), так і внутрішніх (організаційно-правової форми, корпоративних відносин, зокрема, щодо врегулювання питань як матеріальних, так і організаційних між розробниками (в т.ч. ідейними) стартап-проекту та його інвесторами).

Висловлюємо також позицію, що сприйняття стартапу виключно як юридичної особи наразі не є достатньо обґрунтованим через відсутність сприйняття економічної природи стартапу як бізнес-явища, пов'язаної не лише з командною роботою чи партнерством, але й способом залучення позичкового капіталу. Враховуючи, що засновник і одночасно реалізатор стартап-проекту може використати власний чи позичковий капітал, аргументуємо, що стартап-суб'єктом може бути як юридична, так і фізична особа, що обумовлено характером залучення коштів на реалізацію стартап-проекту.

Наведене дає підстави для висновку, що стартапом варто визнавати суб'єкта підприємницької діяльності (фізичну особу-підприємця, юридичну особу), що відповідає критеріям: 1) новоствореність; 2) інноваційна спрямованість діяльності; 3) діяльність колективу, спрямована на розробку, створення, впровадження та реалізацію інноваційної продукції і пошук бізнес-моделі для подальшого її масштабування та розвитку, використання та комерціалізацію прикладного науково-технічного результату. З метою усунення двозначних тлумачень запропоновано використовувати наступну термінологію: стартап-суб'єкт, – суб'єкт підприємництва, орієнтований на створення та впровадження стартап-проекту; стартап-проект – проект, орієнтований на розробку та впровадження інноваційного продукту, що поєднує розробку нових та/ чи впровадження існуючих бізнес-моделі, об'єкта права інтелектуальної власності, бізнес-рішення, технологічного рішення, тощо, з метою його комерціалізації та масштабування.

ЛІТЕРАТУРА:

1. Сітченко Г.М. Венчурне інвестування інноваційної діяльності: цивільно-правовий аспект. Дис. ...РHD: 081 «Право». Харків: Харківський національний університет внутрішніх справ, 2024. 226 с.
2. Сітченко Г.М. Стартап як об'єкт венчурного інвестування інноваційної діяльності. Учасники цивільних відносин: новації рекодифікації цивільного (приватного) права України: матеріали XIX наук.-практ. конф., присвяч. 99-й річниці з дня народж. д-ра юрид. наук, проф., чл.-кор. АН УРСР В.П. Маслова (Харків, 12 берез. 2021 р.). Харків: Право, 2021. С. 349–351.

Сафончик Оксана Іванівна,
*докторка юридичних наук, професорка, професорка кафедри цивільного
права Національного університету «Одеська юридична академія»*

ДЕЯКІ ПИТАННЯ ШЛЮБНИХ ПРАВОВІДНОСИН В ЦИФРОВУ ДОБУ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Гібридна війна між росією та Україною, яка розпочалася ще у 2014 році, суттєво вплинула на різні аспекти суспільного життя, включаючи шлюбні правовідносини. Збройний конфлікт, анексія Криму та бойові дії на Донбасі призвели до значних змін у демографічній ситуації, міграційних процесах та правовому регулюванні сімейних відносин.

Конфлікт спричинив масову міграцію населення з окупованих та прифронтових територій. Багато громадян стали ВПО (внутрішньо переміщена особа), що вплинуло на їхнє особисте життя та можливості укладення шлюбу. Зміна місця проживання, втрата документів та інші труднощі ускладнювали процес реєстрації шлюбів.

На територіях, тимчасово окупованих росією (Донецька, Луганська області, Крим, частини Запорізької та Херсонської областей), діють незаконні російські закони та процедури реєстрації актів цивільного стану.

Слід відмітити, що Україна не визнає документи, видані окупаційними адміністраціями, у тому числі свідоцтва про шлюб.

Люди, які уклали шлюб на тимчасово окупованій території, змушені звертатися до суду для його визнання відповідно до українського законодавства.

Шлюбні правовідносини формуються на основі сім'ї - соціального осередку, що є одним із найдавніших і водночас фундаментальних інститутів суспільства, який відіграє важливу роль у його функціонуванні та розвитку. Сім'я виконує не лише соціальну, а й демографічну функцію, забезпечуючи відтворення населення та передачу культурних, духовних і національних цінностей наступним поколінням. Завдяки складній системі внутрішніх і зовнішніх зв'язків, а також різноманітним соціальним функціям, сім'я надзви-

чайно чутливо реагує на будь-які трансформації соціального, економічного чи правового характеру, які безпосередньо впливають як на її становлення, так і на динаміку розвитку суспільства загалом.

На сьогодні питання визначення понять «сім'я» та «члени сім'ї» є предметом активного наукового обговорення серед дослідників-цивілістів, оскільки правове регулювання зазначених категорій виходить за межі норм виключно сімейного законодавства України й знаходить відображення у правових джерелах інших галузей права [1, с.105].

Оцінка та всебічний аналіз будь-яких правових інститутів сімейного права неможливі без чіткого розуміння змісту базового поняття «сім'я». Це поняття традиційно привертає увагу наукової спільноти не лише в межах юридичної науки, а й у дослідженнях представників філософії, демографії, соціології та інших галузей знань, включаючи фахівців у сфері сімейного права [2, с.101].

Формування сім'ї безпосередньо пов'язане з юридичним фактом укладення шлюбу, який є підставою для виникнення правових взаємин між її членами.

Сім'я – це соціальна спільнота, об'єднана різноманітними зв'язками [3, с.44–45], серед яких значна частина має емоційно-психологічний характер, а інші зумовлені моральними, матеріальними чи діловими чинниками. Особливе місце в ієрархії суспільних інститутів належить сім'ї як об'єднанню осіб, пов'язаних не лише емоційними зв'язками, але й системою взаємних прав та обов'язків, закріплених правовими нормами, які відповідають інтересам держави. Становлення, стабільність і функціональна спроможність сім'ї як соціального осередку безпосередньо впливають на загальний стан і добробут суспільства.

Згідно з загальновизнаними підходами, відображеними в юридичній літературі, сім'я визначається як мала соціальна група, що ґрунтується на шлюбному союзі, спільному веденні господарства та взаємній моральній відповідальності між її членами [4, с.68; 5, с.85–86]. Сім'я виступає первинною основою виникнення сімейних правовідносин і охоплює певне коло осіб, яке, хоча й окреслене нор-

мами сімейного законодавства України, проте не має вичерпного характеру.

Однією з ключових юридичних ознак сім'ї, з позиції сімейного права, є спільне проживання її членів. Намір жити разом зазвичай виступає однією з мотивацій до укладення шлюбу, тоді як його відсутність може свідчити про фіктивний характер такого правового зв'язку.

Шлюбні правовідносини мають переважно особистий характер, оскільки регламентують укладення, припинення шлюбу та особисто-правовий статус подружжя. Водночас лише другорядно ці правовідносини включають майнові аспекти, пов'язані зі спільною чи роздільною власністю подружжя, а також з аліментними зобов'язаннями. При цьому майнові правовідносини в межах сімейного права завжди тісно взаємопов'язані з особистими або безпосередньо з них випливають, тоді як у цивільному праві подібний зв'язок не є обов'язковим.

За загальним правилом, шлюбні права та обов'язки мають особистий, невідчужуваний характер, що виключає їх передачу іншим особам – такі права неможливо продати, подарувати чи заповісти. Це стосується і майнових прав та обов'язків, зокрема аліментних, які також є юридично невідчужуваними [6].

Гібридна війна суттєво змінила соціальну та правову реальність в Україні. Зміни у демографічній ситуації, міграційних процесах та доступі до державних послуг вплинули на можливості громадян вступати у шлюб.

На територіях, непідконтрольних українській владі, виник правовий вакуум. Там запроваджувалися нелегітимні норми та процедури, що не визнаються Україною та міжнародною спільнотою. Це створило проблеми з визнанням шлюбів, укладених у цих регіонах, на підконтрольній Україні території.

У відповідь на виклики війни, український уряд запровадив спрощені процедури реєстрації шлюбів для військовослужбовців та ВПО. Це дозволило швидше укласти шлюби в умовах невизначеності та підвищеного ризику.

Україна відреагувала на виклики війни та внесла зміни у законодавство, щоб полегшити процес одруження для військовослужбовців та громадян, які перебувають у небезпечних умовах.

Серед основних законодавчих змін слід відзначити такі:

Постанова Кабінету Міністрів України № 1024 від 2022 року дозволяла військовослужбовцям укласти шлюб без фізичної присутності. Військові, які перебувають у зоні бойових дій, можуть реєструвати шлюб через довірену особу або за допомогою відео зв'язку.[7]

Пілотний проєкт «Шлюб за добу», запущений ще у 2016 році, цей проєкт набув популярності серед військових і переселенців у зв'язку з війною. Дає змогу зареєструвати шлюб без дотримання стандартного місячного терміну очікування [8].

Бойові дії змусили багатьох переглянути пріоритети у житті, що призвело до збільшення кількості шлюбів серед військовослужбовців. Одруження може надавати додаткові соціальні гарантії, наприклад, право на отримання виплат у разі загибелі військового.

Війна підвищила рівень стресу та невизначеності, що в деяких випадках стимулює швидке укладення шлюбів. Експерти зазначають, що в умовах війни люди схильні прагнути стабільності у вигляді створення сім'ї.

Гібридна війна створила нові умови для виникнення шлюбних правовідносин в Україні. Вплив війни проявляється у збільшеній кількості шлюбів серед військових, міграційних викликах, спрощених процедурах укладення шлюбу, а також проблемах із визнанням шлюбів, зареєстрованих на окупованих територіях. Український уряд адаптував законодавство до нових умов, що сприяло збереженню інституту шлюбу навіть в умовах триваючої війни.

ЛІТЕРАТУРА:

1. Сімейне право: навч.-метод. посібник для здобув. вищої освіти ступеня «бакалавр», за спец. 081 «Право» / К. М. Глиняна, О. І. Сафончик, К. І. Спасова; Нац. ун-т «Одес. юрид. академія». 3-тє вид., перероб. Одеса: Фенікс, 2023.
2. Миронова Г. Моральні засади Сімейного кодексу України. Право України. 2004. № 4. С. 99–102/

3. Сімейне право України: Підручник /За ред. Є.О. Харитонова. Н.Ю. Голубевої. К.: Істина, 2010. 480с.

4. Дякович М.М. Сімейне право України: навчальний посібник. Харків: ЕКУС. 2022. 416 с. 116 с.

5. Сімейне право України: підручник /Л. М. Баранова та ін.; за заг. ред. В.І. Борисової, І.В. Жилінкової. 4-е вид., перероб. і допов. Харків: Право, 2012. 322 с.

6. Сімейне право України: підручник/ Дзера О.В., Боднар Т.В. Суми: Юрінком Інтер, 2020. 520 с.

7. Деякі питання державної реєстрації шлюбу в умовах воєнного стану: Постанова Кабінету Міністрів України від 7 березня 2022 р. № 213. URL: <https://zakon.rada.gov.ua/laws/show/213-2022-%D0%BF#Text> (втрата чинності 30.10.2024).

8. Шлюб за добу. Центральне міжрегіональне управління Міністерства юстиції України. URL: https://centraljust.gov.ua/dergavna_reestracia_aktiv_civil_stanu/shlyub_z_a_dobu

Харитонова Олена Іванівна,

докторка юридичних наук, професорка, членкиня-кореспондент НАПрН України, зав. кафедри інтелектуальної власності та патентної юстиції Національного університету «Одеська юридична академія»

БАГАТОАСПЕКТНІСТЬ РОЗУМІННЯ «ШТУЧНОГО ІНТЕЛЕКТУ»

Визначення поняття і правової природи штучного інтелекту є наразі як найбільш досліджуваною, так і найбільш недослідженою проблемою, оскільки до сьогодні відсутнє єдине розуміння цієї нової для права категорії.

При цьому слід взяти до уваги складність терміно-поняття «штучний інтелект», його багатоаспектність, оскільки він перестає бути лише технологічним інструментом, спричиняючи все більший вплив на гуманітарні науки: філософію, політологію, соціологію, культурологію і, звичайно, право. Тому штучний інтелект повинен розглядатися, як вище було зазначено, не лише як технологічний інструмент, а й як, можливо, в першу чергу, соціально-культурний феномен, що впливає на смислові ознаки та архітектуру, цінності, суспільну взаємодію та взаємовідносини, людську ідентичність, що аналізується у гуманітарному напрямку знання. Саме застосуван-

ня можливостей цього напрямку знання дозволить дослідити ШІ як явище, що впливає, змінює саме природу людського існування та всю сукупність взаємовідносин. Гуманітарний напрямок знання включає в себе: філософію, культурологію, історію, антропологію, лінгвістику, право та ін. [1].

З точки зору філософії найбільш цікавими питаннями є свідомість і моральність штучного інтелекту. Це ті два ключові аспекти, що відкриваються перед філософами та науковцями у контексті розвитку таких машин. Ці аспекти відзначаються складністю і спрямовані на відкриття нових можливостей та викликів у галузі філософії, технології і суспільства. Питання про свідомість штучного інтелекту викликає дуже глибокий інтерес. Чи може машина мати свідомість, або це властивість виключно біологічних істот? Чи можуть технологічні процеси мати свою власну сутність, чи вони лише є інструментами, створеними для виконання завдань, сформульованих людьми?

Крім цього, філософський аспект досліджує проблеми наявності сучасного антропоцентризму (принципу, згідно з яким людина є завершенням еволюції) та нових викликів щодо його сучасної реалізації. Тобто в межах цього аспекту досліджуються самостійні та взаємопов'язані питання, зокрема, про природу людини у «відносинах»: що відрізняє людину від «машини»; чи може мати машина в зв'язку з цим розум та свідомість, свободу волі, творчі здібності, зокрема, й інтелект? Тобто можна так поставити питання: чи відбувається сьогодні так звана «реконструкція» антропоцентризму, ставлячи, «завдяки» можливостям ШІ, під сумнів унікальність та самотутність людського розуму [1]?

Багато хто з філософів вважає, що штучний інтелект не може мати свідомості та самосвідомості, оскільки ці здатності пов'язані з біологічною природою людської розумової діяльності. Інші науковці наголошують, що розумна машина може їх мати, адже ці здатності залежать від певних фізичних процесів, таких як електричні сигнали в мозку, які схожі на ті, що виникають в мозку людини [2, с. 102]. Відповідно, у філософському контексті штучний

інтелект розглядається як широке поняття, що охоплює технології та інженерні системи, які відтворюють риси людського інтелекту. Це поняття пов'язане з нейрофізіологією, робототехнікою, психологією (зокрема розпізнаванням образів і моделюванням психічних процесів), трансгуманізмом і кібернетикою (використання обчислювальних ресурсів для виявлення закономірностей у великих масивах даних). Штучний інтелект трактується як програмна система, здатна автономно або напівавтономно взаємодіяти з навколишнім середовищем, генеруючи результати – прогнози, рекомендації чи рішення – з метою досягнення визначених цілей у процесі цифрової трансформації суспільства. [3, с. 73–74].

Психологія досліджує штучний інтелект у його співвідношенні з інтелектом людини, роблячи акцент на подібних і відмінних аспектах. Так, зокрема, Ю. Трофімов, порівнюючи поняття природного та штучного інтелекту, робить узагальнення, що поняття штучного інтелекту – це сучасний варіант «комп'ютерної метафори», за якої людину розглядають як канал передавання інформації, та разом зазначає, що проблема штучного інтелекту одна з важливих у царині когнітивної психології [4]. Відмічаючи деякі спільні характеристики, психологи зазначають, що є супутні явища, які на сучасному етапі розвитку науки недосяжні для штучного інтелекту. Зокрема, це мотивація, оскільки саме мотиваційні прагнення надають якість діям і «совість», хоча при цьому дослідники зазначають, що це істотна відмінність між інтелектом людини та штучним інтелектом, проте інтелект сам собою не може бути ані моральним, ані аморальним [5, с. 117]. Дослідження штучного інтелекту як категорії психології є важливими, адже оцінка безпечності та етичності використання технологій штучного інтелекту, їх впливу на людей належить, зокрема, до компетенції психологів [6].

Штучний інтелект є об'єктом вивчення комп'ютерної лінгвістики – галузі, що сформувалася ще у 1960-х роках як окрема дисципліна, яка досліджує мову, спираючись на знання з низки суміжних наук: філософії (зокрема методології та герменевтики), семіотики (науки про знакові системи), кібернетики (принципи управління

складними системами) та математики (математичні методи аналізу). У межах лінгвістики штучний інтелект розглядається як напрям комп'ютерної лінгвістики та інформатики, що зосереджується на формалізації завдань, подібних до людської когнітивної діяльності, зокрема здатності інженерних систем здобувати, обробляти, відтворювати й застосовувати знання й навички як на теоретичному, так і на практичному рівні. [7, с. 154].

Штучний інтелект істотно впливає на культуру, змінюючи підходи до створення, аналізу та тлумачення культурних явищ, а також переосмислюючи традиційне розуміння мистецьких творів. Однією з провідних сфер цих змін є музичне мистецтво, де ШІ виступає інструментом генерації нових композицій, що, у свою чергу, порушує питання унікальності та авторського права. [8, с. 75].

Релігія як сфера людської діяльності також зазнала впливу технологій штучного інтелекту, зокрема, у 2020 році Ватикан організував конференцію, у якій брали участь представники найбільш технологічних компаній, таких як IBM, Microsoft, FAO, і спільно з представниками Ватикану та уряду вони створили й підписали документ під назвою «Rome call for AI ethics» [9]. (The Call for AI Ethics, 2020), у якому йдеться про етичний підхід до використання ШІ і наголошується на необхідності винятково відповідального ставлення до таких технологій [10, с. 65].

Одним із напрацювань Ватикану у контексті ШІ є також нещодавня доктринальна записка 2025 року, що пропонує низку етичних рекомендацій щодо використання штучного інтелекту в різних сферах. Документ відображає прагнення Ватикану розглянути виклики сучасного технологічного прогресу в контексті морально-етичних цінностей, що можуть слугувати орієнтиром для відповідального розвитку ШІ.

Antiqua et Nova є спільною рефлексією Дикастерії доктрини віри та Дикастерії освіти і культури, закликає до того, щоб технології використовувались як інструмент для доповнення, а не заміни людського інтелекту. Автори документа вважають «оманливим» використання слова «інтелект» у контексті технологій ШІ. Хоча ШІ

здатний імітувати людський інтелект, виконуючи певні завдання, він залишається обмеженим «логічно-математичними рамками». Машинне навчання відрізняється від розвитку людського інтелекту, який формується досвідом, соціальною взаємодією та контекстом. Тому документ закликає розглядати ШІ не як форму, а як продукт людського інтелекту.

Як зазначається, в основі поглядів на штучний інтелект лежить імпліцитне припущення, що термін «інтелект» можна використовувати однаково для позначення як людського інтелекту, так і ШІ. Однак це не охоплює повного обсягу концепції. У випадку людей інтелект – це здатність, яка стосується людини в її повноті, тоді як у контексті штучного інтелекту «інтелект» розуміється функціонально, часто з припущенням, що діяльність, характерну для людського розуму, може бути розбита на оцифровані кроки, які машини можуть відтворити.

Навіть короткий огляд впливу штучного інтелекту на всі сфери суспільного життя свідчить про багатоаспектність його розуміння у різних галузях, в залежності від мети його використання і ролі, яка відводиться таким технологіям у різних сферах буття. Але звертає на себе увагу момент, що єднає у ставленні до такого бурхливого розвитку штучного інтелекту: побоювання стосовно набуття штучним інтелектом повної автономності і виходу з-під контролю людини. Тому необхідним є встановлення можливості регулювання тих процесів, які відбуваються за участі штучного інтелекту і встановлення ролі і місця останнього у праві і його взаємовідносин з людиною.

ЛІТЕРАТУРА:

1. Стрельцов Є.Л. Штучний інтелект з позицій феномена «кажана»: гуманітарне есе. Передмова Герберта Кюппера (Регенсбург, Німеччина), ЮВУ, № 2–4, січень – лютий 2025 року.
2. Бостром, Н. Суперінтелект. Стратегії і безпеки розвитку розумних машин (А. Ящук, А. Ящук, пер. з англ.). К.: Наш формат. 2020.
3. Vitalina Nikitenko, Valentyna Voronkova, Olga Kyvliuk, Roman Oleksenko, Valeria Suhenko. Philosophical reflection on artificial intelligence and its impact on the development of society, human, and education. Humanities Studies. 2024. Випуск 19 (96). С. 67–74.

4. Психологія: підручник [Ю.Л. Трофімов, В.В. Рибалка, П.А. Гончарук та ін.], за ред. Ю.Л. Трофімова. Київ: Либідь, 2008. 560 с.
5. Дерев'яно С. П., Примак Ю. В., Ющенко І. М. Штучний інтелект та емоційний штучний інтелект як феномени сучасної когнітивної психології. Наукові записки Національного університету «Острозька академія». Серія «Психологія»: науковий журнал. Острог: Вид-во НаУОА, червень 2020. № 11. С. 115–119.
6. Z. Abrams, «AI is changing every aspect of psychology. Here's what to watch for,» Monitor on Psychology, vol. 54, no. 5, Jul. 2023. [Електронний ресурс]. URL: <https://www.apa.org/monitor/2023/07/psychology-embracing-ai>
7. Пушик Н.В. Комп'ютерна лінгвістика та «штучний інтелект». «YoungScientist». № 2 (90). February, 2021. С. 151–155.
8. Антіпіна, І. Штучний інтелект як інструмент трансформації культурологічних ідей. Часопис Національної музичної академії України ім. П.І. Чайковського, 2024. № 3(64), С. 74–90. URL: [https://doi.org/10.31318/2414-052X.3\(64\).2024.314744](https://doi.org/10.31318/2414-052X.3(64).2024.314744)
9. The Call for AI Ethics. (2020). Rome Call for AI Ethics Foundation. URL: [https://www.romecall.org/the-call/Vernon, M. \(2023\). AI and Spiritual Intelligence. Beshara Magazine. URL: https://www.markvernon.com/ai-and-spiritual-intelligence; https://www.vatican.va/roman_curia/pontifical_academies/acdlife/documents/rc_pont-acd_life_doc_20202228_rome-call-for-ai-ethics_en.pdf](https://www.romecall.org/the-call/Vernon,%20M.(2023).%20AI%20and%20Spiritual%20Intelligence.%20Beshara%20Magazine.%20https://www.markvernon.com/ai-and-spiritual-intelligence;https://www.vatican.va/roman_curia/pontifical_academies/acdlife/documents/rc_pont-acd_life_doc_20202228_rome-call-for-ai-ethics_en.pdf)
10. Лавинюкова Анна-Валерія Робертівна. Можливості штучного інтелекту у вивченні релігійного досвіду. Культурологічний альманах. Вип. 4 (12), 2024. С. 64–69.
11. ANTIQUA ET NOVA. Примітка про взаємозв'язок між штучним інтелектом і інтелектом людини. URL.: https://www.vatican.va/roman_curia/congregations/cfaith/documents/rc_ddf_doc_20250128_antiqua-et-nova_en.html#Introduction

Берназ-Лукавецька Олена Михайлівна,

*кандидатка юридичних наук, доцентка, доцентка кафедри цивільного права
Національного університету «Одеська юридична академія»*

ОСОБЛИВОСТІ СТРАХУВАННЯ ПРОФЕСІЙНОЇ ВІДПОВІДАЛЬНОСТІ ІТ КОМПАНІЙ

Останнім часом набирає все більше популярності інститут страхування відповідальності, особливо страхування професійної відповідальності ІТ компаній. Існує багато ризиків, пов'язаних в ІТ індустрії, причому незалежно від того чи то розробник програм-

ного забезпечення чи то консультант. Давайте розберемося в чому полягають основні позитивні риси даного виду страхування.

Так, по-перше, це захист фінансових інтересів власника ІТ компанії, по-друге, можливість конкурентної переваги, а також виконання зобов'язань перед кредиторами (замовниками), контрагентами, партнерами.

На сьогодні таке страхування може застосовуватися у різних сферах. Наприклад, тиск і проблеми, з якими стикаються ІТ-фахівці. Якщо особа є ІТ підрядником або працівником, який працює в технологічній галузі, клієнти можуть звинуватити його у наданні небалого обслуговування або консультації, особливо коли «технологія» виходить з ладу чи не коректно працює і таким чином вжити проти добросовісного надавача послуг юридичних заходів по стягненню грошових коштів. Тому страхові компанії пропонують рівень покриття відповідно до потреб та асортимент продуктів страхування професійної відповідальності ІТ-підрядників поєднує в собі конкурентоспроможність із низкою додаткових переваг.

Багато видів бізнесу вимагають страхування відповідальності ІТ-професіоналів через продукти та послуги, які вони пропонують:

- фахівці з інформаційних технологій та програмного забезпечення, такі як дизайнери веб-сайтів, комп'ютерні консультанти, системні інтегратори, ІТ-підрядники, виробники обладнання та електронних компонентів.
- компанії, що постачають електроніку, наприклад побутову електроніку, комп'ютери, комунікаційне обладнання
- постачальники телекомунікаційних послуг і інтегрованих комунікаційних послуг, як-от оператори місцевого зв'язку, оператори міжміського зв'язку та постачальники послуг Інтернету/додатків.

Також дане страхування активно застосовується в аудиторській та юридичній діяльності, бухгалтерських послугах, діяльності у сфері будівництва, дизайну чи архітектури, управління нерухомістю, а також інші сфери.

Дуже популярним видом діяльності також є робота коректорів та редакторів. Тому, якщо такий клієнт зазнає фінансових втрат, за

які замовних визнається відповідальним, страхування професійної відповідальності захистить і такий бізнес від будь-якої належної компенсації. Відповідно до умов полісу, судові витрати, понесені на захист позову, покриваються.

Щодо фахівців з маркетингу та комунікацій – від рекламних агентів і маркетингових консультантів до консультантів зі зв'язків з громадськістю та цифрових консультантів, вони також несуть відповідальність за надання спеціальних консультацій і послуг, які відповідають очікуванням їхніх клієнтів, підтримуючи при цьому їхню репутацію. Для вирішення цих питань теж може слугувати страхування.

Ще одна цікава сфера застосування пов'язана з кіберзлочинністю, яка зараз стала більш поширеною та витонченою, ніж будь-коли. Страхування кібервідповідальності може допомогти захистити від ризику атаки такий бізнес.

Територія покриття за даних договором може бути як лише територія України чи Європи, а також будь-яка країна світу.

Щодо переліку збитків, які можуть відшкодуватися по договору страхування професійної відповідальності, то до основних можна віднести:

- заподіяння контрагентам (клієнтам, замовникам, кредиторам та іншим особам) фінансової шкоди;
- відшкодування по позовам про нерозголошення комерційної інформації;
- компенсація по понесеним витратам та упущена вигода;
- компенсація витрат по відновленню документів та баз комп'ютерних даних;
- інші.

Таким чином, ми бачимо, що страхування професійної відповідальності ІТ компаній захищає надавача послуг від претензій клієнтів за недбалість або помилки, які можуть бути допущені у роботі. Такі компанії дозволяють зробити страховий поліс, за бажанням клієнта, вибравши необхідні покриття та рівні.

ЛІТЕРАТУРА:

1. Специфіка страхування IT-розробників в Україні. URL: <https://brit-mark.com/ua/articles/spetsifika-strahovaniya-kompaniy-it-razrabotchnikov-v-ukraine>
2. Insurance for media and technology professionals. URL: <https://www.marshcommercial.co.uk/for-business/professional-indemnity-insurance/media-and-technology-professionals.html>

Василевська Надія Станіславівна,

докторка філософських наук, доцентка, доцентка кафедри цивільно-приватних дисциплін Одеського Національного університету ім. І. Мечникова

ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В СИСТЕМІ ОХОРОНИ ЗДОРОВ'Я

Сучасні інформаційні технології зазнають стрімкого розвитку, змінюючи та модернізуючи різні сфери суспільного життя, освіти, науки. Водночас, залежно від особливостей правового регулювання окремих суспільних відносин, застосування різних інформаційних технологій може створювати ризики порушення основних прав та свобод людини та формувати нові виклики щодо захисту персональних даних. Зазначеного впливу зазнає і сфера охорони здоров'я, в якій основними напрямками використання інформаційних технологій є процеси інформатизації, організації надання медичних послуг, використання штучного інтелекту при наданні медичної допомоги, захист персональних даних в діяльності закладів охорони здоров'я.

Термін «інформаційні технології в сфері охорони здоров'я» (ІТ в охороні здоров'я) в першу чергу характеризує використання електронних систем для зберігання та аналізу медичної інформації, комунікації та обміну даними. Закон України «Основи законодавства України про охорону здоров'я» від 19.11.1992 р. № 2801-XII зазначає: «Електронна система охорони здоров'я (е-здоров'я, eHealth), ЕСОЗ) – система взаємоприйнятних інформаційних відносин усіх суб'єктів сфери охорони здоров'я, які базуються на використанні методів, заходів та технологій із застосуванням цифрового сере-

довища, у тому числі інформаційно-комунікаційних технологій, спрямованих на підтримку сфери охорони здоров'я, включаючи медичні послуги, профілактичний нагляд за здоров'ям населення та його зміцненням, покращення якості та збільшення тривалості життя населення, медичну літературу та освіту у сфері охорони здоров'я, знання та дослідження, використання цифрових сервісів з метою отримання необхідної інформації, знань і навичок для надання медичної та/або реабілітаційної допомоги, виконання оперативних функцій системи громадського здоров'я» [1]. Ця система складається з центральної бази даних та електронних медичних інформаційних систем (МІС), між якими відбувається автоматичний обмін медичними даними про пацієнта та документами через відкритий програмний інтерфейс. Функціонування МІС дозволяє створювати електронні медичні картки, які містять всю інформацію про пацієнта, та відстежувати, обробляти і оперативно обмінюватись даними з колегами, залученими до наступних етапів надання медичної допомоги. На практиці відсутність взаємодії між МІС різних розробників, не коректна робота електронної бази та несвоєчасне занесення медичної інформації становлять нагальну проблему в функціонуванні ЕСОС.

Активне використання інформаційних технологій змінює організаційні процеси надання медичних послуг в сфері охорони здоров'я. В «Порядку організації медичної допомоги на первинному, вторинному (спеціалізованому), третинному (високоспеціалізованому) рівнях із застосуванням телемедицини» затвердженому Наказом МОЗ України від 19.10.2015 р. № 681, надається визначення категорій «телемедичне консультування – надання медичної допомоги пацієнту лікарем із застосуванням телемедицини; телемедицина – комплекс дій, технологій та заходів, що застосовуються при наданні медичної допомоги, з використанням засобів дистанційного зв'язку у вигляді обміну електронними повідомленнями» [2]. Для реалізації телемедичного консультування заклад охорони здоров'я повинен створити відповідний кабінет з необхідним матеріально-технічним оснащенням та забезпечити кваліфікацію медичних

працівників для його обслуговування. Зазначимо, що МОЗ України вказує на «Порядок надання медичної допомоги із застосуванням телемедицини, реабілітаційної допомоги із застосуванням теле-реабілітації на період дії воєнного стану в Україні або окремих її місцевостях», затверджений Наказом МОЗ України від 17.09.2022 р. № 1695 [3]. Правомірність надання медичної допомоги, призначення лікування, постановка діагнозу за допомогою стільникового зв'язку та різного виду месенджерів не визначена.

Використання інформаційних технологій та функціонування електронної системи охорони здоров'я впливає на питання захисту медичної інформації про пацієнта, як частини його персональних даних. Уповноважений Верховної Ради України з прав людини, пояснюючи «Порядок повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних» від 08.01.2014 р., зазначає «стан здоров'я особи – медична інформація про особу, що містить свідчення не лише про стан здоров'я, а й про історію її хвороби, про запропоновані дослідження й лікувальні заходи, прогноз можливого розвитку захворювання, у тому числі про наявність ризику для життя і здоров'я (виняток становлять медичні довідки, листи працездатності і т.д., які обробляються володільцем при реалізації трудових відносин)» [4]. «Впровадження електронної системи охорони здоров'я (далі ЕСОЗ), перенесення медичної інформації про пацієнта в електронний вигляд, збільшення кола медичних працівників, які мають доступ до такої інформації, проблеми технічного характеру та потреба в фахівцях впливає на систему захисту персональних даних в системі охорони здоров'я. Особливої уваги потребує розробка належного рівня технічного забезпечення, коректної роботи медичних інформаційних систем та знання основних принципів обробки, зберігання та захисту персональних даних» [5].

З'являються нові способи використання інформаційних технологій не лише для організації процесів збереження та обміну даними в сфері охорони здоров'я, видозмінюються способи надання

медичної допомоги, наприклад з використанням технологій штучного інтелекту. Вже сьогодні за допомогою ШІ проводять діагностичні процедури, аналізують дані МРТ, обробляють інформацію про стан здоров'я пацієнта. Безперечно, залученість ШІ в діяльність медичних працівників буде зростати і потребувати правового регулювання.

Розвиток та впровадження інформаційних технологій в системі охорони здоров'я необхідно проводити за принципами правової захищеності учасників медичних правовідносин. Основні з них: отримання достовірної, своєчасної і повної інформації про стан свого здоров'я, збереження таємниці про стан здоров'я, інформована згода на медичне втручання, застосування методів діагностики, профілактики, лікування; використання доступних засобів телемедицини тощо. Правове регулювання інформаційних технологій в сфері охорони здоров'я дозволить зробити медичну допомогу якісною, ефективною, результативною, доступною, прийнятною, орієнтованою на пацієнта, справедливою та безпечною, своєчасною та інтегрованою. Екологічна та якісна охорона здоров'я є важливою для досягнення Цілей сталого розвитку 3 (ЦСР3): «Забезпечення здорового життя та сприяння добробуту для всіх у будь-якому віці», де завдання 3.8 наголошує на важливості високоякісних базових медичних послуг [6]. Тільки система охорони здоров'я, що базується на інтегрованих та орієнтованих на людину медичних послугах з залученням сучасних інформаційних технологій, може досягти мети універсального охоплення послугами охорони здоров'я.

ЛІТЕРАТУРА:

1. Основи законодавства України про охорону здоров'я: Закон України від 19.11.1992 р. № 2801-XII URL: <https://zakon.rada.gov.ua/laws/show/2801-12#Text>
2. Порядок організації медичної допомоги на первинному, вторинному (спеціалізованому), третинному (високоспеціалізованому) рівнях із застосуванням телемедицини: Наказ МОЗ України від 19.10.2015 р. № 681 URL: <https://zakon.rada.gov.ua/laws/show/z1400-15#Text>
3. Порядок надання медичної допомоги із застосуванням телемедицини, реабілітаційної допомоги із застосуванням телереабілітації на період дії воєнного стану в Україні або окремих її місцевостях: Наказ

МОЗ України від 17.09.2022 р. № 1695 URL: <https://zakon.rada.gov.ua/laws/show/z1155-22#Text>

4. Про затвердження документів у сфері захисту персональних даних: Наказ від 08.01.2014 р. № 1/02-14 Уповноважений Верховної ради України з прав людини. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text

5. Василевська Н. С. «Основні засади захисту персональних даних в діяльності закладів охорони здоров'я» // Наукові перспективи. Серія «Право» № 2(56). 2025 р. URL: <http://perspectives.pp.ua/index.php/np/article/view/20791/20767>

6. 17 цілей сталого розвитку URL: <https://globalcompact.org.ua/tsili-stijkogo-rozvytku/>

Галунова Лариса Ігорівна,

*кандидатка юридичних наук, доцентка,
доцентка кафедри інтелектуальної власності та патентної юстиції
Національного університету «Одеська юридична академія»*

КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ПРАВОВОЇ ОХОРОНИ РЕЗУЛЬТАТІВ ТВОРЧОЇ ДІЯЛЬНОСТІ, СТВОРЕНИХ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ

Актуальність дослідження правової охорони творчих результатів, створених за допомогою штучного інтелекту, обумовлена стрімким розвитком цифрових технологій і зростаючим впливом штучного інтелекту на різні сфери людської діяльності. Сучасні алгоритми здатні генерувати тексти, музику, живопис, архітектурні проекти та багато іншого, що ставить перед правовою наукою питання про належність прав на такі об'єкти.

Сьогодні в світі існує кілька основних підходів до правової охорони творів, створених штучним інтелектом:

Традиційний підхід (автор – виключно людина) – згідно з цим підходом, авторське право може належати лише фізичній особі, яка здійснила творчий внесок у створення твору. Якщо ШІ діяв автономно, такий твір не підлягає охороні авторським правом. Цей підхід закріплений у законодавстві США та багатьох інших країн [1].

Підхід «ШІ як інструмент» – твір, створений із використанням штучного інтелекту, охороняється так само, як і твори, створе-

ні за допомогою інших технологічних засобів. Автором визнається людина (розробник, користувач або замовник), яка контролювала творчий процес і визначила кінцевий результат. Цей підхід застосовується в Європейському Союзі [2].

Право sui generis (спеціальний правовий режим) – пропонується створити окрему категорію правового захисту для творів, створених ШІ, яка не є класичним авторським правом, але надає обмежені права на використання таких творів.

Визнання ШІ автором – радикальний підхід, за яким штучний інтелект може бути самостійним суб'єктом права та володіти авторськими правами на створені ним твори. Це дискусійний підхід, який поки що не підтриманий жодною державою, але активно обговорюється в наукових колах.

Договірний підхід – у разі відсутності законодавчого врегулювання сторони (розробники, користувачі) можуть укладати угоди, що визначають права на використання творів, створених штучним інтелектом. Такий підхід уже застосовується в бізнес-середовищі.

Кожен із цих підходів має свої переваги та недоліки, і їх застосування залежить від рівня розвитку правової системи конкретної країни та ступеня автономності штучного інтелекту у творчому процесі.

Законодавство України, зокрема Закон України «Про авторське право та суміжні права», визначає автора як фізичну особу, яка своєю творчою працею створила твір. Це означає, що для визнання авторських прав необхідна безпосередня участь людини у процесі створення твору. Відповідно, об'єкти, створені виключно штучним інтелектом без суттєвого втручання людини, не підпадають під традиційний режим авторського права [3]. У новій редакції Закону України «Про авторське право та суміжні права» введено поняття права особливого роду (*sui generis*) для неоригінальних об'єктів, згенерованих комп'ютерною програмою. Це стосується результатів, створених штучним інтелектом без творчого внеску людини. Суб'єктами такого права можуть бути особи, які мають майнові права щодо відповідної комп'ютерної програми, наприклад, автори

програми штучного інтелекту або її правомірні користувачі. Строк чинності права *sui generis* становить 25 років з моменту генерації об'єкта [1]. Таким чином, українське законодавство робить кроки щодо адаптації правових норм до сучасних технологічних реалій, зокрема через введення права *sui generis*. Однак, для ефективного регулювання необхідне подальше вдосконалення законодавства та міжнародна гармонізація підходів до правової охорони результатів діяльності штучного інтелекту.

Разом із законодавчими змінами постає питання про сутність творчості у контексті людської та машинної діяльності. Людська творчість традиційно асоціюється з глибинними процесами самовираження, інтуїцією, здатністю до оригінальних рішень, які часто виходять за межі логічного мислення. Це не просто генерація нових ідей, а складний процес, що включає емоції, культурні традиції, моральні та етичні складові.

На відміну від цього, машинна творчість ґрунтується на алгоритмах і базах даних, що дозволяє штучному інтелекту генерувати нові твори, але без залучення таких суб'єктивних чинників, як емоційний досвід або моральні переконання. Хоча штучний інтелект здатний створювати вражаючі результати, вони є наслідком аналізу та обробки великих масивів даних, відтворення та комбінування існуючих патернів, а не самостійного самовираження. Тому головним викликом залишається визначення меж між машинною і людською творчістю та встановлення справедливих правових механізмів регулювання цих процесів. Власники технології або користувачі системи штучного інтелекту часто стикаються з юридичними труднощами, що стосуються визнання авторських прав на твори, створені автоматизованими машинами.

З технічної точки зору, штучний інтелект здатний значно пришвидшити процеси генерації нових ідей та творів, а також здійснювати їх модифікацію або покращення. Проте це піднімає питання: чи можуть такі твори бути оригінальними, якщо вони створюються на основі алгоритмів, розроблених людиною, і в якому сенсі вони можуть бути визнані результатом творчої діяльно-

сті? Можливо, таке покоління творів здатне змінити уявлення про творчість як таку, але чи зможе воно колись зрівнятися з людською здатністю до інновацій і самовираження?

Між тим, машинна творчість відкриває нові горизонти для креативних індустрій, зокрема в музиці, дизайні та кінематографії, дозволяючи створювати нові форми мистецтва, які були б неможливими без допомоги технологій. Разом з тим, необхідно усвідомлювати, що навіть у випадку розвитку високотехнологічних алгоритмів, людська творчість, яка ґрунтується на культурному контексті, емоціях та інтуїції, залишається унікальною та неповторною. Потрібно також зазначити, що творча діяльність людини передбачає не лише створення нових ідей, але й їх емоційне сприйняття та суспільну значущість, що є важливою складовою творчості [4].

Питання авторства в контексті участі штучного інтелекту є складним і багатоаспектним, оскільки традиційні підходи до авторства, закріплені в правових системах, ґрунтуються на уявленні про фізичну особу як автора твору. Однак з розвитком штучного інтелекту виникає необхідність перегляду цих підходів, оскільки штучний інтелекту здатен створювати нові твори без безпосередньої участі людини, що ставить під сумнів традиційні принципи авторства.

Оскільки багато правових систем у світі поки що не передбачають можливості надання авторських прав створенням, здійсненим виключно ШІ, виникає необхідність у створенні нових правових норм. У деяких країнах вже розглядається питання про адаптацію законодавства до реалій цифрової епохи.

Різні країни та міжнародні організації вже працюють над адаптацією авторського права до нових умов. Європейський Союз, наприклад, обговорює можливість включення в законодавство нових категорій прав, які б регулювали авторство творів, створених за допомогою штучного інтелекту, а також питання щодо розмежування прав на такі твори.

Підходи до визначення авторства при участі штучного інтелекту постійно змінюються, адже розвиток технологій та їх вплив на творчу діяльність потребує нових правових рішень. Визначення авторства в такому контексті може включати як традиційний підхід до людини як автора, так і нові моделі, в яких обговорюється роль технології в створенні творчих результатів.

Розвиток штучного інтелекту у творчій сфері ставить під сумнів традиційні концепції авторського права, оскільки чинне законодавство більшості країн визнає авторами лише фізичних осіб, залишаючи твори, створені штучним інтелектом, без належного правового захисту. Водночас міжнародна практика демонструє тенденцію до адаптації правових норм, зокрема шляхом надання прав розробникам або користувачам штучного інтелекту [5]. Вирішення цієї проблеми може відбуватися через запровадження спеціального правового режиму для таких творів або розробку нових концепцій інтелектуальної власності. Враховуючи виклики правозастосування, необхідне міжнародне узгодження підходів, що дозволить захистити права розробників і користувачів штучного інтелекту, забезпечуючи баланс між інноваціями та охороною прав інтелектуальної власності.

ЛІТЕРАТУРА:

1. Спесивцева О. Право *sui generis*: як штучний інтелект адаптує під себе авторське право? URL: <https://cedem.org.ua/analytics/shtuchnyi-intelekt-pravo/>
2. Юшина А. Штучний інтелект: кому належать авторські й майнові права. URL: <https://mind.ua/openmind/20255019-shtuchnij-intelekt-komu-nalezhat-avtorski-j-majnovi-prava>
3. Харебова Т. Авторські права на об'єкт, створений штучним інтелектом. URL: https://jurliga.ligazakon.net/analytics/225383_avtorsk-prava-na-obkt-stvoreniy-shtuchnim-ntelektom
4. Шумилович Б. Творчість людей і творчість машин. URL: https://zaxid.net/tvorchist_lyudey_i_tvorchist_mashin_n1522567
5. Адаптація законодавства ЄС у сфері штучного інтелекту до виборчих процесів: шлях для України. URL: <https://www.ifesukraine.org/wp-content/uploads/2025/01/ifes-ukraine-artificial-intelligence-ukr.pdf>

Калітенко Оксана Михайлівна,
*кандидатка юридичних наук, доцентка, професорка кафедри цивільного
права Національного університету «Одеська юридична академія»*

ІНФОРМАЦІЙНЕ СЕРЕДОВИЩЕ, ЯК СТРАТЕГІЧНИЙ РЕСУРС У ГІБРИДНИХ КОНФЛІКТАХ

Сучасні міжнародні конфлікти людства дедалі частіше набувають гібридного характеру, у межах якого інформаційне середовище стає не лише каналом комунікації, але й потужним інструментом впливу, знищення авторитету інституцій, маніпулювання масовою свідомістю, підризу легітимності державної влади. У цьому контексті наукове осмислення правових, політичних і технологічних аспектів функціонування інформаційного середовища як одного з головних інструментів гібридної війни набуває особливої актуальності для формування ефективних заходів правового реагування.

Інформаційне середовище останнім часом трансформувалося у визначальний фактор гібридної війни. Воно охоплює цифрові канали комунікації, соціальні мережі, штучний інтелект, алгоритми поширення контенту та віртуальні платформи. У рамках гібридної агресії інформаційне середовище виступає не лише як інструмент поширення пропаганди, але й як спосіб здійснення психологічного тиску, провокування панічних настроїв, делегітимації державної влади та створення ілюзії політичної кризи. Інформаційна агресія охоплює елементи кібертероризму, інформаційних атак, дезінформації та маніпулювання громадською думкою.

Гібридна війна – це поєднання традиційних військових дій із невійськовими засобами: політичним тиском, економічними санкціями, інформаційними та психологічними операціями. Основною метою є досягнення політичних і стратегічних результатів без оголошення повномасштабної війни. Інформаційна складова передбачає використання фейкових новин, інформаційних вкидів, атак на медіаінститути, поширення панічного або роз'єднувального контенту. Згідно з дослідженнями НАТО, у сучасних конфліктах понад 70% успіху залежить від ефективності інформаційної кампанії (NATO Strategic Communications Centre of Excellence, 2021).

Україна з 2014 року перебуває під системним впливом інформаційної агресії з боку РФ. Російські інформаційні кампанії мають на меті підрив довіри до української державності, армії, міжнародних союзників, а також маніпулювання історичною пам'яттю, етнічною ідентичністю, мовними й релігійними маркерами. Інструментами агресії виступають бот-мережі, автоматизовані платформи поширення контенту, кіберфлуди, фейкові експертні коментарі. Міністерство цифрової трансформації України у 2022–2023 роках зафіксувало понад 4 тис. випадків цілеспрямованих інформаційних атак на державні інституції та стратегічні об'єкти інфраструктури.

Сучасна міжнародна правова система наразі не містить ефективного механізму боротьби з інформаційною агресією. Наявні правові інструменти кіберзахисту, інформаційного суверенітету та відповідальності за поширення фейків є розпорошеними, а механізми юрисдикційного переслідування – складними і не гарантованими у реалізації. Водночас в Україні триває активний процес нормативного забезпечення інформаційної безпеки, зокрема ухвалено Закон України «Про національну безпеку України» (2018), «Про основи національного спротиву» (2021), а також розробляється Концепція інформаційної стійкості. Потребує вдосконалення судова практика в частині боротьби з фейками, мови ворожнечі, деструктивного контенту, що порушує національну безпеку країни.

Глобальне посилення сучасної інформаційної безпеки має здійснюватися на основі міждисциплінарного, комплексного підходу: поєднання правових, технологічних, освітніх, філософських та культурологічних стратегій. Як свідчить практика, необхідно розширювати правову експертизу щодо категорій «інформаційна атака», «цифрова суверенність», «штучна дезінформація», а також удосконалювати систему державного реагування на правопорушення в медіапросторі. Медіаосвіта, формування критичного мислення, фактчекінг, розробка національних цифрових платформ з прозорими алгоритмами – є фундаментальними інструментами формування інформаційної стійкості нації. Додатково, застосування технологій ШІ для ідентифікації фейків, бот-активності, коорди-

нованих дезінформаційних кампаній може стати елементом національної інформаційної політики.

Правова протидія інформаційним атакам в умовах гібридної війни потребує комплексного підходу, що має поєднувати як національні законодавчі ініціативи, так і участь у міжнародному правотворенні. Одним із першочергових напрямів є запровадження спеціального законодавства, яке б комплексно регулювало питання інформаційної безпеки та протидії дезінформації. Йдеться, зокрема, про нормативне закріплення таких категорій, як «інформаційна атака», «координована інформаційна операція», «деструктивний контент» тощо. Таке законодавство має визначити чіткі підстави правової відповідальності для організацій та осіб, що беруть участь в інформаційній агресії, зокрема в межах цифрових платформ і соціальних мереж. Аналогічні механізми уже успішно застосовуються у правових системах країн ЄС, наприклад у Франції (закон 2018 року про протидію інформаційним маніпуляціям) та Німеччині (NetzDG).

Наступним кроком має стати розширення кримінально-правових заходів реагування на інформаційні загрози. Йдеться про кодифікацію окремих складів злочинів, таких як умисне поширення фейкових повідомлень у період воєнного стану, публічне виправдання колабораціонізму через цифрові платформи, участь в інформаційних диверсійних структурах. Особливої актуальності набуває кваліфікуюча ознака участі в діяльності організованих груп або в координації з державою-агресором. В умовах війни такі дії мають прирівнюватися до інформаційного тероризму й розглядатися як загроза національній безпеці.

Окрему увагу слід приділити врегулюванню діяльності цифрових платформ у межах національної юрисдикції. Це передбачає запровадження правових механізмів державної взаємодії з глобальними соціальними мережами та пошуковими системами. Йдеться про обов'язок реагувати на запити держави щодо блокування інформаційного контенту, що має ознаки дезінформації, пропаганди чи мови ворожнечі, а також про вимогу прозорості алгоритмів ранжування новин. Подібні підходи уже запроваджено в Європей-

ському Союзу у межах Digital Services Act (2022), який встановлює правила відповідальності для цифрових посередників.

Важливим інструментом протидії є також розвиток національної інфраструктури стратегічних комунікацій. Йдеться не лише про оперативне спростування фейків, але й про формування стійкої інформаційної парадигми, орієнтованої на демократичні цінності, прозорість державного управління та збереження національної ідентичності. Центри стратегічних комунікацій, які об'єднують ресурси держави, медіа, академічної спільноти та громадських організацій, мають діяти на постійній основі та в координації з міжнародними партнерами. Яскравим прикладом є Центр стратегічних комунікацій та інформаційної безпеки, створений в Україні у 2021 році.

Останнім, проте ключовим, напрямом є удосконалення міжнародного правового регулювання у сфері протидії інформаційній агресії. Необхідно ініціювати створення спеціального міжнародного правового інструменту – наприклад, конвенції про цифровий суверенітет або про відповідальність за інформаційні атаки як форму агресії. Також варто визначити чіткі критерії, за яких інформаційні дії держави можуть розглядатися як порушення міжнародного гуманітарного права або Статуту ООН. З огляду на глобальну природу інформаційних загроз, лише консолідована правова позиція всіх держав світу може забезпечити ефективний захист у гібридному вимірі сучасної війни.

Кривенко Юлія Василівна,

*кандидатка юридичних наук, доцентка, доцентка кафедри цивільного права
Національного університету «Одеська юридична академія»*

ДО ПИТАННЯ СПАДКУВАННЯ ЦИФРОВОЇ РЕЧІ

Питання, що виникають у процесі спадкування майна, займають одне із ключових місць у цивільному праві. Сучасна людина накопичує безліч цифрових об'єктів впродовж життя – від електронної пошти та облікових записів у соціальних мережах до файлів, фотографій та інших даних, що зберігаються в хмарних сервісах. Після смерті власника виникає потреба передачі цих об'єктів його

спадкоємцям. Передати у спадок можна будь-яке майно: гроші, цінні папери, коштовності, машини, нерухомість та інші об'єкти. Найчастіше у судовій практиці виникають складнощі при передачі спадкоємцям специфічних об'єктів цивільних прав, наприклад, цифрових речей, таких як цифрові валюти та криптовалюти, акаунти в соціальних мережах та доменні імена.

Враховуючи динамічний розвиток нових інститутів цивільно-правової науки, актуальними є питання спадкування цифрових речей.

Проте, на відміну від матеріальних об'єктів, цифрові об'єкти не мають чітко визначеного правового статусу. Відсутність належного законодавчого регулювання створює правову невизначеність та ускладнює процес спадкування:

- Неясно, хто саме (спадкоємці, представники, оператори) має право доступу та розпорядження цифровими об'єктами після смерті власника.

- Виникають складнощі з ідентифікацією всіх цифрових об'єктів, що належали спадкодавцю, оскільки вони можуть бути розподілені різними онлайн-сервісами.

- Інтернет-компанії та провайдери послуг часто відмовляються надавати доступ до облікових записів померлого через побоювання порушення конфіденційності.

Слід зазначити, що спадкове право зазвичай є однією з найбільш консервативних сфер правового регулювання. Вплив цифрових технологій на спадкове право поки що мінімальний, хоча абсолютно залишатися осторонь процесів, що відбуваються в усьому світі, неможливо. Ситуація зараз дещо спрощується малою кількістю кейсів. Однак коли такі виникають (наприклад, знаменита суперечка з приводу доступу спадкоємців до облікового запису померлого в FB), починаються суперечки. Водночас нерідко такі дискусії стосуються лише конкретного випадку. Системного концептуального розуміння «цифрових» об'єктів спадкового правонаступництва зараз відсутня.

Розвиток технологій, що прискорився під час пандемії коронавірусу, призвів до появи таких об'єктів, про які класична циві-

лістика не могла й підозрювати. Вочевидь, цивільне право будується виходячи з принципу свободи договору і, в принципі, суб'єкти можуть охоплювати будь-які об'єкти, крім тих, обіг яких прямо заборонений, чи здійснювати подібні правочини з урахуванням законодавчо встановлених обмежень. Проте технічна сторона питання стала настільки визначальною, що юристам не завжди вдається зрозуміти особливості відносин, що виникають.

Відповідно до ст. 179 ЦК України «Цифровою річчю є благо, що створюється та існує виключно у цифровому середовищі та має майнову цінність» [1].

Норми статті 179 ЦК України містять вказівку на належність цифрової речі до об'єктів цивільних прав, що належать до іншого майна, зокрема, до майнових прав.

Виходячи із змін до Цивільного кодексу, всі цифрові речі, як об'єкти цивільних прав, поділяються на: віртуальні активи; цифровий контент; інші блага, в розумінні заданого визначення. [2]

Узагальнюючи теоретичні дослідження сучасних вчених, цифрові об'єкти права слід розглядати як: по-перше, як самостійний об'єкт права -»новий» об'єкт, що входить у поняття «інше майно» або як вид вже існуючих певних об'єктів, але з особливим способом його фіксації у фізичній реальності, за допомогою спеціальних технічних пристроїв. [3]

Економічний оборот йде суттєво попереду законодавства. Так, розвиненим став обіг акаунтів у соціальних мережах та комп'ютерних іграх. Будь-який бажаючий може придбати, скажімо, обліковий запис гри «World of Tanks», причому вибір широкий як за ціною, так і за якістю («рівнем прокачування»). Інше питання, чи підпадають такі відносини під дію права та як саме право має їх регулювати.

Наприклад, деякі соціальні мережі включають до правочину з користувачем пункт, який визначає порядок переходу облікового запису після його смерті. Технічно такий підхід видається обґрунтованим. Більше того, вчені пропонують на підставі механізму криптографії створити систему он-лайн заповіту, засновану на технології блокчейну та смарт-контрактів.

Цифровий актив має входити у спадкову масу, оскільки він відповідає основним необхідним характеристикам об'єкта спадкових правовідносин (насамперед щодо нього виникають економічні відносини). Однак, визнавши це, ми приходимо до неможливості реалізувати основні засади та правила спадкового права. Тут і про процедурні моменти, і про захист прав учасників відносин.

Згадаймо про смарт-контракт і подумаємо, що буде з правами та обов'язками після смерті громадян, які вирішили використати такий технічний засіб. Дослідники пишуть, що «може бути вирішена проблема уявної неможливості поступки права (вимоги) за початковим смарт-контрактом» [4]

Виходить, що правонаступництво у спадок можливе в цій ситуації. Однак не зовсім зрозуміло, як, у якому порядку і до кого слід звертатися за реалізацією таких прав. Припустимо, виконання відбулося автоматично (передана криптовалюта), але спадкоємець не може її отримати через відсутність ключа.

Отже, питання спадкування цифрових речей стає дедалі актуальним у багатьох країнах світу у зв'язку зі зростанням значущості цифрових речей у суспільстві. При цьому правове регулювання цієї галузі поки що недостатньо врегульоване, що створює низку проблем для спадкоємців.

ЛІТЕРАТУРА:

1. Цивільний кодекс України. *Відомості Верховної Ради України*. 2003. №№ 40–44, ст. 356
2. Цифрові речі та цифровий контент: новації законодавства, договорні відносини. URL: https://biz.ligazakon.net/analytics/223070_tsifrov-rech-ta-tsifroviy-kontent-novats-zakonodavstva-dogovrn-vdnosin
3. Некіт К.Г. Віртуальні активи як різновид цифрових речей. *Часопис цивілістики*. 2022. Вип. 45. С. 53–57.; Сліпченко А.С., Сліпченко О.С. Визначення юридично значущої сутності цифрової речі в цивільному праві України. *Форум Права*. 2024. № 1. 88–96.; Харитонов Є.О. Вітчизняна концепція права власності перед викликами інформаційного суспільства. *Часопис цивілістики*. 2018. Вип. 29. С. 82–88.
4. Яроцький В.Л.; Філонова Ю.М. Зустрічне виконання зобов'язань у смарт-контрактах за цивільним законодавством України. *Академічні візії*. 2024. 31.

Маковій Віктор Петрович,

кандидат юридичних наук, професор, зав. кафедри цивільно-правових дисциплін інституту права та безпеки Одеського державного університету внутрішніх справ

ПРАВОВИЙ СТАТУС СТАРТАПУ ЯК СУБ'ЄКТА ІТ-ВІДНОСИН

Дослідження світового рейтингу стартапів свідчить, що в числі перших позицій знаходяться проекти, пов'язані з обробкою інформації різного роду, за допомогою нейромережових інструментів та інших розробок в сфері інформаційних технологій, які поєднують засоби моделювання та інші методи опрацювання даних різноманітної природи. Відповідним чином, в українському варіанті такого рейтингу в межах першої десятки продуктів представлені інноваційні інформаційно-технологічні проекти, які прямо або опосередковано пов'язані з використанням штучного інтелекту та (або) програмного продукту в якості засобів до вирішення задач різноспектрового характеру суспільного буття [1]. Тобто зміст стартапів безпосередньо пов'язаний з ІТ сферою, що потребує з'ясування їх природи та встановлення місця в межах даного роду правовідносин.

До природи стартапу як соціальної категорії є декілька підходів, переважна сутність яких безпосередньо відтворена у економічній площині. Зокрема, пропонується сприймати стартап в якості форми організації підприємницької діяльності, яка віднаходить розвиток у певній ідеї, плані її просування на ринку, стратегії розвитку компанії та поєднує при цьому оптимальне (обмежене) використання ресурсів [2, с. 104–105]. Першопочатківець серед дослідників та впровадження моделей стартапу Стив Бланк у своїй роботі детермінує стартап в якості тимчасової організації, яка використовується для пошуку повторюваної та масштабованої бізнес-моделі [3, с. 18]. В межах Web-ресурсу StartupRanking стартап визначений як організація з високою інноваційною компетенцією й сильною технологічною базою, яка наділена здатністю до прискореного зростання в економічному вимірі й зберігає незалежність у часі з максимальним строком реалізації до 10 років [4].

Згідно Положення щодо конкурсного відбору проектів для державного стимулювання створення і використання винаходів (корисних моделей) та промислових зразків, затвердженого наказом Міністерства економічного розвитку і торгівлі України від 12 грудня 2018 року № 1879, стартап визначений як проект, пов'язаний зі створенням та/або використанням винаходів, корисних моделей, промислових зразків, ноу-хау та інших результатів інтелектуальної, творчої діяльності. Системно-структурний аналіз нормативних приписів зазначеного положення свідчить про сприйняття стартапу саме як різновиду проекту, який по суті є формою інноваційної діяльності, яка може бути реалізована зі створенням для цієї мети певного господарюючого суб'єкта, в межах вже існуючого господарюючого суб'єкта або ж шляхом укладення та реалізації змісту договору про спільну діяльність з відповідною інвестиційною метою.

За іншим підходом стартап сприймається як елемент національної інноваційної системи, що вирізняється відповідною правосуб'єктністю в межах зазначеного виду діяльності. При цьому стартап, як суб'єкт господарської діяльності відповідного виду, цілком ототожнюється з правосуб'єктністю фізичної особи-підприємця, приватного підприємства, товариства з обмеженою відповідальністю або, навіть, структурним підрозділом певного господарюючого суб'єкта [5, с. 66–74]. Така позиція цілком узгоджується з дефініцією інноваційної діяльності як такої, що спрямована на використання і комерціалізацію результатів наукових досліджень та розробок і зумовлює випуск на ринок нових конкурентоздатних товарів і послуг, яка міститься у ст. 1. Закону України «Про інноваційну діяльність». Наведене визначення інноваційної діяльності вигідно вирізняється, під кутом висловленого, від змісту ст. 325 Господарського кодексу України, яка мову веде про довгострокові науково-технічні програми та науково-технічні досягнення у змісті подібної діяльності. Більше того, викладені риси стартапу як інноваційного продукту також корелюють зі змістом ст. 16 останнього нормативно-правового акту, де інноваційним підприємством визнається підприємство (об'єднання підприємств) за умови, що питома вага

(більше ніж 70 відсотків) його продукції в грошовому еквіваленті є саме інноваційні продукти і (або) інноваційна продукція.

Оскільки інноваційний продукт у всіх його варіаціях згідно ст. 14 розглянутого закону є реалізацією (впровадженням) об'єкта інтелектуальної власності (винаходу, корисної моделі, промислового зразка, топографії інтегральної мікросхеми, селекційного досягнення тощо), забезпечує підвищення науково-технічного і технологічного рівня, наділений новизною вищими техніко-економічними показниками, то його створення в питомій вазі в період існування інформаційного суспільства покликане відтворити відповідні здобутки саме в IT-сфері, що і пояснюється наведеною вище статистикою виникнення та розвитку стартапів. Подібне цілком слушно має бути відтворене й щодо сутності інноваційної продукції у змісті діяльності стартапів.

З позиції розгляду стартапу в якості форми підприємницької діяльності пропонується детермінація наступних його ознак: 1) висока здатність до адаптації; 2) висока вірогідність досягнення поставлених інноваційних цілей, орієнтованих на потреби ринку; 3) мінімальні витрати ресурсів з боку авторів стартапу; 4) висока швидкість реалізації проекту; 5) максимальна ефективність від реалізації проекту у контексті співвідношення здійснених затрат та отриманих вигід; 6) здатність такого проекту до масштабування шляхом його повторення та розширення; 7) короткий цикл операційної діяльності в межах проекту. При цьому передумовою до реалізації такої форми інвестиційної та підприємницької діяльності пропонується визнавати потребу у ефективному та оперативному впровадженню інноваційного проекту на противагу більш ємкому та тривалішому періоду реалізації його в межах діяльності великих корпорацій [6, с. 27].

Існує позиція, що головною ознакою стартапу серед наведених вище є його інноваційність та новизна, які ототожнюються у сенсі здійснення підприємницької діяльності в певній сфері суспільного буття [7, с. 16]. Вочевидь, з огляду на викладене така думка має бути цілком підтриманою, однак з такими зауваженнями. Інноваційність

як діяльність, що спрямована на використання і комерціалізацію результатів наукових досліджень та розробок і зумовлює випуск на ринок нових конкурентоздатних товарів і послуг, відображає родову рису й решти форм інноваційної діяльності, про що мова йшла вище. Разом з тим, з огляду на класично сформовану структуру стартапу, перш за все, як економічної категорії, варто звернути увагу на відображені саме для цієї форми інноваційної діяльності ознаки, серед яких пріоритетними є оперативний (короткий) виробничий цикл та максимальна ефективність, яка проявляється у двох алгебраїчних показниках: 1) співвідношення витрат до отриманої вигоди (незначні витрати й максимальні вигоди); 2) висока вірогідність досягнення інноваційного результату у порівнянні з іншими формами такої діяльності.

На подовження викладеного пропонується сприймати стартап як недавно створену компанію, яка являє інноваційну форму здійснення підприємницької діяльності, що наділена обмеженими ресурсами й планує реалізувати таку правосуб'єктність на ринку [8, с. 122]. Тобто, серед іншого зосереджується увага на таких розрізняльних рисах як короткий період існування та закладення у зміст установчих документів такого виду інноваційної діяльності, що окреслює гіпотетичний характер наведеної форми інноваційності шляхом детермінації відповідної мети. Вочевидь, необхідно апелювати до такого міркування, оскільки немає потреби звужувати форму та зміст інноваційної діяльності у площині діяльності стартапу. Також визначення гіпотетичних прагнень в межах установчих документів, які стосуються комерціалізації та впровадження науково-технічних досягнень в межах стартапу, може бути доцільним тільки у випадку, коли маємо справу зі спеціальною правосуб'єктністю юридичної особи, яку уособлює розглянутий вид інноваційної діяльності. Водночас, зазначені риси мають бути цілком сприйнятими у змісті та формах, що уособлюють правосуб'єктність юридичної особи, а саме в рішеннях органів управління та договірній практиці такого стартапу як суб'єкта.

Ну, і нарешті, щодо організаційно-правової форми, то варто згадати І.М. Кучеренко, яка на підставі аналізу наявних напра-

цювань організаційно-правовою формою юридичних осіб назвала видову характеристику юридичних осіб, в основі виділення якої лежить визначена приписом законодавства сукупність певних ознак, що створюють підстави вирізняти одну юридичну особу від іншої у зовнішньому прояві. При цьому до істотних ознак, які відмежовують різні організаційно-правові форми, вона відносить наявність чи відсутність об'єкта права власності засновників та вид відповідальності або право учасників на отримання майна після ліквідації юридичної особи й покладення на таких майнових обов'язків. При цьому мета, вид, способи здійснення мети, особливості формування та розпорядження майном юридичної особи, на її думку, ні в якому разі не можуть братись за ознаку виділення тієї чи іншої організаційно-правової форми як такі, що за своєю сутністю не є цивільно-правовими. Вказане узгоджується з думкою, що окремі ознаки юридичних осіб характеризують їх організаційно-правову форму, а окремі – відображають специфіку їх діяльності [9, с. 12–16]. Разом з тим, пропонується виділення три організаційно-правові форми стартапу як різновиду інноваційної діяльності: ФОП, приватне підприємство, товариство з обмеженою відповідальністю (ТОВ). Вочевидь, з урахуванням викладеного, коректніше буде сприймати такі форми саме як види стартапу, а не організаційно-правові форми юридичної особи. Разом з тим, необхідно розширити такий перелік, однак з огляду на природу решти організаційно-правових форм юридичних осіб та особливостей прояву проаналізованих вище ознак стартапу.

Викладене надало можливість, детермінувати стартап в якості однієї з форм інноваційної діяльності, для якої вирізняльними є риси оперативного виробничого циклу та максимальної ефективності (співвідношення витрат до отриманої вигоди, висока вірогідність досягнення інноваційного результату у порівнянні з іншими формами такої діяльності). Стартап як суб'єкт ІТ-правовідносин може бути представлений ФОП або юридичною особою, яка за організаційно-правовою формою у повній мірі відповідає наведеним ознакам.

ЛІТЕРАТУРА:

1. Startup Ranking. 2025. URL: <https://www.startupranking.com/what-is-a-startup>.
2. Оксенюк К.І. Розвиток стартапів в Україні. *Економічні науки: збірник наукових праць Луцького національного технічного університету. Серія «Регіональна економіка»*. Випуск 16 (63). Луцьк: ІВВ Луцького НТУ, 2019. С. 102–107.
3. Blank S., 2013. The startup. Owner's manual, translation from English. Moscow: Alpina Publisher, 485 p.
4. What is a startup? URL: <https://www.startupranking.com>
5. Учасники національної інноваційної системи: інституційно-функціональний аналіз в праві: монографія. За заг. ред. С.В. Глібка, Ю.В. Георгієвського. Харків: Право, 2018. 270 с.
6. Корнух О.В., Маханько Л.В. Стартап як прогресивна форма інноваційного підприємництва. *Інвестиції: практика та досвід*. 2014. № 23. С. 26–30.
7. Зеліско А., Соломка Т. Стартап-компанії в Україні: правове підґрунтя. *Актуальні проблеми вдосконалення чинного законодавства України: збірник наукових статей*. 2021. № 57. С. 13–25.
8. Чазов Є. Стартап як нова форма ведення бізнесу. *Наукові праці Національного університету харчових технологій*. 2013. № 52. С. 122–128.
9. Кучеренко І.М. Організаційно-правові форми юридичних осіб приватного права. Київ: Ін-т держави і права ім. В.М. Корецького НАН України, 2004. 328 с.

Омельчук Олександр Сергійович,

*кандидат юридичних наук, доцент, доцент кафедри цивільного права
Національного університету «Одеська юридична академія»*

ПОТЕНЦІАЛ ТА ПРОБЛЕМИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ НА ДЕЙТИНГ-ПЛАТФОРМАХ

Розвиток інформаційних технологій, значні досягнення сучасної науки й техніки, перетворення інформації у найдорожчий товар зумовили цифровізацію суспільних відносин. Результатом такої цифровізації стала трансформація суспільства, основою якого є глобальна мережа «Інтернет» [1, с. 45].

Перманентний розвиток технологій і засобів комунікації створює нові можливості самовираження в мережі Інтернет. Поряд з цим така тенденція зумовлює необхідність регулювання, щоб

забезпечити етичне використання та відповідальність учасників таких правовідносин. Правове регулювання в контексті нових технологій стає складним завданням, оскільки потрібно забезпечити баланс між свободою вираження думок, захистом прав споживачів та обмеженням шкідливого та незаконного вмісту [5, с. 160].

На сьогоднішній день явище знайомств та побудови відносин в мережі Інтернет вже не є чимось надзвичайним. Широкий попит на дані послуги зумовив зростання ринку онлайн-дейтингу. Сьогодні сервіси для онлайн-знайомств – одна з найпопулярніших категорій мобільних програм.

Під онлайн-дейтингом зазвичай розуміється діяльність спеціалізованих цифрових платформ, які використовуються користувачами для знайомств в мережі Інтернет. Основною метою користувачів дейтинг-платформ є пошук людини на основі своїх уподобань, для чого означені сервіси використовують різні механіки пошуку за певними критеріями.

Вже зараз з метою забезпечення ефективності надання комунікативних послуг дейтинг-сервіси застосовують сучасні технології, в тому числі ШІ. Так, наприкінці 2024 року компанія Match Group, яка володіє такими популярними додатками для знайомств як Tinder та Hinge, оголосила про плани інтегрувати генеративний ШІ у свої сервіси для покращення біографій та профілів користувачів [2]. Крім того ШІ та нейромережі використовуються дейтинг-платформами для оцінки сумісності пари, надання порад в спілкуванні та оформленні профілю, опосередкованого спілкування замість користувача, здійснення перекладу текстових та голосових повідомлень тощо.

Одночасно з цим штучний інтелект в дейтинг-сфері використовується також і з метою надання користувачу послуг персоналізованого спілкування з віртуальним партнером. Слід відмітити розвиток технологічних можливостей таких платформ, що зумовлюється стрімким збільшенням попиту на такий цифровий продукт. Так, сервіси на зразок Candy.ai та Kupid.ai надають можливість користувачу, вибравши статтю майбутнього партнера, створити

вигаданого персонажа, який за допомогою штучного інтелекту дає можливість спілкуватися з ним голосовими повідомленнями [4].

Відкидаючи морально-етичні моменти відносин з цифровою особою слід однак звернути увагу на юридичний контекст, а саме на захист прав користувача подібних дейтинг-платформ. В першу чергу слід говорити про захист інформації, отриманої в межах комунікації з віртуальним партнером, власником платформи від розповсюдження та витоку, а також збереження режиму приватності щодо персональних даних та самого факту надання послуг, адже користувач може не бажати публічності факту надання таких послуг дейтинг-сервісом.

Сучасні додатки для знайомств вже збирають величезну кількість чутливої інформації, такої як геолокація, їхні вподобання, історію листування та навіть фото і відео [3]. Окрім традиційного неконтрольованого поширення таких даних загрозу становить також використання таких даних для створення небіологічних осіб, наділених штучним інтелектом, які, навчаючись на зазначених даних, можуть створювати цифрові клони реальної людини, тим самим користуючись чужою особистістю та вводячи в оману осіб, з якими спілкується в подальшому.

Використання таких цифрових копій осіб вже зараз зумовило проблему поширення випадків свідомого використання можливостей ШІ для маніпулювання емоціями і шахрайських схем. На даний момент практично надзвичайно важко захистити свої права щодо такого «викрадення» особистості через складність доказування та відсутність законодавчих механізмів захисту від використання чужої особистості без дозволу особи.

Підсумовуючи вищевикладене, можна зробити висновок, що проблема свавільного використання штучного інтелекту в дейтинг-індустрії вже зараз ставить перед юридичною наукою завдання вироблення способів захисту прав осіб в мережі Інтернет. Питання збереження індивідуальності особи та загроза потенційного викрадення особистості актуалізують дослідження теоретичних та практичних аспектів доказування в справах щодо захисту особистої інформації в мережі Інтернет.

ЛІТЕРАТУРА:

1. Давидова Н., Менджул М. Правове регулювання цифровізації як вектора розвитку приватного права на прикладі освітніх відносин. *Університетські наукові записки*. 2021. No 1(79). С. 43–54.
2. Довірити своє серце алгоритмам: як штучний інтелект змінює сучасний дейтинг і що з цим може бути не так? 2025. URL: <https://zaborona.com/doviryty-svoje-sercze-algorytmam-yak-shtuchnyj-intelekt-zminyuye-suchasnyj-dejtyng-i-shho-z-czym-mozhe-buty-ne-tak/>
3. Довірити своє серце алгоритмам: як штучний інтелект змінює сучасний дейтинг і що з цим може бути не так? 2025. URL: <https://zaborona.com/doviryty-svoje-sercze-algorytmam-yak-shtuchnyj-intelekt-zminyuye-suchasnyj-dejtyng-i-shho-z-czym-mozhe-buty-ne-tak/>
4. Коноплицький С. Майбутнє дейтингу – «Тіндер» для знайомств із ШІ-моделями. URL: <https://speka.media/maibutnje-deitingu-tinder-dlya-znaiomstv-iz-si-modelyami-pk4lzd>

Резніченко Семен Васильович,

кандидат юридичних наук, професор, професор кафедри цивільно-правових дисциплін Одеського державного університету внутрішніх справ

НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ПЕРЕВЕЗЕНЬ ПАСАЖИРІВ АВТОБУСАМИ

Перевезення пасажирів стало невід’ємною часткою життя суспільства. Більше того, у контексті розуміння перевезення пасажирів у якості одного з можливих способів реалізації права людини на свободу пересування, виникає необхідність забезпечення, включаючи нормативне, можливості реалізації даного права. Враховуючи нерівне правове положення перевізників (деякі з них займають монополічне місце) в силу їх затрат на придбання транспортних засобів і специфіку функціонування транспорту на певних маршрутах, рейсах тощо, виникає ряд питань пов’язаних з встановленням нормативів, що забезпечують вирівнювання правового статусу пасажирів.

Частково це питання вирішується шляхом закріплення у ЦК України ст. 633 (публічний договір), ст. 634 (договір приєднання), які відображають специфіку фактичних правовідносин між перевізником та пасажиром, специфіку договірної конструкції, що застосовується для регулювання відносин, які досліджуються. Та-

кож необхідно сказати про те, що саморегулювання ніяким чином не може захистити права «слабкої сторони». А це значить, що тільки нормативне врегулювання організації перевезень (у нашому випадку це автобусне перевезення) може захистити права «слабкої сторони».

Концепція чинного Цивільного кодексу України (далі ЦКУ) передбачає врегулювання правовідносин на принципах, які можуть забезпечити якісне функціонування сучасного ринку. Ст. 3 ЦКУ закріпила основи цивільного законодавства, серед яких:

- 1) неприпустимість свавільного втручання у сферу особистого життя людини;
- 2) неприпустимість позбавлення права власності, крім випадків, установлених Конституцією України та законом;
- 3) свобода договору;
- 4) свобода підприємницької діяльності, яка не заборонена законом;
- 5) судовий захист цивільного права та інтересу;
- 6) справедливість, добросовісність та розуміння [1, ст. 3].

Більшість договорів врегульовано Цивільним кодексом України. П'ята Книга кодексу поділена на договірні та недоговірні відносини. Цивільно-правовий договір є формою моделювання диспозитивної активності учасників цивільного обороту. Шляхом використання договору у якості основного регулятора суспільних відносин можна досягти необхідного результату правового регулювання у сфері перевезень, включаючи перевезення пасажирів автобусами.

При перевезенні пасажирів транспортом загального користування спрацьовує конструкція договору про приєднання, що нівелює свободу користувача транспортних послуг. Таким чином, виникає необхідність компенсувати частку свободи пасажира шляхом нормативних гарантій забезпечення правового положення, правового статусу пасажира, закріпивши певний комплекс прав і обов'язків сторін договору автобусного перевезення. Такі гарантії

передбачені Статутом автомобільного транспорту Української РСР від 27 червня 1969 року N401 [2], Правилах надання послуг пасажирського автомобільного транспорту від 18.02.1997 р. [3] та в ін.

Посилання на статuti і правила може поставити під сумнів роль цивільно-правового договору в регулюванні суспільних відносин по перевезенню пасажирів автобусом. У якості контраргументу можна навести тезу Самойленка Г.В. про походження правил поведінки. Якщо нормативно-правовий акт виражає волю законодавця то цивільно-правовий договір виражає індивідуалізовану волю сторін. Якщо нормативно-правовий акт породжує загальнообов'язкове правило поведінки, то договір розрахований на регулювання персоналізованої поведінки сторін [4, с. 9].

Сам нормативно-правовий акт у контексті конкретного правовідношення грає неоднозначну роль, з *однієї сторони* він є регулятором суспільних відносин, тобто ідеальною моделлю. Річ у тім, що законодавець ті чи інші ідеї перетворює на норми, тобто існує схема: ідея – норма – правовідношення.

З *другої сторони* він (законодавець) встановлює певні рамки договірної свободи, які слугують свого роду «пісочницею», у межах якої дозволена реалізація свободи і суб'єктивних цивільних прав. З точки зору Зазуляка І.І. надані законодавцем можливості сторонам самостійно встановлювати умови договору виходять з принципу диспозитивності і дозволяють у кожному конкретному випадку досягти домовленості за умовами, які є суттєвими у конкретному договорі. Однак, в такому випадку не повинна порушуватися природа договору з одного боку, а з іншого не повинні існувати протиріччя імперативним приписам норми закону [5, с. 157].

З *третьої сторони* нормативно-правовий акт може містити окремі умови договору. У такому випадку вони є невід'ємною частиною договірних умов. Виходячи з цього Погрібний С.О. стверджує, що правове регулювання договірних відносин є впливом суб'єкта правового регулювання (учасників цивільних правовідносин чи держави) на цивільні суспільні відносини шляхом встановлення норм цивільного права (договірної чи уставної) та їх реалізації

з метою впорядкування зазначених відносин у відповідності до ідеальної моделі, закладеної у цих нормах [6, с. 37].

Фактичні відносини, що пов'язані з перевезенням пасажирів автобусами, складаються таким чином, що, не дивлячись на свободу підприємницької діяльності, свободу договору, вони представляють собою таку модель правовідносин, яка має правову форму. Органи державної влади і місцевого самоврядування активно впливають на дану сферу суспільних відносин шляхом формування механізму їх правового регулювання. Основними елементами цього механізму є правова норма і сама діяльність пов'язана з реалізацією цих норм.

На теоретичному рівні правовою доктриною визнані форми реалізації таких норм, як дотримання (утримання від неправомірних дій); виконання (здійснення активних дій щодо виконання юридичних обов'язків позитивного спрямування); використання (здійснення правомочностей особи) та застосування. А ось, що стосується організаційного характеру, то цивілісти продовжують спори чи включати їх, чи не включати до предмету цивільно-правового регулювання. Але вважається, якщо законодавець включив попередній договір (ст. 635 ЦКУ), а також ряд йому подібних до предмету правового регулювання, які по своїй суті мають організаційний характер, тим самим він визнав сферу організаційних правовідносин сферою цивільно-правового регулювання.

Безумовно, організаційна діяльність у більшості є результатом управлінської діяльності, але їх акти все ж таки, як результат такої управлінської діяльності (включаючи і перевезення пасажирів автобусами) є актами цивільного законодавства, оскільки вони містять ряд приписів, пов'язаних з механізмом правового регулювання саме цивільно-правових відносин.

Самойленко Г.В. стверджує, що стосовно цього питання у науковій літературі такий феномен часто розуміється як «опублікування» цивільного права, як вторгнення публічного права у сферу приватного права. І тут виникає питання, чи є інші способи досягнення мети цивільно-правового регулювання забезпечення прав

пасажира, який у всьому цивілізованому світі вважається «слабкою стороною» договору. Відповідь – скоріше ні, ніж так [7, с. 71].

Виникає питання, якою все ж таки повинна бути ідеальна модель організації перевезення пасажирів автобусами? Відповідь – така, щоб досягти ефективного результату, тобто, забезпечити населення транспортом і комплексом відповідних прав.

Сьогодні існує декілька моделей організації перевезень пасажирів автобусами. *Перша* – це вільний ринок приватних перевізників, які обслуговують певні маршрути на умовах, визначених державними органами чи органами місцевого самоврядування, залежно від виду перевезень (міські, приміські, міжміські та міжнародні). Так, в ст. 14–15 Правил надання послуг автомобільного транспорту закріплено, що регулярні перевезення організовують органи виконавчої влади (по суті вони виступають замовниками перевезень) відповідно з програмами розвитку автомобільного транспорту на певній території з метою задоволення населення у перевезеннях [2]. Ці організатори самі визначають умови перевезень на відповідній території. Така модель організації перевезень успішно застосовується в Україні і в ряді країн Європи.

В Україні більшість ДТП вчиняють приватні перевізники так званих маршрутних таксі, оскільки конкуренція часто породжує агресивну манеру керування. Відсутність жорстких вимог до водіїв є наслідком хамського ставлення до пасажирів, порушення їх прав. Неохайність, куріння за кермом та нав'язливе прослуховування музики не сприяє позитивним емоціям пасажирів.

Друга модель – повноцінна діяльність муніципального транспорту. Вона має свої переваги і недоліки. Основним недоліком є більш висока вартість перевезення по відношенню до перевезень приватними автобусами, але одночасно, на муніципальному транспорті краща культура обслуговування пасажирів і безпека перевезень (Німеччина, Франція).

Третя модель (застосовується в Барселоні, частково в Україні) змішана – це поєднання муніципального автобусного парку і приватного. Воно породжує здорову конкуренцію, результатом

якої плата знижується до оптимальної, а якість перевезень і безпека руху підвищуються. До речі самі іспанці таку модель вважають ідеальною. В Одесі є невеликий муніципальний автобусний парк. Як правило, він використовується як тимчасова заміна перевезень трамваями та тролейбусами.

Підсумовуючи викладене, можна вважати, що ідеальною моделлю перевезень є барселонська модель. У той же час, сама по собі конкуренція серед перевізників не здатна повністю забезпечити охорону і захист прав та інтересів пасажирів, що визиває необхідність застосування нормативного забезпечення реалізації прав пасажирів.

ЛІТЕРАТУРА:

1. Цивільний кодекс України: Закон України від 16.01.2003 № 435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15>.
2. Статут автомобільного транспорту Української РСР від 27 червня 1969 року N401: Постанова Ради Міністрів Української РСР. ЗП УРСР. 1969. № 7. ст. 88.
3. Правила надання послуг пасажирського автомобільного транспорту від 18.02.1997 р.: Постанова Кабінету Міністрів України від 18 лютого 1997 р. № 176 (Офіційний вісник України, 1997 р., число 8, ст. 142).
4. Цивільно-правове регулювання перевезень пасажирів таксі: монографія / О.М. Нечипуренко, С.В. Резніченко, Г.В. Самойленко. Одеса: ОДУВС, 2010. 188 с.
5. Зазуляк І.І. Істотні умови договору: теоретичний аспект: дис. ... канд. юрид. наук. 12.00.03. Харків: Харківський національний університет внутрішніх справ, 2009.– 172 с.
6. Погрібний С.О. Механізм та принципи регулювання договірних відносин у цивільному праві України: монографія. Київ: Правова єдність, 2009. 304 с.
7. Самойленко Г.В. Договір перевезення пасажирів: доктринальні та утилітарні проблеми забезпечення прав пасажирів. *Проблеми законності*: сб. науч. трудов. Харьков: Нац. юрид. ун-т имени Ярослава Мудрого, 2018. Вып. 143. 280 с.

Святошнюк Арина Леонідівна,
*кандидатка юридичних наук, доцентка, доцентка кафедри цивільно-
правових дисциплін Одеського Національного університету ім. І. Мечникова*

ЗМІСТ ЦИВІЛЬНО-ПРАВОВИХ ВІДНОСИН У МЕРЕЖІ ІНТЕРНЕТ

У сучасному світі цифрові технології глибоко інтегрувалися в усі сфери економічної діяльності, особливо у фінансовий сектор. Одним із ключових аспектів цього процесу стали електронні платіжні засоби (далі – ЕПЗ), які значно полегшили проведення фінансових операцій, зробивши їх швидшими, зручнішими та безпечнішими. В Україні розвиток електронних платежів є одним із пріоритетів у рамках цифрової трансформації держави та банківської системи.

Відповідно до Закону України «Про платіжні послуги» електронний платіжний засіб – «платіжний інструмент, реалізований на будь-якому носії, що містить в електронній формі дані, необхідні для ініціювання платіжної операції та/або здійснення інших операцій, визначених договором з емітентом» [1].

Загалом, під електронними платіжними засобами розуміють інструменти, які дозволяють ініціювати безготівкові платежі з використанням електронних технологій. До таких засобів належать: 1) банківські платіжні картки (дебетові, кредитні, віртуальні); 2) мобільні платформи для платежів (Apple Pay, Google Pay, Garmin Pay); 3) системи інтернет-банкінгу (наприклад, Приват24, monobank); 4) електронні гаманці та платіжні сервіси (Portmone, EasyPay, iPay.ua); 5) QR-платежі та NFC-технології; 6) криптовалюти та цифрові активи.

Станом на 2025 рік електронні платежі стали домінуючим способом розрахунку в Україні. За даними Національного банку України: кількість платіжних карток перевищила 90 млн частка безготівкових розрахунків зросла до понад 60%; активно розвивається інфраструктура приймання безготівкових платежів: кількість POS-терміналів зросла на понад 15% за рік; мобільні та онлайн-

платежі стали основним каналом оплати для мільйонів українців [2]. Слід також зазначити, що особливо важливу роль у цьому відіграли не лише банки, а й фінтех-компанії, які пропонують інноваційні та зручні рішення.

Зокрема, серед основних переваг електронних платіжних засобів можна виокремити: швидкість та зручність – миттєве проведення операцій; безпека – застосування багаторівневої аутентифікації; прозорість – легкість у відстеженні та контролі витрат; зниження обігу готівки – сприяє зменшенню тіньової економіки; інтеграція в глобальну економіку – спрощення міжнародних платежів.

Не зважаючи на стрімкий розвиток, існують проблеми, які стримують ще ширше впровадження ЕПЗ: нерівномірний доступ до цифрових сервісів між містом та селом; низький рівень цифрової та фінансової грамотності у частини населення; кіберзагрози та фінансове шахрайство; неповна законодавча регламентація новітніх форм платежів; недовіра окремих груп населення до безготівкових операцій.

Проте, ринок електронних платіжних засобів в Україні має значний потенціал для подальшого зростання. Серед ключових напрямів розвитку: розвиток цифрової гривні (eUAH) – пілотний проєкт Національного банку; інтеграція з системами Open Banking – відкриття API для фінансових сервісів; розширення партнерств між банками та фінтех-компаніями; поширення фінансової грамотності серед населення; вдосконалення законодавства щодо новітніх платіжних технологій.

Крім того, очікується, що в найближчі 3–5 років ЕПЗ повністю домінуватимуть у роздрібних платежах в Україні.

Таким чином, ЕПЗ вже стали невід’ємною частиною фінансової системи України. Вони забезпечують зручність, безпеку та ефективність розрахунків, сприяючи прозорості економіки та підвищенню добробуту населення. Надалі успішність розвитку ЕПЗ буде залежати від державної політики, технічної інфраструктури та рівня довіри споживачів до цифрових технологій.

ЛІТЕРАТУРА:

1. Про платіжні послуги: закон України від 30.06.2021 за станом на 15.11.2024 N1591-IX. URL: <https://zakon.rada.gov.ua/laws/show/1591-20#Text>.

2. Звіт НБУ про платіжний ринок України, 2025. Національний банк України. URL: www.bank.gov.ua.

Спасова Катерина Іванівна,

*кандидатка юридичних наук, доцентка, доцентка кафедри цивільного права
Національного університету «Одеська юридична академія»*

ЦИВІЛЬНО-ПРАВОВІ АСПЕКТИ ЦИФРОВОЇ ІДЕНТИЧНОСТІ В СОЦІАЛЬНИХ МЕРЕЖАХ

У ХХІ столітті цифрова ідентичність стала невід’ємною частиною соціального буття людини. У віртуальному просторі формується нова парадигма представлення особистості – від цифрового образу до цифрової особистості. Це викликає потребу у правовому осмисленні цифрової ідентичності та її захисті засобами цивільного права і процесу. Особливої актуальності ця тема набуває в контексті масового поширення соціальних мереж, де кожна особа має змогу створити, модифікувати або втратити контроль над своїм цифровим образом.

Особливої ваги проблема набуває в умовах гібридної війни, коли кіберпростір стає ареною інформаційної боротьби, а соціальні мережі та месенджери – інструментами як впливу, так і зловживань. Сучасні реалії демонструють небезпечні тенденції – масове викрадення облікових записів у Telegram, Viber, WhatsApp, Facebook тощо. Ці випадки супроводжуються привласненням цифрової ідентичності, використанням її для здійснення шахрайських дій, поширення дезінформації або психологічного впливу. Такі дії мають не лише кримінальну, а й цивільно-правову природу, адже завдають шкоди особистим немайновим правам особи та її репутації.

Під цифровою ідентичністю розуміємо сукупність даних, які дозволяють ідентифікувати особу у цифровому середовищі: ім’я, фото, електронні профілі, поведінкові маркери, біометричні дані тощо. У контексті соціальних мереж це – цифровий відбиток ко-

ристувача, створений через його активність, який формує публічне уявлення про нього. Згідно з дослідженням Є.О. Харитонова, О.І. Харитонової, цифрова особистість охоплює всі елементи, що дозволяють представити людину у віртуальному просторі, включно з її комунікацією, уподобаннями, зображенням, поведінковими рисами та контентом, яким вона ділиться онлайн [1, С. 6].

З правової точки зору цифрова ідентичність вважається об'єктом права – вона не є суб'єктом, але може підпадати під захист особистих немайнових прав (ім'я, зображення, недоторканність приватного життя) та частково – інтелектуальної власності. Проблема полягає в тому, що її статус не врегульований на рівні Цивільного кодексу України або спеціального закону. Слід звернути увагу на те, що відсутність чіткого нормативного визначення цифрової ідентичності створює колізії у випадках її порушення, особливо у справах, пов'язаних з репутацією, доступом до акаунтів, або deepfake-контентом.

У цьому контексті важливо звернутися до проблематики порушення немайнових прав інтелектуальної власності у соціальних мережах. Так, платформи типу Facebook, Instagram чи Youtube є осередками масового копіювання контенту – від фото і відео до літературних творів – без згоди авторів. Цифрова природа інформації у мережі нівелює різницю між оригіналом і копією, а традиційні правові механізми виявляються неефективними в умовах бінарного середовища. Сторінка користувача в соціальній мережі, яка поєднує персональні дані, візуальні і текстові елементи, може розглядатись як складний об'єкт авторського права [2, С. 164].

Цифрову ідентичність можна вважати складовою частиною немайнових благ, які згідно зі ст. 201 ЦК України є об'єктами цивільних прав. Статті 277 та 297 ЦК України забезпечують захист честі, гідності та ділової репутації, що може бути застосовано у разі поширення неправдивої інформації або створення фейкового образу особи в мережі. Однак цього часто недостатньо. Соціальні мережі стають не лише платформою для самовираження, а й потенційним джерелом правопорушень, де факт порушення ідентичності складно довести без комплексної правової доктрини.

Одним із ключових інструментів захисту цифрової ідентичності є цивільне судочинство. Позови можуть стосуватися: спростування недостовірної інформації, заборони використання чужого акаунта, відшкодування моральної шкоди, визнання права на доступ або повернення контролю над акаунтом. У зв'язку з цим постає проблема допустимості та автентичності доказів у вигляді скріншотів, записів, метаданих, що вимагає вдосконалення процесуального законодавства, зокрема в частині електронних доказів.

Філософські та соціологічні аспекти цифрової ідентичності дозволяють глибше зрозуміти природу цього явища. Як стверджують Л. А. Усанова, Г. Г. Супрун, цифрова ідентичність є інструментом самопрезентації у мережевому просторі. Вона може бути як справжнім «Я», так і сконструйованим образом, що слугує певній меті – соціальній легітимації, впливу, маніпуляції чи ідентифікації у певному соціальному контексті. У цьому контексті особливої ваги набуває поняття мобільної ідентичності, що змінюється залежно від середовища і цілей користувача [3, С. 69].

Окремої уваги заслуговує явище цифрової спадщини. Після смерті користувача його акаунти, контент, цифрові образи не зникають, а продовжують існувати у віртуальному просторі. О. І. Харитонova і Є. О. Харитонов вводять термін «цифрова смерть» – момент, коли цифрова ідентичність особи переходить у режим спадщини. Важливим є питання про те, хто має право на управління цими активами: спадкоємці, платформи чи держава? Наразі ст. 1236 ЦК України лише частково зачіпає це питання, але комплексного підходу у законодавстві поки немає.

Отже, цифрова ідентичність у соціальних мережах – це складний правовий, соціальний та технологічний феномен. Вона потребує:

- доктринального осмислення як об'єкта цивільних прав;
- включення у класифікації нематеріальних благ та об'єктів особистих немайнових прав;
- оновлення підходів до процесуального захисту – особливо у сфері електронних доказів;

- розробки спеціального законодавства щодо цифрової спадщини та цифрових прав особи;
- введення спеціального режиму правового регулювання соціальних мереж, який забезпечить реальний захист цифрової ідентичності, включаючи право розпорядження контентом, створеним користувачем;
- врахування ризиків кіберзагроз і масового привласнення цифрової особистості у період гібридної війни – як додаткового чинника, що потребує негайного юридичного реагування.

Вивчення цифрової ідентичності на стику права, філософії та соціальних комунікацій дає змогу сформулювати нові підходи до розуміння особистості в епоху інформаційного суспільства.

ЛІТЕРАТУРА:

1. Харитонova О. І., Харитонов Є. О. Цифрова людина, цифрова особа та цифрова особистість: до проблеми співвідношення. *Часопис цивілістики*. 2023. Вип. 49. С. 5–13. URL: http://nbuv.gov.ua/UJRN/Chas_2023_49_3
2. Відшкодування шкоди завданої розповсюдженням недостовірної інформації в соціальних мережах. *Науковий вісник Міжнародного гуманітарного університету. Серія «Юриспруденція»*. 2019. № 42. Т. 1. С. 162–165.
3. Усанова Л. А., Супрун Г. Г. Цифрова ідентичність як відображення інформаційного суспільства. *Актуальні проблеми філософії та соціології*. 2021. № 13. С. 67–70. URL: http://apfs.nuoua.od.ua/archive/30_2021/13.pdf

Токарева Віра Олександрівна,

*кандидатка юридичних наук, доцентка, доцентка кафедри цивільного права
Національного університету «Одеська юридична академія»*

ДО ПИТАННЯ ВИКОРИСТАННЯ АВТОНОМНИХ СИСТЕМ У ЗБРОЙНОМУ КОНФЛІКТІ

Протягом останнього десятиліття дискусії навколо використання автономних систем у військовій сфері значною мірою були зосереджені на автономних системах зброї. Використання автономних систем зброї дійсно викликають гостре занепокоєння, оскільки використання автономних систем полягає в тому, що вони вико-

ристовується для збору розвідданих та для підтримки військових для вибору і ураження цілей. Останній аспект викликає занепокоєння.

Наразі випадки ІІІ під час ведення ввоєнних дій не завершуються наданням автономії збройовим системам, таким як включення системи в командування і управління даними, логістику та навчання. Занепокоєння викликає саме те, що автономні системи у озброєнні можуть запропонувати військові цілі та давати рекомендації своїм (людським) операторам, які можуть самостійно атакувати цілі, з урахуванням оброблених даних.

Відповідно до оборонних стратегій Організації Північноатлантичного договору зазначається, що критичними проблемами майбутніх десятиліт може саме дані які генеруються системами, а не робототехнік як така або притаманна їй автономія. Адже стверджується, що такі системи здатні розробляти дієві автономні системи для поліпшення таргетування, з огляду на оброблені данні[1]. Разом з тим, ефективність систем штучного інтелекту визначається якістю навчальних даних, оскільки вони забезпечують їх основні специфікації. Крім того, автономним системам властива непередбачуваність як призводить до проблем, ставлячи виклик міжнародному гуманітарному праві в цілому. В свою чергу виклики автономних систем полягають у відсутності розуміння та чинності для людини функціонування «чорного ящик». Тому, постає актуальними підтримання якості та походження даних, а також збереження за людиною прийняття остаточного рішення щодо вибору та залучення цілі.

Таргетування широко визначається як застосування сили сторін конфлікту проти окремих осіб або об'єктів поза їх контролем. Відповідно до міжнародного гуманітарного права цільовий відбір та залучення повинні дотримуватися основних принципів розрізнення, пропорційності, людяності та вимоги вжити всіх можливих запобіжних заходів.

Слід зазначити, що міжнародне гуманітарне право зобов'язує військових командирів та інших осіб, відповідальних за напади, за-

сновувати свої рішення на інформації з усіх джерел, доступних їм у відповідний момент часу. Зокрема, Міжнародний Комітет Червоного Хреста (далі МКЧХ) в контексті ведення міської війни рекомендує, проводити перевірку даних про наявність цивільних осіб та цивільних об'єктів, яка міститься у відкритих джерелах, таких як Інтернет. Відповідно до висновків МКЧХ системи підтримки прийняття рішень на основі ІІІ можуть допомагати збору та обробці даних, для сприяння оперативного прийняття рішень в умовах конфлікту та мінімізації ризиків для цивільного населення [2].

Прихильники використання систем штучного інтелекту у воєнних конфліктах стверджують, що ця технологія покликана «підвищити» військову точність. Разом з цим, дане твердження є не однозначним, оскільки походження та надійності даних які обробляються системою може бути сумнівним. Відтак одна із провідних проблем пов'язана із низькою якістю навчальних даних, що може призводити до упереджень, неправильних оцінок, ризиків втручання у приватність та втрати контролю управління над системою, які в поєднанні з непередбачуваністю технології створюють проблеми для ідентифікації цілей. Відсутність репрезентативності в навчальних даних здатно призвести до того, що автономні системи можуть некоректно ідентифікувати представників різних етнічних груп, в якості мішені або сприймати цивільних чоловіків, в якості як учасників бойових дій, через заковані гендерні упередження [3].

Не лише держави змагаються у лідерству озброєння але й лідери Big Tech також активно створюють та просувають свої технології збройним силам держав. Незважаючи на виникаючі ризики, автономні системи озброєння активно використовуються під час конфліктів, що не виключає ризиків ураження та цивільного населення.

Слід зазначити, що використання ІІІ протягом всього процесу таргетування спирається на прогнози, засновані на розпізнаванні образів і класифікації, через узагальнення даних, що використовуються під час навчання системи. Таким чином, здатність автономних систем рекомендувати цілі залежить від здатності «виявляти»

подібність між наявними та непрямими даними про населення та даними на яких систем навчалась. Це може викликати проблеми, через недосконалість автономних систем та можливі проблеми коректної ідентифікації через те, що навчальні данні та реальні поля відрізняються [3]. Оскільки, попри всі зусилля розробників, не можливо заздалегідь спроектувати усі варіанти можливих сценаріїв

Враховуючи викладене слід констатувати наступні основні проблеми використання автономних систем під час збройних конфліктів: ризики некоректної ідентифікації цивільного населення в якості цілі; неякісні початкові дані без належної репрезентативності вразливих груп та меншин, що призводить до упередженості даних та упередженості автономних систем.

ЛІТЕРАТУРА:

1. Summary of the NATO Artificial Intelligence Strategy. 2021. URL: https://www.nato.int/cps/en/natohq/official_texts_187617.htm
2. Stewart R. Hinds G. Algorithms of war: The use of artificial intelligence in decision making in armed conflict. October 24, 2023. URL: <https://blogs.icrc.org/law-and-policy/2023/10/24/algorithms-of-war-use-of-artificial-intelligence-decision-making-armed-conflict/>
3. Alvarez J.S. The risks and inefficacies of AI systems in military targetingsupport. 2024. URL: <https://blogs.icrc.org/law-and-policy/2024/09/04/the-risks-and-inefficacies-of-ai-systems-in-military-targeting-support/>

Вовчок Руслан Володимирович,

аспірант 2 року навчання Миколаївського навчально-наукового інституту права Національного університету «Одеська юридична академія».

Науковий керівник: к.ю.н., доц., доц. кафедри цивільного права Фасій Б. В.

ІНФОРМАТИЗАЦІЯ ТА ЦИФРОВІЗАЦІЯ СУСПІЛЬСТВА В ЕПОХУ СТІМКОГО РОЗВИТКУ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

У XXI столітті світ вступив у фазу глобальної цифрової трансформації. Інформатизація та цифровізація стали невід'ємною частиною розвитку суспільства. На цьому тлі особливе місце займає стрімкий розвиток штучного інтелекту (ШІ), який змінює не лише технологічні підходи, а й соціальні, економічні та культурні процеси.

Інформатизація являє собою процес широкомасштабного впровадження сучасних інформаційних технологій у всі сфери суспільного життя з метою забезпечення ефективного доступу до інформації, її зберігання, обробки та використання.

Основна мета інформатизації – підвищення ефективності діяльності в освіті, медицині, промисловості, управлінні, науці тощо завдяки впровадженню комп'ютерної техніки та програмного забезпечення. Цей процес передбачає створення та розвиток інформаційних систем, автоматизацію документообігу та управління, створення інформаційно-комунікаційної інфраструктури (Інтернет, бази даних, хмарні сервіси) та навчання населення основам роботи з ІКТ (інформаційно-комунікаційними технологіями).

Цифровізація насамперед є процесом перетворення традиційних аналогових процесів у цифрові, а також впровадження цифрових технологій у всі сфери життя з метою якісної трансформації діяльності, комунікації, управління та обслуговування. Вона є наступним етапом після інформатизації, який охоплює не лише інструменти, а й перегляд та зміну підходів до взаємодії в суспільстві. Основними ознаками цифровізації є створення цифрових сервісів для населення, використання великих даних, хмарних технологій, Інтернету речей та самого штучного інтелекту, а також розвиток цифрової економіки та цифрової держави (типу порталу «Дія», онлайн-банкінгу, онлайн-навчання та цифрових паспортів).

Інформатизація створює основу для цифровізації. Якщо інформатизація забезпечує «інструменти» та «ресурси», то цифровізація використовує ці інструменти для повноцінної трансформації способу життя, роботи та взаємодії в суспільстві.

Штучний інтелект (ШІ) є галуззю комп'ютерних наук, яка створює системи, здатні самостійно аналізувати інформацію, навчатися, ухвалювати рішення та виконувати інтелектуальні задачі, що раніше вимагали участі людини. ШІ є одним з ключових рушіїв цифрової трансформації, оскільки здатен обробляти великі обсяги даних і автоматизувати складні процеси у найрізноманітніших сферах.

Основні напрямки застосування ІІІ в цифровізації:

1. Автоматизація рутинних процесів: ІІІ дозволяє замінювати ручну працю в офісах, на підприємствах, у сфері обслуговування. Наприклад, чат-боти в банках та службах підтримки автоматично відповідають на запити клієнтів.

2. Аналітика та прогнозування: ІІІ здатен обробляти великі масиви даних (Big Data), знаходити закономірності, робити прогнози. Прикладом є медичні системи, що прогнозують хвороби, або економічні моделі, які передбачають зміни на ринку.

3. Персоналізація послуг: Алгоритми ІІІ допомагають адаптувати контент під користувача: рекомендації в YouTube, Netflix, інтернет-магазинах.

4. Розпізнавання образів та мови: Технології комп'ютерного зору використовуються в безпеці, охороні, медицині (наприклад, виявлення пухлин).

5. Розумне управління містами та інфраструктурою: «Розумні міста» використовують ІІІ для оптимізації транспорту, енергоспоживання, екологічного моніторингу.

Інформатизація та цифровізація є ключовими процесами формування інформаційного суспільства, у якому головним ресурсом стає інформація та знання, а провідну роль відіграють інформаційно-комунікаційні технології (ІКТ).

Етапи цифрової трансформації суспільства:

1. Інформатизація (1980–2000-ті роки): Комп'ютеризація підприємств і навчальних закладів, формування глобального Інтернету, поява електронного документообігу.

2. Цифровізація (з 2010-х): Цифрова економіка, цифрова освіта, цифрове здоров'я, держава в смартфоні (наприклад, «Дія»), масове використання хмарних технологій, мобільних додатків, Big Data.

3. Інтелектуалізація (сучасний етап): Впровадження штучного інтелекту у всі сфери життя, розумні системи ухвалення рішень, автономний транспорт, нейромережі, робототехніка, перехід до суспільства «інтелектуальних технологій». Інтелектуалізація

є процесом активного впровадження інтелектуальних технологій (зокрема, штучного інтелекту, машинного навчання, нейромереж, експертних систем) у різні сфери життя людини, з метою оптимізації рішень, автоматизації складних процесів та підвищення ефективності управління знаннями.

Інформатизація та цифровізація є одними з найвпливовіших процесів сучасності, що кардинально змінюють обличчя людської цивілізації. У поєднанні з розвитком технологій штучного інтелекту вони формують абсолютно нову реальність, у якій перетворюються не лише засоби комунікації та праці, а й цінності, соціальні інститути та саме бачення майбутнього.

Штучний інтелект, будучи логічним продовженням цифрової трансформації, стає не просто інструментом, а новим партнером людства. Завдяки йому ми можемо підвищити ефективність виробництва, вдосконалити охорону здоров'я, зробити освіту більш доступною та персоналізованою, забезпечити прозорість у державному управлінні та якісно змінити взаємодію між людиною й машиною.

Цифрове майбутнє не є чимось віддаленим – воно вже сьогодні формується нашими діями, вибором і знаннями. Завдання сучасного суспільства – не лише адаптуватися до змін, а активно формувати цифрову культуру, засновану на знаннях, етиці та інноваціях.

ЛІТЕРАТУРА:

1. Закон України «Про національну програму інформатизації». <https://zakon.rada.gov.ua/laws/show/2807-20#Text>
2. Стадніченко, О (2013). Інформатизація як чинник розвитку суспільства і держави. <http://conferences.neasmo.org.ua/>
3. Іванов, А. (2019). Штучний інтелект в епоху цифрової трансформації. Журнал «Технічні інновації», № 5, стор. 112–124.
4. Міністерство цифрової трансформації України. (2023). Цифрове майбутнє України: програма розвитку електронного урядування. <https://thedigital.gov.ua/>

ВЕРИФІКАЦІЯ БАНКІВСЬКИХ КАРТ КЛІЄНТА

Верифікація (перевірка) картки має вирішальне значення для компаній, оскільки вона допомагає запобігти шахрайству та відкликанню платежів. Перевіряючи особу власника картки, продавці можуть зменшити ризик несанкціонованих операцій, захищаючи як бізнес, так і його клієнтів.

Під верифікацією картки розуміється процес підтвердження особи власника картки під час транзакції. Це відбувається за допомогою різних методів, таких як введення PIN-коду, підпису або біометричної автентифікації, щоб переконатися, що особа, яка здійснює платіж, має право використовувати картку [1, 2].

Також перевірка картки важлива з кількох ключових причин, зокрема:

1. Захист клієнтів. Перевірка карток пропонує клієнтам певну фінансову безпеку. Ефективна система може позначати несанкціоноване використання втрачених або вкрадених карток на ранніх стадіях транзакції, зменшуючи потенційний фінансовий збиток для власника картки.

2. Взаємодія з клієнтами. Правильно виконана перевірка картки покращує взаємодію з клієнтами та сприяє безпеці транзакцій. Ця підвищена впевненість може призвести до підвищення лояльності клієнтів і збільшення кількості повторних транзакцій. Крім того, нижчий рівень випадків шахрайства дає змогу командам обслуговування клієнтів спрямувати свою увагу на інші проблеми та покращити загальну якість обслуговування.

3. Фінансовий стан. Ефективні заходи перевірки карток допомагають бізнесу підтримувати стабільне фінансове середовище. Менший дохід, втрачений через шахрайство та повернення платежів, означає більше ресурсів для інших проєктів, орієнтованих на зростання.

4. Заходи перевірки карток допомагають компаніям дотримуватися галузевих стандартів і правил, що не підлягає обговоренню

для компаній, які обробляють платежі картками. Дотримання стандартів відповідності також мінімізує ризик зіткнутися зі штрафними санкціями або юридичними проблемами, які можуть дорого коштувати підприємствам.

До основних методів перевірки картки можна віднести:

По – перше, перевірка верифікаційного значення картки (CVV) Перевірка три- або чотиризначного коду на звороті картки є простим і ефективним методом перевірки. Запитуючи у клієнтів цей код під час оформлення замовлення, підприємства можуть ускладнити неавторизованим особам здійснення покупки за допомогою даних викраденої картки.

По – друге, за допомогою AVS (служба перевірки адреси) компанії співвідносять платіжну адресу, надану під час транзакції, з адресою, пов'язаною з картою. Невідповідність може викликати додаткові етапи перевірки або навіть призупинити транзакцію.

Наступний етап це двофакторна автентифікація (2FA). 2FA пропонує додатковий рівень безпеки, який зазвичай надсилає текстові повідомлення або сповіщення програми на телефон власника картки. Ця система допомагає підтвердити, що особа, яка намагається здійснити транзакцію, також має доступ до телефону, пов'язаного з картковим рахунком.

Також це може бути метод токенизації. Який замінює конфіденційні дані картки випадково згенерованим числом або «токеном». Коли компанії зберігають цей токен, а не інформацію про картку, вони мінімізують ризик витоку даних і роблять хакерам складнішим отримати корисну інформацію.

Щодо геофільтрація, то за таким методом підприємства можуть установлювати межі на основі географічного походження транзакції. Якщо картку походить із країни чи регіону з високим рівнем шахрайства, компанія може запровадити додаткові перевірки, щоб підтвердити легітимність транзакції.

Цікавим методом є поведінкова біометрія. Цей складний метод вивчає поведінку клієнта під час транзакції. Такі елементи, як динаміка натискання клавіш, рухи миші та навіть кут, під яким

тримають мобільний пристрій, можуть допомогти перевірити особу особи, яка здійснює транзакцію.

До останнього методу можна віднести алгоритми машинного навчання. З часом системи можуть навчитися виявляти підозрілу активність на основі даних транзакцій. Цей метод, що самовдосконалюється, є одним із найсучасніших способів боротьби з шахрайством, оскільки він постійно адаптується до нових методів, які використовують шахраї. Кожен із цих методів сприяє створенню багаторівневої системи перевірки карток. Ця система пропонує компаніям гнучкий захист від шахрайських транзакцій, надаючи клієнтам більш безпечний і надійний спосіб оплати [3, 4, 5].

Підсумовуючи, необхідно зазначити, що з появою цифрових платежів банківські картки набувають все більшої популярності, саме тому верифікація карток є дуже важливою та має свої особливості з якими користувачі можуть стикатися на практиці.

ЛІТЕРАТУРА:

1. Словник з визначенням верифікації. URL: https://csrc.nist.gov/glossary/term/identity_verification
2. Верифікація картки (Verify). URL: <https://wiki.wayforpay.com/view/852189>
3. General information. URL: <https://docs.tranzzo.com/docs/transactions-lookup/overview/>
4. Understanding Card Verification: What It Is and How It Worksndi. URL: [nverhttps://staxpayments.com/blog/understanding-card-verification/#:~: text=It%20is%20a%20three%2Ddigit, physical%20possession%20of%20the%20card](https://staxpayments.com/blog/understanding-card-verification/#:~:text=It%20is%20a%20three%2Ddigit,physical%20possession%20of%20the%20card)

Коштура Богдан Вячеславович,

*аспірант 1 року навчання кафедри цивільного права та процесу ДВНЗ
«Ужгородський національний університет».*

ШТУЧНИЙ ІНТЕЛЕКТ ЯК УЧАСНИК ЕЛЕКТРОННИХ ПРАВОЧИНІВ

Стрімкий розвиток штучного інтелекту та його активне впровадження в електронну комерцію та інші цифрові сервіси зумовили необхідність переосмислення традиційних цивілістичних кон-

струкцій, зокрема категорії правосуб'єктності. На сучасному етапі ІІІ-системи здатні не лише обробляти запити та аналізувати інформацію, а й автономно ініціювати, укладати та виконувати електронні правочини. Це ставить під сумнів сталі уявлення про суб'єктів цивільного права, які традиційно пов'язуються виключно з фізичними або юридичними особами.

Проблема правосуб'єктності ІІІ в електронних правочинах полягає у відсутності чіткого нормативного статусу таких систем. Виникає низка запитань: чи може штучний інтелект виступати стороною договору, які наслідки матиме укладення правочину за участю ІІІ, хто несе відповідальність у разі порушення умов такого правочину? Відповіді на ці питання є критично важливими для забезпечення правової визначеності та передбачуваності правовідносин у цифровому середовищі.

Наразі в українському законодавстві, як і в більшості інших країн, відсутній спеціальний правовий режим для штучного інтелекту, що породжує колізії та ускладнює захист прав та інтересів суб'єктів ІТ-відносин. Тому дослідження правосуб'єктності ІІІ в контексті електронних правочинів є актуальним і необхідним з точки зору розвитку цивільного законодавства, адаптованого до цифрової трансформації суспільства.

Актуальність теми полягає в необхідності правового реагування на нову реальність, у якій штучний інтелект здатен автономно брати участь в електронних правочинах. Відсутність визначення правового статусу таких систем створює ризики для учасників цивільних правовідносин, знижує рівень правової визначеності та ускладнює захист прав споживачів і контрагентів у цифровій сфері.

Завдання дослідження полягають у наступному: визначити можливість і межі визнання ІІІ суб'єктом електронного правочину; проаналізувати правові наслідки участі ІІІ в укладенні та виконанні правочинів; окреслити перспективи законодавчого закріплення правового статусу ІІІ в цивільному праві України.

Наукова новизна полягає у формулюванні підходу до розгляду штучного інтелекту як особливого учасника цивільних право-

відносин, здатного виступати стороною електронного правочину. Обґрунтовано доцільність запровадження нової правової конструкції – «електронного агента» – для систем ШІ, які діють автономно в межах надання послуг.

Електронні правочини стали невід’ємною частиною сучасних цивільних правовідносин у сфері надання послуг. Відповідно до чинного законодавства, електронний правочин – це дія однієї або кількох осіб, спрямована на встановлення, зміну або припинення цивільних прав і обов’язків, що вчиняється з використанням інформаційно-комунікаційних технологій. З огляду на розвиток цифрової економіки та діджиталізацію суспільства, дедалі більше правочинів укладаються саме в електронній формі – через веб-платформи, мобільні застосунки або автоматизовані системи. [1]

На сьогодні сторонами електронного правочину можуть бути фізичні або юридичні особи, а також суб’єкти публічного права. В електронному середовищі ідентифікація сторін забезпечується через кваліфіковані електронні підписи, облікові записи або інші електронні засоби. При цьому всі суб’єкти, які беруть участь в електронному правочині, повинні мати волю, правоздатність та здатність нести юридичну відповідальність. Однак стрімкий розвиток штучного інтелекту зумовлює появу нового виклику: чи може автономна система ШІ бути стороною електронного правочину? [2]

У сучасному правовому полі автономні системи ШІ поки що не визнані повноцінними суб’єктами права. Проте на практиці вони вже сьогодні виконують функції укладання договорів без прямого втручання людини. Наприклад, в електронній комерції широко застосовуються чат-боти та алгоритми ШІ, які самостійно обробляють замовлення, формують пропозиції, погоджують умови та надсилають підтвердження угод. У таких випадках виникає правове питання: хто є реальною стороною правочину – користувач, що налаштував ШІ, чи сама система, що діяла самостійно? [3]

У зарубіжній практиці вже спостерігаються спроби вирішити це питання. Наприклад, у Сінгапурі Національне агентство з інформаційних технологій у 2021 році опублікувало концепцію «дове-

ного електронного агента», відповідно до якої системи штучного інтелекту можуть укладати угоди в інтересах своїх користувачів, якщо останні належним чином запрограмували їх на відповідні дії. Аналогічний підхід простежується в Ізраїлі, де на рівні рекомендацій розглядається можливість юридичного визнання автономних агентів як інструментів здійснення правочинів. У Сполучених Штатах Америки окремі штати (зокрема, Вермонт і Невада) законодавчо закріпили можливість використання смарт-контрактів і автономних програм для укладення угод без участі людини, покладаючи відповідальність на власника або розробника такого ПЗ. [4, с. 123]

Конструкція «електронного агента» – це новий підхід у цивільному праві, який передбачає можливість виконання електронних правочинів від імені людини або юридичної особи автономною системою, зокрема штучним інтелектом. Такий агент діє за попередньо заданим алгоритмом або в межах дозволених повноважень, не потребує прямого втручання особи в кожен правочин.

Юридично «електронний агент» не є суб'єктом права, однак визнається як засіб реалізації волі сторони, яка його використовує. Відповідальність за дії агента несе той, хто його створив, налаштував або використав. Ця конструкція дозволяє легалізувати участь ІІІ в електронних правочинах без необхідності надання йому правосуб'єктності, забезпечуючи гнучке правове регулювання в умовах цифровізації.[5, с. 13]

Таким чином, хоча законодавство України поки що не визнає ІІІ як самостійну сторону електронного правочину, міжнародний досвід свідчить про актуальність формування нових підходів до правосуб'єктності автономних систем. Це, своєю чергою, потребує розвитку національного цивільного законодавства з урахуванням технологічної реальності та потреб безпечного, правово визначеного використання штучного інтелекту в сфері надання послуг.

ЛІТЕРАТУРА:

1. Calo, R., Kerr, I. & McGregor, L. (2022). Robot Rules: Regulating Artificial Intelligence. 2nd ed. Oxford: Oxford University Press
2. European Commission. (2023). Proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). Brussels: COM(2022) 496 final. URL: <https://eur-lex.europa.eu>

3. Pagallo, U. (2023). AI Agents and the Law: On Rights, Duties, and Responsibilities. In: Corrales, M., Fenwick, M., & Forgó, N. (Eds.), Law and Technology in a Global Digital Society. Springer.
4. Wischmeyer, T. (2022). A Legal Framework for Artificial Intelligence: European and Global Perspectives. German Law Journal, 23(2), 121–135
5. Koops, B.-J., & Leenes, R. (2022). Responsibility and Accountability in a Hybrid Human-AI World. Law, Innovation and Technology, 14(1), 1–24.

Романовський Денис Сергійович,
*аспірант 2 року навчання кафедри цивільного права Національного
університету «Одеська юридична академія», адвокат.*

ІТ ПРАВА ТА КІБЕРБЕЗПЕКА ЛЮДЕЙ ПОХИЛОГО ВІКУ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Сучасне суспільство стрімко цифровізується, що відкриває нові можливості для соціальної інтеграції та забезпечення прав людини. Цифрові технології відіграють ключову роль у забезпеченні доступу громадян до інформації, державних послуг і соціальних гарантій. Водночас цифровізація суспільства породжує низку викликів для вразливих категорій населення, зокрема людей похилого віку. В умовах гібридної війни кіберзагрози стають не лише інструментом економічної та політичної дестабілізації, а й безпосередньою загрозою для інформаційної безпеки літніх осіб, які нерідко мають обмежені навички користування цифровими технологіями. Люди похилого віку часто стають мішенню для кібератак, онлайн-шахрайства, інформаційних маніпуляцій, що ставить під загрозу їхні особисті дані, фінансову безпеку та доступ до державних послуг.

Згідно звіту про діяльність Департаменту кіберполіції Національної поліції України у 2024 році, негативний вплив на криміногенну ситуацію у кіберпросторі Україні мали такі фактори: збройна агресія РФ проти України; поширення глобальних кіберзагроз, таких як атаки на ланцюги постачання (supply chain attacks), кібервикрадення даних (data breaches) та використання штучного інтелекту для вчинення злочинів; масове поширення таких способів вчинення кримінальних правопорушень як фішинг, вішинг, бейтінг, скі-

мінг, злам облікових записів тощо; поширення особистих даних, що сприяє вчиненню майнових злочинів у кіберпросторі; використання сервісів анонімізації під час вчинення кримінальних правопорушень; зростання обсягів використання інтернет-банкінгу. [1]

Відповідно до інформації Державної служби статистики України станом на 1 січня 2022 року майже кожен 4 житель України є старшим 60 років [2]. Тобто люди похилого віку є значним пластом населення України, який, з огляду на стрімко зростаючу важливість інформаційних технологій, потребує відповідної уваги.

На підставі даних Всеукраїнського опитування проведеного Київським міжнародним інститутом соціології у вересні 2022 року, серед респондентів людей похилого віку 48,4% не користуються інтернетом, 17,7% користуються 2–3 години на тиждень і рідше, 32,1% щодня не менше 3-х годин. [3] Згідно аналогічного опитування проведеного у вересні-жовтні 2023 року частка регулярних користувачів інтернетом, серед людей похилого віку, порівняно з 2022 роком зросла до 50%, а частка тих, хто взагалі не користується інтернетом, відповідно, знизилася до 30%. [4] Вказане свідчить про значне зростання кількості людей похилого віку, які є регулярними користувачами інтернету. Проте залишається суттєва частка людей похилого віку, яка має обмежений доступ (або взагалі немає) до банківських послуг в інтернеті, телемедицини, державних електронних послуг тощо.

Недостатній рівень цифрової грамотності унеможливорює ефективне користування державними електронними послугами, онлайн-банкінгом, телемедициною та іншими сервісами, що робить літніх осіб більш вразливими перед кібератаками та інформаційними маніпуляціями.

Кількість випадків шахрайства та кібератак, спрямованих на людей похилого віку, стрімко зростає. Серед найбільш поширених видів шахрайства, можливо виділити, ті з якими найчастіше стикаються люди похилого віку:

Фішингові атаки – створення підроблених вебсайтів або електронних листів для отримання персональних даних, паролів та фінансової інформації;

Соціальна інженерія – методи маніпулювання з метою отримання конфіденційної інформації;

Фейкові державні виплати – розсилання неправдивих повідомлень про «грошову допомогу», пенсійні надбавки чи субсидії;

Шахрайські онлайн-інвестиції – залучення до фальшивих інвестиційних програм з обіцянкою високих доходів.

У подальшому люди похилого віку змушені звертатись до відповідних державних, в тому числі судових, органів за допомогою та захистом, проте процедура отримання відшкодування завданих збитків (переважно фінансових) є тривалою та не завжди позитивною.

Частими є випадки зняття коштів з кредитної карти, після отримання доступу до онлайн банкінгу, або створення онлайн кабінетів в фінансових установах чи укладення кредитних договорів онлайн, з метою виведення коштів.

Фінансові установи, що обліковують кредиторську заборгованість, яка виникла внаслідок шахрайських операцій, у подальшому подають позови про стягнення заборгованості. Такі позовні заяви обґрунтовані наявністю дій або бездіяльності зі сторони особи, що сприяли у доступі до конфіденційної інформації, за допомогою якої відбулись шахрайські операції. Також, є практика подання позовних заяв про визнання недійсними спірних кредитних договорів. В обох випадках лише наявність обставин, які безспірно доводять, що користувач своїми діями чи бездіяльністю сприяв втраті, незаконному використанню ПІН-коду або іншої інформації, яка дає змогу ініціювати платіжні операції, є підставою для притягнення його до цивільно-правової відповідальності.

Відповідно до Постанови Верховного Суду від 13.06.2022 по справі № 587/586/21, наведені правила визначають предмет дослідження та відповідним чином розподіляють між сторонами тягар доведення, а отже, встановленню підлягають обставини, які беззаперечно свідчитимуть, що користувач своїми діями чи бездіяльністю сприяв втраті, незаконному використанню ПІН-коду або іншої інформації, яка дає змогу ініціювати платіжні операції від його іме-

ні. У разі недоведеності обставин, які безспірно свідчать про те, що користувач своїми діями чи бездіяльністю сприяв втраті, незаконному використанню ПІН-коду або іншої інформації, яка дає змогу ініціювати платіжні операції, необхідно виходити з відсутності вини користувача у перерахуванні чи отриманні спірних грошових коштів. [5]

Вказане можливе лише після отримання відповідної конфіденційної інформації, яку люди похилого віку не рідко самі надають, не розуміючи можливих наслідків. Зокрема, проблема загострюється через:

- використання слабких або однакових паролів для різних сервісів;
- недостатню обізнаність про механізми налаштування конфіденційності в соціальних мережах;
- відсутність двофакторної автентифікації у фінансових та державних онлайн-сервісах.

Рішенням Правління Національного банку України від 12.04.2024 року затверджено Національну стратегію розвитку фінансової грамотності до 2030 року, якою зокрема, передбачено удосконалення навичок з управління особистими фінансами, забезпечення фінансової стійкості населення, захисту від фінансового шахрайства. Однією із цільових груп стратегії є люди похилого віку. [6]

У 2023 році Міністерством цифрової трансформації України презентовано освітній серіал на платформі Дія.Освіта «Базові цифрові навички для людей елегантного віку». Цей ресурс призначений для людей похилого віку, які не мають достатньої впевненості у використанні цифрових технологій, і допоможе їм освоїти навички користування смартфоном та електронними послугами в найбільш поширених життєвих ситуаціях.

Кібербезпека та цифрові права людей похилого віку, з огляду на їх чисельність, є важливим аспектом національної безпеки України. Для ефективного захисту необхідно якісно впровадити державні освітні програми з цифрової грамотності та посилити боротьбу з кіберзлочинністю. Лише комплексний підхід дозволить створити

безпечне цифрове середовище для людей похилого віку та забезпечити їхню соціальну інтеграцію в цифровий простір.

ЛІТЕРАТУРА:

1. Звіт про діяльність Департаменту кіберполіції Національної поліції України у 2024 році URL: <https://cyberpolice.gov.ua/news/zvitpro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u-roczi-7074/>

2. Державна служба статистики України URL: https://www.ukrstat.gov.ua/operativ/menu/menu_u/ds.htm

3. Аналітичний звіт «Думки і погляди населення України щодо державних електронних послуг». на замовлення Програми розвитку ООН в Україні й у партнерстві з Міністерством цифрової трансформації України. Київ – 2022 URL: <https://www.undp.org/sites/g/files/zskgke326/files/2023-01/Report%20Opinions%20and%20views%20of%20the%20Ukrainian%20population%20regarding%20state%20electronic%20services.pdf>

4. Аналітичний звіт «Думки і погляди населення України щодо державних електронних послуг». на замовлення Програми розвитку ООН в Україні й у партнерстві з Міністерством цифрової трансформації України. Київ – 2024 URL: <https://www.undp.org/sites/g/files/zskgke326/files/2024-01/infographic-e-services-use-in-ukraine-2023.pdf>

5. Постанова Верховного Суду у складі колегії суддів Першої судової палати Касаційного цивільного суду від 13.06.2022 по справі № 587/586/21 URL: <https://reyestr.court.gov.ua/Review/104794162>

6. Національна стратегія розвитку фінансової грамотності до 2030 року затверджена рішенням Правління Національного банку України від 12.04.2024 року № 119-пш. URL: https://bank.gov.ua/admin_uploads/article/NBU_Strategy-Financial-Literacy.pdf?v=12

7. Дія.Освіта «Базові цифрові навички для людей елегантного віку» URL: <https://osvita.diia.gov.ua/courses/basic-digital-skills-for-the-elegant-age>

Рябченко Вікторія Олександрівна,
*аспірантка 2 року навчання кафедри цивільного права
Національного університету «Одеська юридична академія».*

ПРОБЛЕМИ ЗАХИСТУ НЕПОВНОЛІТНІХ ВІД ВЕРБУВАННЯ ФСБ У СОЦМЕРЕЖІ «ТЕЛЕГРАМ»

XXI століття сьогодні ототожнюють з ерою комп'ютерів, інформаційною епохою чи епохою соціальних мереж. Безумовними перевагами соціальних мереж є швидкий доступ до наукової, роз-

важальної інформації, вільний доступ до новин, онлайн спілкування з друзями. Однак завжди за перевагами йдуть недоліки. Соціальні мережі, забезпечуючи миттєвий доступ до інформації, водночас створюють ризики маніпуляцій чи дезінформації з боку заінтересованих на це осіб.

За даними проведеного дослідження громадянською мережею «Опора» однією з популярніших соціальних мереж в Україні станом на 2024 рік є телеграм (ним користується 78,1% опитаних), друге і третє місце посідають ютуб (59,5%) та фейсбук (44,6%) відповідно [3]. Варто відзначити, що ще в 2023 році телеграму перевагу надавало 71,3% опитаних осіб, тобто за один рік кількість нових прихильників зросла на 6,8%. Телеграм-канали набирають популярності завдяки своїй анонімності, можливості безперешкодно створювати закриті групи, тим самим об'єднувати людей зі спільними інтересами і швидко поширювати контент будь-якого характеру.

Російсько-українська війна, інша назва якої, гібридна, неодноразово починаючи з 2014 року демонструвала на які дії може піти країна-агресор задля досягнення поставлених перед собою цілей. Для такої війни характерним є використання зі сторони-агресора різноманітних важелів впливу: політичних, економічних, військових, інформаційних чи навіть вдаватись до терористичних і підливних засобів, використовуючи для цього в тому числі соціальні мережі.

За даними Служби Безпеки України за 2024 рік було встановлено та затримано понад 450 осіб (тому числі і неповнолітні), які за дорученням так званих «кураторів» через закриті телеграм-канали за обіцяну грошову винагороду займались підпалами на території України [4].

Можна стверджувати, що неповнолітні особи з незміцнілою психікою є ідеальним об'єктом для вербування, адже є більш вразливими до різного роду маніпуляцій і тиску, що в свою чергу, є серйозним викликом і потребує уваги з боку суспільства і держави.

«Куратори» залучають молодь не тільки до підготовки терактів, а й до участі в них як виконавців. За офіційними повідомлен-

нями правоохоронних органів в період з лютого 2022 року по березень 2025 щонайменше 50 неповнолітніх брали участь у підпалах і підривах. За цей же період відбулись 42 підпали і підриви в адміністративних будівлях, ТЦК, 88 підпалів і підривів військових, військової техніки та правоохоронців [2]. Вербуванню піддаються особи, які відшукують легкий заробіток, повною мірою не обізнані про наслідки своїх дій і про настання юридичної відповідальності неповнолітніх.

В результаті постає питання яким чином і за допомогою яких превентивних заходів можна попередити вербування неповнолітніх. Восени 2024 року рішенням Національного координаційного центру кібербезпеки держслужбовцям і військовослужбовцям було заборонено використовувати телеграм в службових цілях, тож першочергово спадає на думку необхідність заборони соціальної мережі телеграм на території всієї України для всіх громадян без виключень. Однак, навіть ці дії не зможуть гарантувати необхідний результат, акцент має бути на вчасному інформуванні та вихованні молоді.

Міністерством освіти і науки України батькам стосовно їх дітей рекомендовано: спостерігати за поведінкою, навчати фінансової грамотності, привчати до цифрової безпеки та розпізнаванню маніпуляцій і найголовніше – мати з неповнолітнім відкрите спілкування та підтримувати довірливі стосунки [5].

Так, відповідно до ч. 2 ст. 150 Сімейного кодексу України батьки зобов'язані піклуватися про фізичний, духовний і моральний розвиток дитини [1]. Батьки мають не тільки створити безпечне середовище для розвитку своєї дитини, а й піддавати її контролю. Інакше кажучи, раціональний та свідомий батьківський контроль може стати запобіжником девіантної поведінки неповнолітнього. Саме для цього існує низка корисних сервісів для батьків, за допомогою яких можна наглядати за неповнолітнім, при цьому не порушуючи його особистих кордонів, таких як Google Family Link, Qustodio, Bark та інші.

Наступним превентивним заходом може бути співпраця Міністерства освіти і науки України зі Службою безпеки України чи з Національною поліцією України з метою інформування молоді, яка за своїм віком є найбільш вразливою до вербування. Зустрічі на базі шкіл в будь-якому форматі: онлайн чи офлайн з представниками влади підвищують рівень обізнаності неповнолітніх та зорієнтують в алгоритмі дій у разі виникнення сумнівних пропозицій.

Підсумовуючи вищевикладене, необхідно зазначити, що залучення через соціальні мережі країною-агресором неповнолітніх до протиправних діянь є серйозною проблемою, яка потребує негайного реагування з боку суспільства і держави. Для ефективного вирішення даної проблеми необхідна спільна робота батьків, навчальних закладів та влади з метою підвищення обізнаності неповнолітніх про ризики та наслідки їх дій.

ЛІТЕРАТУРА:

1. Сімейний кодекс України: Закон України від 10.01.2002 № 2947-III // Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2947-14#Text>
2. Гарасим А., Кельм Н., Романишин Н. Вимкніть телеграм. Він робить з українських дітей терористів (інфографіка). *Texty.org.ua*– *Тексти.org.ua*. URL: <https://texty.org.ua/articles/114801/vymknit-telehram-vin-robyt-z-ukrayinskyh-ditej-terorystiv-infohrafika/>
3. «Опора»: найпопулярнішими соцмережами в Україні є телеграм, ютуб та фейсбук. URL: <https://ms.detector.media/sotsmerezhi/post/35557/2024-07-16-opora-naupopulyarnishymy-sotsmerezhamy-v-ukraini-ie-telegram-yutub-ta-feysbuk/>
4. СБУ проводить інформкампанію «Спали» ФСБшника» для протидії вербуванню молоді спецслужбами РФ (відео). URL: <https://ssu.gov.ua/novyny/sbu-provodyt-informkampaniiu-spaly-fsbshnya-dlia-protydii-verbuvanniu-molodi-spetssluzhbyam-ru-video>
5. *Як розпізнати ознаки вербування дитини? Рекомендації батькам і освітянам*. URL: <https://mon.gov.ua/news/yak-rozpiznaty-oznaky-verbuvannia-dytyny-rekomendatsii-batkam-i-osvitanam>

Балик Даша Вікторівна,
студентка 2-го курсу факультету прокуратури та слідства (кримінальна юстиція) Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., доц., проф. кафедри цивільного права
Калітенко О.М.

ОСОБЛИВОСТІ ЗДІЙСНЕННЯ ПРАВА ВЛАСНОСТІ НА ЦИФРОВІ РЕЧІ

У ХХІ столітті цифрові технології стали невід’ємною частиною нашого повсякденного життя. Від традиційного обміну товарами та послугами ми перейшли до обігу цифрових активів, таких як криптовалюти, цифрові товари (музика, фільми, програмне забезпечення), а також віртуальні об’єкти у відеоіграх чи на онлайн-платформах. З’явилася нова форма права власності – право на цифрові речі. Це унікальне право потребує спеціального правового регулювання, оскільки цифрові активи не мають фізичної форми, і питання доступу, використання та захисту таких активів набувають особливого значення.

Актуальність теми полягає в тому, що сучасне цивільне законодавство не встигає за швидкими змінами в сфері цифрових технологій, що робить необхідним пошук ефективних способів правового регулювання прав на цифрові речі. У цьому контексті важливе значення має правильне розуміння того, що таке право власності на цифрові речі, яким чином здійснюється доступ до таких об’єктів і які юридичні механізми повинні забезпечувати захист прав власників.

У серпні 2023 року Президент підписав два важливі законопроекти, які вводять нові правила для цифрової сфери в Україні. Це законопроекти № 6447 та № 6576.

Перший з них (проект № 6447) вносить зміни до Цивільного кодексу України, доповнюючи перелік об’єктів цивільних прав новим видом – цифровими речами. Крім того, встановлюється положення, що об’єкти цивільних прав можуть існувати як у матеріальному світі, так і в цифровому середовищі, що визначає форму цих об’єктів, а також особливості їх набуття, здійснення та припинення цивільних прав і обов’язків щодо них.

Також до змісту Цивільного кодексу додається нова стаття 179–1, яка дає визначення цифрової речі: цифрова річ – це благо, яке створюється і існує виключно в цифровому середовищі і має майнову цінність [1].

Особливий інтерес викликає питання, як відрізнити цифрові блага, що мають майнову цінність, від тих, що її не мають, оскільки законодавство не дає точних уточнень. Для кращого розуміння можна звернути увагу на приклад електронних грошей, які мають цінність, оскільки є одиницею вартості. У випадку з цифровими речами, цифровий запис не матиме такої цінності, якщо за ним не стоїть право вимоги на інший об'єкт цивільного права, наприклад, гроші, цінні папери, майно або майнові права. Однак вартість деяких віртуальних активів, таких як криптовалюта (Bitcoin, Ethereum тощо), визначається переважно попитом і пропозицією на ринку та не залежить від наявності майна, яке умовно «забезпечує» її.

Другий законопроект № 6576 впроваджує комплексне регулювання через окремий Закон «Про цифровий контент та цифрові послуги» (далі – Закон). Цей Закон регулює взаємодію між виконавцем та споживачем при наданні цифрового контенту та/або цифрових послуг, а також поширюється на відносини, що стосуються розробки контенту згідно зі специфікацією споживача, надання цифрового контенту на матеріальних носіях для його зберігання, а також відносини, що передбачають передачу цифрового контенту та/або послуг разом з персональними даними споживачів [3].

Отже, з чинним законодавством, цифрові речі не є матеріальними об'єктами, що призводить до особливого підходу до їх правового регулювання. Оскільки цифрові речі не мають фізичного втілення, виникають питання щодо того, як вони підлягають обігу, передаванню прав власності та захисту.

Згідно з останніми змінами до Цивільного кодексу, всі цифрові речі як об'єкти цивільних прав поділяються на такі категорії:

1. Віртуальні активи;
2. Цифровий контент;
3. Інші блага, згідно з визначенням [1].

Детальніше розглянемо різницю між цими категоріями. Відповідно до Закону України «Про віртуальні активи» (який ще не набрав чинності), віртуальний актив – це нематеріальне благо, що є об’єктом цивільних прав, має певну вартість і існує у вигляді даних в електронній формі. Віртуальні активи поділяються на дві групи:

- Забезпечені віртуальні активи – це активи, які посвідчують майнові права, зокрема права вимоги на інші об’єкти цивільних прав;
- Незабезпечені віртуальні активи – активи, які не посвідчують жодних майнових чи немайнових прав. До цієї категорії належать NFT та криптовалюта, які є специфічними типами цифрових речей.

Натомість цифровий контент – це дані, що створюються та надаються в цифровому вигляді. До цього контенту належать, зокрема, комп’ютерні програми, мобільні застосунки, відео, аудіофайли, музика, цифрові ігри та електронні книги. Цифрова послуга, в свою чергу, передбачає можливість користувача створювати, обробляти, зберігати та поширювати дані у цифровій формі або отримувати доступ до таких даних. Окрім цього, користувач може виконувати інші дії з даними, які були створені чи завантажені ним або іншими користувачами.

Незважаючи на певну схожість, законодавець чітко розмежовує ці поняття. Особливістю цифрового контенту та послуг є встановлення спеціальних умов для їх надання, критеріїв відповідності та санкцій за порушення договірних зобов’язань.

Також варто звернути увагу на взаємозв’язок цифрового контенту з авторським правом. Відповідно до статті 10 Закону України «Про авторське право і суміжні права», авторське право та право власності на матеріальний чи цифровий об’єкт, в якому втілено твір, не залежать одне від одного [2]. Наприклад, якщо ви придбали електронну книгу, ви отримуєте доступ до файлу, але авторські права залишаються у автора чи видавця. Ви можете читати книгу або поділитися нею з іншими, але не маєте права на копіювання чи поширення її в мережі без дозволу правовласника. Такий підхід

стосується також програмного забезпечення, ігор та інших цифрових творів. Якщо продукт існує лише в цифровому вигляді, то можливість поширення його обмежена, а в разі банкрутства компанії або санкційні обмеження можуть призвести до втрати доступу до нього.

Особливим випадком є контент, що створюється самими споживачами. Наприклад, споживач може створювати власні цифрові твори за допомогою інструментів, наданих виконавцем послуги. У таких випадках споживач має право безкоштовно та безперешкодно отримати доступ до створеного контенту.

Право власності на цифрові речі можна охарактеризувати як сукупність прав, що дозволяють особі володіти, користуватися та розпоряджатися цифровими активами. Це право включає можливість здійснювати дії, що є притаманними для традиційного права власності: користування, володіння, розпорядження. Однак через специфіку цифрових активів, відмінних від фізичних об'єктів, правове регулювання права власності на них потребує нових підходів.

Важливою складовою права власності на цифрові речі є доступ до них, який здійснюється через механізми автентифікації та авторизації. Цей аспект є основою для забезпечення права на використання цифрових активів і їх управління.

- Автентифікація – це процес підтвердження особи, яка має доступ до цифрового ресурсу. Вона може здійснюватися через введення логіну, паролю, використання біометричних даних або інших форм ідентифікації. Автентифікація є першим кроком у забезпеченні доступу до цифрової речі, підтверджуючи, що користувач є тим, ким він себе видає.

- Авторизація – це наступний етап, який визначає, які конкретно дії має право здійснювати користувач після успішної автентифікації. Наприклад, авторизація може визначати, чи має особа право змінювати налаштування акаунту, чи може вона передавати доступ до цифрової речі іншій особі, чи має право здійснювати операції з цифровими активами. Ці механізми є важливими для забезпечення прав власності на цифрові речі, адже вони дозволяють

не лише підтвердити особу, але й регулювати її можливості щодо управління активами.

Абсолютне право на цифрову річ є концепцією, що визначає належність цифрового активу особі, яка має право доступу до нього. Це право відрізняється від традиційного права власності тим, що воно часто не прив'язане до фізичної форми активу, а визначається через право доступу та управління.

Наприклад, у випадку криптовалют, власник активу має доступ до свого криптовалютного гаманця через автентифікацію, що підтверджує його право на цей актив. Це право доступу є основою для визначення власності на цифрову річ, що дозволяє особі здійснювати будь-які правомірні дії з активом.

З точки зору цивільного права, абсолютне право на цифрові речі може бути реалізоване через визнання цифрових активів об'єктами права власності, а не просто правами доступу до них. Це дозволяє надійно захистити інтереси власників цифрових активів та забезпечити можливість обороту таких активів у правовій площині.

Однією з особливостей цифрових речей є необхідність моніторингу їхнього стану. Це важливо не тільки для криптовалют, але й для інших цифрових активів, таких як акаунти в іграх чи цифрові бібліотеки (музика, фільми, електронні книги). Власники цифрових речей повинні мати можливість перевіряти кількість активів, їх стан або доступність через відповідні інтерфейси.

Наприклад, у разі криптовалют власник може перевірити баланс свого гаманця, перевести кошти на інший рахунок або здійснити інші операції. Для ігрових акаунтів власник має можливість перевірити наявність віртуальних товарів чи досягнень, а також змінити параметри акаунту.

Перевірка стану цифрових активів є важливою складовою здійснення права власності, оскільки вона дозволяє власнику контролювати свої активи та бути впевненим у їхній наявності та безпеці.

Передача прав на цифрові речі є ще одним важливим аспектом, що потребує регулювання. Цей процес може здійснюватися

через зміну доступу до цифрових активів, наприклад, шляхом передачі логіну та паролю іншим особам. Однак це питання не є простим, оскільки передача цифрових активів часто пов'язана з обмеженнями, що встановлюються виробниками або постачальниками цих активів.

Право власності на цифрові речі є важливою частиною сучасного цивільного права, що потребує спеціального регулювання та адаптації існуючих норм до цифрових технологій. Його особливістю є нематеріальна природа об'єктів, відсутність єдиного підходу до їх правового статусу, а також складність у встановленні і реалізації правомочностей власника. Процес доступу, авторизації, перевірки стану та передачі цифрових активів має бути чітко врегульований для забезпечення прав власників.

ЛІТЕРАТУРА:

1. Цивільний кодекс України: Закон України від 16.01.2003 р. № 435-IV: URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>
2. Про авторське право і суміжні права: Закон України від 01.12.2022 р. № 2811-IX: URL: <https://zakon.rada.gov.ua/laws/show/3792-12#Text>
3. Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 р. № 3321-IX URL: <https://zakon.rada.gov.ua/laws/show/3321-20#Text>

Білошкурський Микола Миколайович,
студент 2-го курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., доц., доц. кафедри цивільного права
Завальнюк С. В.

ЦИВІЛЬНО-ПРАВОВИЙ СТАТУС ІГРОВОЇ ОНЛАЙН-РЕЧІ НА ПРИКЛАДІ СЕРВІСУ STEAM

Онлайн-відеоігри почали з'являтися у кінці минулого століття та, фактично, планомірно розвивалися поряд із розвитком ІТ-технологій. Так, у різних джерелах можна знайти інформацію про те, що перша онлайн-відеогра з'явилася ще у далекому 1970-му році. Хоча за іншою версією свій основний розквіт такі ігри отримали у 1988-му, з появою перших домашніх комп'ютерів [5]. У будь-яко-

му випадку, нині онлайн-відеоігри посідають особливе місце та мають численну кількість користувачів. Так, за підрахунками Фабіо Дуарте, кількість гравців в онлайн-відеоіграх з 2015 по 2024 рік збільшилася з 2,03 мільярдів до 3,32 мільярдів, а ринок всіх відеоігор може оцінюватись у 282 млн дол. США [11].

Щоправда, науковий інтерес до онлайн-відеоігор, особливо в Україні, виник відносно нещодавно, перш за все, він був пов'язаний з розвитком кіберспорту як спортивної дисципліни. Так, Є. Харитонов та Ю. Толмачевська у межах дослідження кіберспорту як сфери цивільно-правових відносин доходять висновку, що його варто розглядати саме «як сферу приватноправового регулювання, яка має свій предмет, передусім майнові відносини, що складаються у зв'язку зі здійсненням кіберспортивної діяльності» [9, с. 74]. М. Ткалич, аналізуючи спортивні клуби як учасників цивільних правовідносин, стверджує, що завдяки комерціалізації спортивної діяльності та зміни у всій українській системі організації спорту було зумовлене домінування приватно-правових форм забезпечення діяльності вітчизняного спорту та його розвитку [7, с. 1]. Подекуди також з'являються дослідження, пов'язані з регулюванням окремих видів відносин у кіберспорті шляхом учинення правочинів. Наприклад, Ю. Толмачевська аналізує цивільно-правові договори, які, як зазначає дослідниця, хоч і є ексклюзивними, мало чим відрізняються від інших договорів у класичному спорті [8, с. 33].

Проте, незважаючи на кількість досліджень, пов'язаних з онлайн-відеоіграми, особливо у контексті кіберспорту, досі не до кінця визначеним є статус ігрових речей у онлайн-відеоіграх. Переважна більшість наявних досліджень на тему цифрових активів не акцентують увагу на статусі речей в онлайн-відеоіграх, а оперують більш узагальненою термінологією. Так, В. Ващак досліджує концепцію віртуальної власності у розумінні оновлення цивільного законодавства та наголошує на необхідності законодавчого врегулювання та визнання віртуальних активів як об'єкта цивільних правовідносин, що на думку автора сприятиме також розвитку ІТ-сфери в Україні [1, с. 47]. К. Некіт теж наголошує на необхідно-

сті законодавчого поширення правового режиму власності ще й на віртуальні активи, а також підкреслює важливість розмежовувати поняття «віртуальна власність» та «право інтелектуальної власності» [4, с. 41–42]. С. Завальнюк під час дослідження прогалин, як характерної ознаки цивільного законодавства, також зазначає, що вплив науково-технічного та суспільного прогресу накладає свій відбиток на будь-які приватноправові відносини [3, с. 13]. Тому такий науково-технічний прогрес суспільства, як поява «цифрових активів» зумовлює виникнення деяких прогалин у цивільному законодавстві, а, відповідно, актуалізується проблема необхідності вдосконалення чинного законодавства, як на цьому і наголошують згадані вище автори.

Навіть побіжний аналіз наявних досліджень дає зрозуміти, що незважаючи на широкий інтерес до кіберспорту та віртуальних активів, онлайн-відеоігри не є на стільки ж частими об'єктами дослідження, так само, як і речі у цих онлайн-відеоіграх. Саме тому вважаємо за доцільне дослідити статус речі в онлайн-відеоіграх та відповісти на важливі запитання: чи доцільно відносити річ в онлайн-відеоігрі до поняття «цифровий актив»?; чи можна взагалі розглядати річ в онлайн-відеоігрі як власність гравця, навіть за умови, що він витратив на неї реальні кошти (у контексті окремого ігрового сервісу)?

Відповідаючи на перше запитання, розглянемо нормативно-правову базу. Так, поняття «віртуальні активи» (що у нашому розумінні є тим же, що і «цифрові активи») повинні були бути закріплені у ст. 1 Закону України «Про віртуальні активи», проте він так і не набрав чинності [6]. Серед нині чинного законодавства «цифрові активи» частково регулюються положенням ст. 177 Цивільного Кодексу України (Надалі – ЦК України). Відповідно до ч. 2 ст. 177 ЦК України: «Об'єкти цивільних прав можуть існувати у матеріальному світі та/або цифровому середовищі...» [10]. Тобто, «цифровий актив» може бути об'єктом цивільних прав, а, виходячи з цього, і об'єктом власності. Проте, досі не визначеним є те, чи доцільно відносити речі в онлайн-відеоіграх до категорії «цифрових активів».

Для того, щоб відповісти на це запитання, слід дослідити який статус мають такі речі. Пропонуємо розглянути це на прикладі ігрового сервісу Steam, через який реалізована не тільки купівля онлайн-відеоігор, а і купівля вже згаданих речей у цих онлайн-відеоігор. Steam є онлайн-сервісом від компанії Valve, який пропонує всім охочим з 13 років зареєструватися підписниками, попередньо уклавши угоду встановленого зразка, якою декларуються права та обов'язки підписників [13]. Після реєстрації підписник матиме доступ як до безкоштовних ігор, наприклад, Counter-Strike 2 [14] чи Dota 2 [15], так і платних. Слід зазначити, що у безкоштовних іграх також передбачені деякі платні послуги, зокрема зовнішній вигляд ігрових персонажів, ігрової зброї тощо [2, с. 13].

Будь-який підписник має змогу поповнювати свій гаманець Steam і витрачати кошти на платний контент. Згідно з угодою підписника, зокрема пункту 3 підпункту А, під час поповнення власного цифрового гаманця Steam, підписник гарантує законність власності на карту, ПІН-код, ключ або обліковий запис, пов'язані з цим платежем, й уповноважує Valve списати кошти зі своєї кредитної (дебетової) картки чи обробити платіж стороннім платіжним оператором для оплати, передплати, поповнення цифрового гаманця Steam, придбання віртуального товару чи фінансування інших витрат [13]. У аналізованому онлайн-сервісі також присутній торговельний майданчик. Підписники сервісу можуть виставляти на цьому майданчику свої ігрові предмети, при цьому користувачі можуть витрачати гроші зі свого цифрового гаманця Steam для купівлі у іншого користувача будь-якого віртуального предмету для онлайн-відеоігор на торговельному майданчику Steam.

Після зняття обумовленої суми з гаманця Steam, до якої входять вартість цифрового предмету, комісія онлайн-сервісу Steam та обсяг податку, предмет опиняється в інвентарі покупця-користувача. Власне, підписник безпосередньо не купує цифровий предмет або право на володіння ним, а обмінює або купує виключно підписку на право користуватись таким предметом, що зазначається у пункті 3 підпункту D угоди підписника, з положеннями

якої під час реєстрації погоджується кожен майбутній користувач сервісу Steam [11].

Підписник, у ході придбання ігрового предмету в когось з підписників, може використовувати, але не має можливості продавати його на торговельному майданчику чи обмінюватися з іншими користувачами сервісу впродовж наступних 14 днів. Якщо з моменту купівлі-обміну ігрового предмета минає 14 днів, користувач Steam отримує можливість продавати його на торговельному майданчику чи здійснювати обмін з іншими підписниками. Щодо продажу ігрового предмету й одержання реальних коштів – згідно з нормами поведінки у ігровому сервісі Steam, на які погоджується кожен підписник автоматично, заборонено займатися комерційною діяльністю, а, отже, й обмінювати ігрові предмети на реальні гроші. При цьому для купівлі-продажу дозволено користуватися виключно внутрішньою ігровою валютою в гаманці Steam, або ж здійснювати бартер між предметами [15].

Тобто, можемо говорити про те, що усі ігрові речі в будь якій онлайн-відеогрі, придбані на ігровому сервісі Steam, є власністю виключно цього ігрового сервісу, а, відповідно, очевидно є відповідь на друге запитання: чи можна взагалі розглядати річ в онлайн-відеогрі як власність гравця, навіть за умови, що він витратив на неї реальні кошти (у контексті окремого ігрового сервісу)? На основі проведеного дослідження можна дійти висновку, що речі в онлайн-відеоіграх, куплені гравцем за реальні кошти, судячи з положень та угод між користувачем-підписником та сервісом Steam, не є власністю гравця.

Проте, вважати правовідносини, які складаються між гравцем-підписником та онлайн-сервісом Steam зобов'язальними теж недоречно. Якщо аналізувати цю юридичну ситуацію через призму зобов'язального права – підписки на право користування, куплена гравцем за реальні кошти може розглядатися як «договір оренди», проте за пунктом 3 підпункту D угоди підписника [11], сервіс Steam може без врахування позиції власника скасувати йому таку підписку як на користування окремою річчю в онлайн-

відеоігри, так і взагалі позбавити його можливості користуватись ігровим сервісом Steam. Більше того, якби подібні правовідносини були зобов'язальними та розумілись як такі, що з'являються унаслідок укладання між підписником та сервісом Steam договору оренди, то підписник не міг би продати таку підписку, лише здати в суборенду, а отже, при «обміні» або «продажі» підписки іншому користувачу сервісу його користування річчю в онлайн-відеоігри повинно було б здійснюватися на умовах суборенди, проте це не є так, адже особа, яка передала йому підписку на ігрову річ втрачає будь-які права на неї. Відповідно, вважати договором оренди чи суборенди подібну купівлю підписки на користування річчю в онлайн-відеоігри не зовсім доречно.

Разом з тим, користувачі сервісу Steam можуть безперешкодно обмінюватися між собою такими підписками, продавати їх на торговельному майданчику сервісу, кошти ж, отримані за ці продажі, зараховуються на їх онлайн-гаманець Steam і, хоча не можуть виводитись у реальний світ, все одно можуть слугувати гравцю для купівлі інших речей або платних ігор у ігровому сервісі Steam. Крім того, існують випадки викрадення підписок на користування речами в онлайн-відеоіграх через ведення їх власника в оману, або шляхом недобросовісного отримання доступу до аккаунту окремого користувача на сервісі Steam. Таким чином, якщо подібну підписку на користування річчю в онлайн-відеоігри можна продати, обміняти, або навіть вкрати, її доцільно відносити до «цифрових активів».

Отже, підсумовуючи, можемо зробити висновок про те, що речі в онлайн-відеоіграх, якщо розглядати їх через сервіс Steam, доцільно відносити до «цифрових активів», керуючись як ч. 2 ст. 177 ЦК України [10], так і тим фактом, що такі речі в онлайн-відеоіграх можна купити, продати, обміняти та навіть вкрати. Проте, важливо зазначити, що називати їх «речами» некоректно, адже користувач сервісу купує не саму річ в онлайн-відеоігри, а лише підписку на право користуватися такою річчю, при чому, відповідно до пункту 3 підпункту D угоди підписника [11], яку обов'язково укладає кожен користувач, сервіс Steam без врахування думки та згоди чи

заперечень користувача, може позбавити останнього можливості користуватись як підпискою на право користування окремою річчю, так і підпискою користуватися сервісом Steam в цілому. Також, на нашу думку, розглядати такі правовідносини як зобов'язальні також не зовсім правильно. Безперечно, порушена проблематика потребує подальших наукових розвідок та стане темою наших наступних досліджень.

ЛІТЕРАТУРА:

1. Ващак В. А. Концепція віртуальної власності в рамках оновлення Цивільного кодексу України. *Офіційна концепція оновлення Цивільного кодексу України: проблеми практичної реалізації*: матеріали Всеукр. круглого столу (м. Одеса, 25 лютого 2021р.) / за заг. ред. Є. О. Харитонов, О. І. Харитонові. Одеса: Фенікс, 2021. С. 45–47.
2. Давидова І. В., Білошкурський М. М. Використання платних послуг у онлайн-відеоіграх як спосіб приховати корупційні злочини. *Lex Sportiva*. 2023. № 2. С. 10–17.
3. Завальнюк С. В. Прогаляністість як характерна ознака цивільного законодавства. *Прикарпатський юридичний вісник*. 2020. С. 3(32). С. 12–15.
4. Некіт К. Г. Віртуальна власність: поняття та сутність. *Право і суспільство*. 2019. № 2. С. 37–42.
5. Орещенко А. В. Історія розвитку комп'ютерних ігор: значення для картографії. *Часопис картографії*. 2012. № 4. С. 154–179.
6. Про віртуальні активи: Закон України від 17.02.2022 р. № 2074-IX (не набрав чинності). URL: <https://zakon.rada.gov.ua/laws/show/2074-20#Text>
7. Ткалич М. О. Лінгвальні засоби авторизації в сучасному англomовному журнальному дискурсі: когнітивно-риторичний аспект: автореф. дис. ... канд. юрид. наук: 12.00.03. Одеса, 2010. 20 с.
8. Толмачевська Ю. О. Цивільно-правові договори у кіберспорті: правовий аналіз. *Lex Sportiva*. 2023. № 1. С. 28–34. DOI: <https://doi.org/10.32782/lexsportiva/2023.1.6>
9. Харитонов Є. О., Толмачевська Ю. О. Кіберспорт як сфера цивільно-правового регулювання. *Часопис цивілістики*. 2019. Вип. 32. С. 72–75. URL: <http://clj.nuoua.od.ua/archive/32/15.pdf>
10. Цивільний кодекс України: Закон України від 16.01.2003 р. № 435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>
11. Duarte F. How Many Gamers Are There? (New 2024 Statistics). *Exploding Topics*. February 23, 2025. URL: <https://explodingtopics.com/blog/number-of-gamers>

12. Steam Online Conduct. Steam. URL: https://store.steampowered.com/online_conduct
13. Steam Subscriber Agreement. *Steam*. 2025. URL: https://store.steampowered.com/subscriber_agreement/english/
14. Steam. Counter-Strike 2. 2025. URL: https://store.steampowered.com/app/730/CounterStrike_2/
15. Steam. Dota 2. 2025. URL: https://store.steampowered.com/app/570/Dota_2/

Забудько Анастасія Сергіївна,

студентка 2-го курсу факультету цивільної та господарської юстиції

Національного університету «Одеська юридична академія»

Науковий керівник: к.ю.н., доц., доц. кафедри цивільного права

Завальнюк С. В.

ОСОБЛИВОСТІ СПАДКУВАННЯ ЦИФРОВИХ АКТИВІВ

Цифровий актив визначається як будь-яка форма активу, що існує у цифровій чи електронній формі, незалежно від його природи та призначення. Це може включати криптовалюти, токени, цифрові права на власність, електронні гроші, файли, дані та інші об'єкти. Однак, як зазначають дослідники, цифрові активи можуть мати різні технічні та правові характеристики. Вони охоплюють ресурси, які мають вартість або власника (або обидва ці параметри) в цифровому середовищі. До таких активів відносяться криптовалюти, смарт-контракти, право власності на інтелектуальну власність та інші цифрові об'єкти [3].

Для чіткого визначення категорії цифрових об'єктів С. С. Аліна пропонує класифікувати їх за такими критеріями: функціональний, майновий, аксіологічний, об'єктиваційний та юридичний. За функціональним критерієм виділяються текстові, графічні та аудіовізуальні контенти, програмні компоненти, інструменти індивідуалізації в соціальних мережах, віртуальні гроші та цінні папери, а також об'єкти віртуальних ігор. У рамках критерію «майновості» цифрові об'єкти поділяються на майнові (які можна оцінити в грошах) та немайнові (які не мають грошової оцінки, такі як особисті немайнові блага, інформація або результати інтелектуальної

діяльності). Майновими цифровими активами можуть бути криптовалюти, токени, цифрові гроші та інші форми цифрового майна. Немайнові об'єкти включають персональні цифрові архіви, історії в месенджерах, інтернет-репутацію тощо [1].

З розвитком цифрових технологій, інтернет-платформ та криптовалют у сучасному світі виникають нові питання правового регулювання, зокрема, у сфері спадкування. Цифрові активи, які включають криптовалюти, електронні гаманці, інтелектуальну власність, акаунти в соціальних мережах та інші форми цифрових цінностей, стають важливим аспектом спадкових справ. Оскільки законодавство багатьох країн не встигає за технологічними змінами, виникає потреба в удосконаленні правових норм щодо спадкування таких активів.

В Україні поки що відсутнє спеціалізоване законодавство, яке б детально регулювало спадкові права на цифрові активи. Водночас загальні норми спадкового права, передбачені Цивільним кодексом, можуть бути застосовані і до цифрових активів. Згідно з цими нормами, спадкоємці мають право на спадщину, яка включає всі види майна, зокрема й цифрові активи. Для успішного наслідування таких активів важливо мати належні документи та докази, що підтверджують право власності померлого на цифрові активи. Це можуть бути доступи до криптогаманців, паролі та приватні ключі. Крім того, слід враховувати питання оподаткування: при отриманні цифрових активів у спадок може виникнути зобов'язання щодо сплати податків. Важливо слідувати податковим вимогам і забезпечити правильний облік активів.

Наслідування цифрових активів може супроводжуватися різними труднощами, зумовленими специфікою цих активів. Однією з головних проблем є відсутність доступу до гаманців з різними цифровими активами та акаунтів померлого, що може статися через втрату паролів, приватних ключів або технічні обмеження. Ще однією складністю є правова невизначеність, адже у деяких юрисдикціях статус активів у спадкових справах досі не врегульований, що може призвести до судових суперечок. Також слід враховувати

питання безпеки активів, оскільки цифрові активи можуть стати мішенню для хакерських атак, фішингу та інших загроз. Недостатній рівень захисту або неправильно організоване зберігання ключів може призвести до їхньої втрати.

Наслідкування цифрових активів є складним процесом, який вимагає дотримання певних кроків та застосування сучасних технологій. Важливо правильно організувати цей процес, щоб забезпечити законність і безпеку передачі цифрових активів спадкоємцям. Спочатку необхідно визначити сукупність активів, що підлягають спадкуванню. Це означає, що слід з'ясувати, які саме цифрові об'єкти можуть бути включені до спадщини. Серед них можуть бути файли на комп'ютерах, електронні документи, фотографії, відеозаписи, акаунти в соціальних мережах, електронна пошта, а також віртуальні активи, наприклад криптовалюта. Хоча цей перелік може бути розширеним, він повинен охоплювати основні категорії цифрових активів.

Наступним етапом є аналіз чинного законодавства щодо правового регулювання в країні, де проживає спадкодавець. На сьогодні в деяких країнах існують закони, що регулюють питання цифрового спадкування. У цьому контексті спадкодавець повинен бути обізнаний із межами національного законодавства, що стосується спадщини.

Третій етап передбачає визначення волі спадкодавця. Особа, яка залишає спадщину, повинна чітко вказати, як повинні бути розпоряджені її цифрові активи після смерті. Це включає інформацію про спадкоємців, рекомендації щодо використання або зберігання цифрових активів, необхідні паролі та інші способи захисту об'єктів цифрової спадщини.

Останнім етапом у процесі оформлення цифрової спадщини є вибір спеціалізованих сервісів, які допомагають управляти цим питанням. Наразі деякі компанії та платформи пропонують відповідні послуги. Наприклад, Apple, запровадила механізми цифрового спадкування для власників своїх пристроїв. Зокрема, користувачі можуть призначити довірену особу, яка після їхньої смерті отримає

доступ до облікових записів, або налаштувати автоматичне видалення певних даних у разі їхньої раптової смерті [4].

О. О. Дмитрик ретельно досліджує питання спадкування цифрових активів і наголошує, що їх слід розглядати як окрему категорію цифрових об'єктів, які мають певну цінність, зберігаються у цифровій формі та можуть бути об'єктом обміну. Основними характеристиками таких активів є їхній електронний формат, що означає відсутність фізичної матеріальності та збереження на цифрових пристроях. Вони функціонують на основі сучасної технології блокчейн, яка забезпечує їхню децентралізацію, виключаючи необхідність централізованого контролю та посередників. Також цифрові активи мають криптографічний захист, оскільки кожен з них має унікальний ключ доступу. Вони вирізняються анонімністю та відносною безпекою, адже власники можуть здійснювати транзакції без розкриття особистих даних. Ще однією важливою особливістю є те, що їхній обіг не вимагає залучення посередників чи фінансових установ. Крім того, цифрові активи використовуються для різних цілей: інвестування, збереження вартості, проведення фінансових операцій, а також створення цифрових колекцій мистецтва та ігор. До цієї категорії належать криптовалюти, такі як Bitcoin і Ethereum, токени, NFT, цифрові цінності, смарт-контракти та інші цифрові ресурси. Водночас існують віртуальні активи, які також існують у цифровому форматі, проте зазвичай не мають безпосередньої фінансової цінності у реальному світі. Головна відмінність між цими двома видами активів полягає в тому, що цифрові активи можна обміняти на грошові кошти або інші матеріальні ресурси, тоді як віртуальні активи існують виключно у межах певного цифрового середовища й можуть обмінюватися лише в його рамках. [2, с. 250].

Отже, питання спадкування цифрових активів є надзвичайно актуальним у сучасному світі, де цифрові цінності набувають все більшої ваги. Але питання спадкування активів в свою чергу є досить проблемним, оскільки більшість країн не мають достатнього правового забезпечення цієї сфери, тому спадкоємцю важливо мати

документальне підтвердження наявності та власності цифрових активів. Врахування специфіки цифрових активів, як особливого виду майна, є ключовим моментом у забезпеченні справедливого та ефективного спадкоємства для власників таких активів.

ЛІТЕРАТУРА:

1. Аліна С.С. Спадкування ІТ-об'єктів за сучасним цивільним законодавством: дис. ... д-ра філософії: 081 –Право / Національний університет «Одеська юридична академія», Одеса, 2020. 204 с.
2. Дмитрик О.О. Віртуальні активи і цифрові активи: до питання про співвідношення понять. Право та інноваційне суспільство. № 2 (17). 2021. С. 248-254. URL: <https://apir.org.ua/index.php/lais/article/view/403/353>
3. Загоруй Л. М., Загоруй І. С. Цифрова спадщина: проблеми формування і перспективи. Актуальні проблеми права: теорія і практика. 2024. №1 (47). С. 71–82.
4. Калітенко О. Саморегулювання в сфері цифрового спадкування: окремі аспекти. Юридичний вісник. 2023. 4. С. 38–43.

Костенко Олександр Сергійович,

*студент 2-го курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., доц., доц. кафедри цивільного права
Завальнюк С.В.*

АВТОРСЬКІ ПРАВА НА ОБ'ЄКТИ, СТВОРЕНІ ШТУЧНИМ ІНТЕЛЕКТОМ: ПРАВОВІ АСПЕКТИ РЕГУЛЮВАННЯ

З моменту популяризації технологій штучного інтелекту (надалі – ШІ) у повсякденному житті дедалі частіше виникають дискусії щодо правового статусу контенту, створеного алгоритмами, а також питання відповідальності та правомірності використання таких творів. Новації, що несе ШІ під час створення зображень, творів, програмного забезпечення ставлять під сумнів традиційні концепції авторського права та права інтелектуальної власності.

Звертаючись до чинного законодавства, авторами вважаються фізичні особи, які власною творчою працею створили твір [4]. У випадку об'єктів авторського права, згенерованих за допомогою ШІ, відсутній традиційний автор, що ставить під сумнів правомірність їх охорони авторським правом. Варто погодитись з думкою Васи-

ля Крата, що застосування ст. 33 Закону України «Про авторське право і суміжні права» має враховувати положення Цивільного кодексу України [2]. Автором було зазначено, що об'єкти, згенеровані комп'ютерною програмою, не відповідають традиційним принципам авторського права через відсутність фізичного автора. Відповідно законодавець вводить правовий режим прав особливого роду (*suī generis*), який визначає його як «квазіавторське право». Тобто правовий режим прав особливого роду на неоригінальні об'єкти, згенеровані комп'ютерною програмою, є тільки схожим на авторське право, але не є ним за своєю сутністю.

У зв'язку з цим виникає питання про правовий статус об'єктів, створених штучним інтелектом. Якщо розглядати ШІ як інструмент у творчій діяльності людини, то постає питання про те, чи може така особа в повній мірі вважатися автором відповідного твору. Наразі на міжнародному правовому полі не має спільного підходу до вирішення цього питання, проте варто виокремити підходи США та ЄС.

Так, у США діє практика ототожнення авторства з людиною, що підтверджується Керівними принципами Бюро авторського права США. Згідно з цими принципами, Бюро реєструватиме оригінальні твори лише за умови, що їхнім автором є людина. Підґрунтям до вироблення цієї позиції пов'язується з судовим рішенням у справі «Naruto v. Slater», яке детально було розглянуто у межах дослідження К. Міліциної [3, с. 344]. У цій судовій справі організація PETA підтримала мавпу, виступаючи як представник недієздатної особи (так званий *next friend*). Суд дійшов висновку, що авторство може належати лише людині, а тварини не мають авторських прав відповідно до законодавства США. Ба більше, суд постановив, що тварини не можуть виступати в суді, отже, PETA не має права діяти від їхнього імені [7]. Ці висновки вважаються впливовими, оскільки вони стосуються не лише авторських прав тварин, але й підходу США до творів, створених штучним інтелектом або за його участі. Відповідно до Керівних принципів Бюро авторського права США, реєстрація творів, створених виключно

машиною чи внаслідок механічного процесу без творчого внеску людини, неможлива. Хоча ці принципи не є нормативно-правовим актом, на практиці вони визначають підхід Бюро до питань охороноздатності творів і використовуються судами як аргумент у відповідних справах [5].

Звертаючись до базису законодавства Європейського Союзу, варто виокремити підходи, що закріплені у наступних нормативно – правових актах: Директива Європейського Парламенту і Ради (ЄС) 2019/790 від 17 квітня 2019 року та Акт про штучний інтелект. Директива Європейського Парламенту і Ради (ЄС) 2019/790 чітко вказує, що правова охорона авторських прав надається лише для творів, створених людьми. Твори, які були створені штучним інтелектом без значного втручання людини, не можуть розраховувати на правовий захист. Проте, цей нормативно – правовий акт також визнає важливість технологій у творчому процесі, зокрема в контексті автоматизованого аналізу тексту та даних (text and data mining), що дозволяє використовувати авторські матеріали для навчання штучного інтелекту за певних умов [1]. Акт про штучний інтелект (англійською – EU AI Act) – це перший у світі комплексний нормативний документ, який встановлює чіткі вимоги до прозорості та відповідальності розробників систем штучного інтелекту. Він закріплює, що штучний інтелект не може претендувати на авторські права, а матеріали, створені за його допомогою, повинні бути чітко позначені як такі, що мають штучне походження. Це допомагає знайти баланс між захистом прав людини, стимулюванням інновацій та розвитком цифрового ринку. Таким чином прийняття та впровадження Акта про ШІ, зокрема Україною, є надзвичайно важливим для розвитку правового регулювання штучного інтелекту, особливо в сфері авторського права [6].

Підсумовуючи результати вищесказаного, законодавство України у сфері авторського права потребує модернізації для врахування викликів, пов'язаних із застосуванням штучного інтелекту. Серед важливих напрямків змін варто виділити запровадження особливого правового режиму для об'єктів, створених штучним

інтелектом, чітке визначення статусу таких творів, а також розмежування контенту, створеного виключно алгоритмами, і продуктів, які були створені в співпраці з людьми. Важливо також запровадити механізми прозорості та відповідальності для розробників, включаючи маркування контенту, а також забезпечити дотримання етичних принципів у використанні ШІ. До того ж гармонізація національного законодавства з міжнародними стандартами допоможе захистити права творців, стимулювати інновації та інтегрувати Україну в глобальне цифрове середовище.

ЛІТЕРАТУРА:

1. Директива Європейського Парламенту і Ради (ЄС) 2019/790 від 17 квітня 2019 року про авторське право і суміжні права на Єдиному цифровому ринку та про внесення змін до директив 96/9/ЄС та 2001/29/ЄС. URL: [https://zakon.rada.gov.ua/laws/show/984_022-19#Text](https://zakon.rada.gov.ua/laws/show/984_022-19#Text)
2. Крат В. Чи буде штучний інтелект керувати «авторським» світом: міркування судді щодо природи правового регулювання ШІ. ВЕРХОВНИЙ СУД. URL: <https://supreme.court.gov.ua/supreme/pres-centr/news/1600363/>
3. Міліцина К. Об'єкти, створені з використанням штучного інтелекту та безпосередньо штучний інтелект, і авторське право США. Підприємництво, господарство і право. 2019. Т. 5. С. 343–346. URL: <https://doi.org/10.32849/2663-5313/2019.5.64>
4. Про авторське право і суміжні права: Закон України від 01.12.2022 № 2811-IX: станом на 15 листоп. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/2811-20#Text>
5. Compendium of U. S. Copyright Office Practices. Third Edition. United States Copyright Office. 2017. Chapter 300, P. 4. URL: <https://www.copyright.gov/comp3/docs/compendium.pdf>
6. EU Artificial Intelligence Act. EU Artificial Intelligence Act. URL: <https://artificialintelligenceact.eu/ai-act-explorer/>
7. Naruto v. Slater, No. 16–15469 (9th Cir. 2018). United States Court of Appeals for the Ninth Circuit. 2018. URL: <http://cdn.ca9.uscourts.gov/datastore/opinions/2018/04/23/16-15469.pdf>

Мурашева Катерина Василівна,
*студентка 2-го курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія»
Науковий керівник: к.ю.н., доц., доц. кафедри цивільного права
Завальнюк С. В.*

ПЕРСОНАЛЬНІ ДАНІ ТА ЇХ ЗАХИСТ: ЦИВІЛЬНО-ПРАВОВІ АСПЕКТИ В УМОВАХ КІБЕРЗАГРОЗ

Розвиток інформаційних технологій в сучасному суспільстві приносить багато користі різним сферам життя, але і ускладнює життя новими викликами. Тема кіберзагроз, після кібератаки на державні реєстри України – хакерські атаки на сайти Національних інформаційних систем та Міністерства юстиції України, актуальна як ніколи. Актуальними є також проблеми правового регулювання персональних даних у цивільно-правовому вимірі в умовах кіберзагроз, а саме: збільшення масштабів кібератак – безперервне вдосконалення методів атак та недосконалість систем безпеки становлять загрозу конфіденційності персональних даних; труднощі з ідентифікацією відповідальності – складність визначення відповідального за витік чи неправомірне використання даних у випадку кібератак або неналежного захисту інформації; недостатня дієвість механізмів захисту прав суб'єктів персональних даних – ускладнена процедура подання скарг і притягнення до відповідальності порушників; юридична відповідальність за порушення – неефективність санкцій та відсутність дієвих механізмів притягнення до відповідальності за незаконну обробку персональних даних.

Визначення персональних даних згідно з національним та міжнародним законодавством можна трактувати так:

Персональні дані – це будь-яка інформація, що стосується ідентифікованої або такої, що може бути ідентифікована, фізичної особи (суб'єкта персональних даних). Вони можуть містити ім'я, дату народження, адресу, номер телефону, електронну пошту, ідентифікаційний код, біометричні та генетичні дані тощо. Відповідно до міжнародного законодавства, зокрема Загального регламенту про захист даних Європейського Союзу, персональні дані охоплю-

ють будь-яку інформацію, що прямо чи опосередковано стосується фізичної особи. Схоже визначення надає Конвенція № 108 Ради Європи [5]. В Україні регулювання у сфері захисту персональних даних відбувається згідно з Законом України «Про захист персональних даних». [2]Згідно з цим законом, персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Обов'язки що полягають на суб'єктів для обробки персональних даних (контролерів і процесорів) містять: обробку даних відповідно до принципів законності, прозорості та добросовісності; захист даних від несанкціонованого доступу, втрати чи пошкодження; виконання вимог законодавства щодо згоди на обробку даних; надання особам можливості реалізовувати свої права на захист даних [7].

Цивільно-правовий захист персональних даних є важливим елементом сучасного правового регулювання, особливо в умовах цифрової ери. Персональні дані містять відомості про особу, які можуть бути використані для її ідентифікації, і тому потребують особливого підходу до їхнього захисту.

В Україні захист персональних даних регулюється Законом «Про захист персональних даних», який визначає права фізичних осіб на доступ до своїх даних та контроль над їхнім використанням. Особи мають право знати, хто є розпорядником їхніх даних, з якою метою вони обробляються, а також можуть вимагати виправлення або видалення цих даних. Обробка персональних даних повинна відповідати принципам законності, прозорості, визначеності мети та мінімізації даних, що забезпечує їхнє використання виключно в законних межах.

Українське законодавство враховує міжнародні стандарти, зокрема положення Загального регламенту про захист даних ЄС (GDPR), що сприяє гармонізації правових норм і захисту прав осіб у міжнародному контексті. Особливу увагу варто приділити питанням захисту персональних даних в умовах воєнного стану, коли ризики кіберзагроз значно зростають.

Важливо зазначити, що порушення законодавства про захист персональних даних передбачає адміністративну та кримінальну відповідальність, включаючи штрафи або навіть позбавлення волі в окремих випадках. Ці положення покликані забезпечити належний рівень правового захисту і відповідальності за недобросовісне поводження з персональними даними.

Цілісний підхід до захисту персональних даних потребує дотримання норм законодавства та активного застосування сучасних технологій для захисту приватності, що є ключовим у забезпеченні безпеки особистої інформації.

Порушення права на захист персональних даних може спричинити цивільно-правову, адміністративну або кримінальну відповідальність. До цивільно-правових механізмів захисту можна віднести: вимогу про припинення неправомірного використання персональних даних, вимогу про видалення або виправлення неправдивих чи недостовірних даних, вимогу про відшкодування збитків, завданих незаконним використанням персональних даних. Особа, персональні дані якої були незаконно використані, має право вимагати відшкодування матеріальної та моральної шкоди [9]. Матеріальна шкода може містити реальні збитки, спричинені використанням персональних даних. Моральна шкода охоплює нематеріальні втрати, як-от психологічний дискомфорт або репутаційні ризики.

У нинішньому цифровому світі кіберзагрози стали серйозним викликом для безпеки особистих даних [4]. Оскільки більшість інформації зберігається в електронному вигляді, зловмисники вдаються до різних методів, щоб отримати несанкціонований доступ до конфіденційної інформації. Це створює серйозні ризики як для окремих осіб, так і для організацій.

Заключають такі типи кіберзагроз: хакерські атаки – це дії зловмисників, спрямовані на проникнення в інформаційні системи з метою викрадення, зміни або знищення даних. Фішинг – метод шахрайства, при якому зловмисники видають себе за довірених осіб або організації для отримання конфіденційної інформації, як-от логіни, паролі та фінансові дані[10].

Витоки даних – це несанкціоноване розповсюдження або продаж особистої інформації. Соціальна інженерія – маніпулятивні техніки, що використовуються для отримання доступу до конфіденційної інформації шляхом введення жертви в оману. Кіберзагрози можуть мати серйозні наслідки для приватного життя людей. Викрадення особистих даних може призвести до фінансових втрат, шахрайства, крадіжки особистості та навіть шантажу [1].

Важливо також звернути увагу на судову практику в Україні в питаннях кібербезпеки. У постанові Верховного Суду від 21.04.2021 у справі № 579/806/19 підкреслено, що особа має право відкликати згоду на обробку своїх персональних даних. Суд зазначив, що обробка персональних даних без згоди особи допускається лише у випадках, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. [8]

Перспективи розвитку правового регулювання включають гармонізацію національного законодавства з міжнародними стандартами, посилення контролю за діяльністю операторів особистих даних, а також розширення прав громадян щодо контролю над своїми даними. Одним із ключових напрямків удосконалення правового регулювання є збільшення відповідальності за порушення у сфері захисту особистих даних. Це може включати збільшення штрафів для компаній, які неправомірно використовують особисті дані, впровадження нових механізмів розслідування порушень, а також посилення ролі наглядових органів у сфері захисту особистих даних [3].

Захист особистих даних вимагає не тільки вдосконалення законодавства, а й використання інноваційних технічних рішень. Важливим є розвиток механізмів саморегулювання у сфері цифрової безпеки, що дасть змогу швидше адаптуватися до нових викликів.

Окрім правових та технічних аспектів, важливою складовою ефективного захисту особистих даних є підвищення цифрової грамотності населення. Громадяни повинні бути обізнані зі своїми правами та ризиками, пов'язаними з обробкою особистих даних. Освітні кампанії, тренінги та інтеграція теми цифрової безпеки у шкільну

та вищу освіту допоможуть формувати усвідомлене ставлення до використання особистих даних у цифровому середовищі [8].

Дослідивши проблематику можна зробити такі висновки: потреба у посиленні кібербезпеки – збільшення кількості кібератак та удосконалення тактик змушує поліпшити технічний захист особистої інформації та оновити системи безпеки. Зміцнення захисту прав осіб, чиї дані обробляються – слід спростити процедури подання скарг та підвищити ефективність розгляду справ про порушення прав тих, чиї дані обробляються. Підвищення юридичної відповідальності – теперішні санкції за незаконну обробку особистої інформації недостатньо ефективні, тому необхідні суворіші заходи та дієвіші механізми їх застосування. У цілому, відчувається потреба у комплексному реформуванні правового регулювання у сфері захисту персональних даних, яке буде враховувати технічні, організаційні та юридичні аспекти [11].

ЛІТЕРАТУРА:

1. Цивільний процесуальний Кодекс України. 2008 С. 3–214
2. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI: станом на 18 січ. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
3. Про електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII: станом на 18 груд.2024 р. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>
4. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII: станом на 28 черв. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.
5. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Конвенція Ради Європи від 28.01.1981: станом на 6 лип. 2010 р. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text
6. ZakonOnline. Постанова від 21.04.2021 по справі № 579/806/19 Касаційний цивільний суд | ZakonOnline – Право знати!. Аналітично-правова система ZakonOnline. URL: https://zakononline.com.ua/court-decisions/show/96501519?utm_source (дата звернення: 11.04.2025).
7. Братасюк О.Б. Захист персональних даних: українські реалії та зарубіжний досвід. Закарпатські правові читання. Право як інструмент стійкості та розвитку в умовах сучасних цивілізаційних викликів. Частина 1. 2023. URL: <https://doi.org/10.36059/978-966-397-298-5-38>

8. Брижко В.М. Сучасні основи захисту персональних даних в правових актах. Інформація і право. 2016. № 3 (18). С. 45–57.
9. Зеркаль О.В. Деякі питання захисту персональних даних. Бюлетень Міністерства юстиції України. 2012. № 1 (123). С. 5–14.
10. Кондратенко Н.М. Щодо правового регулювання захисту персональних даних. Держава та регіони. Право. 2012. № 3 (37). С. 62–66.
11. Похиленко І. Правове регулювання захисту персональних даних. Scientific works of National Aviation University. Series: Law Journal «Air and Space Law». 2023. Т. 4, № 69. С. 94–99. URL: <https://doi.org/10.18372/2307-9061.69.18322>

Рогожа Валерія Василівна,

студентка 2-го курсу факультету прокуратури та слідства (кримінальна юстиція) Національного університету «Одеська юридична академія».

Науковий керівник: к.ю.н., доц., проф. кафедри цивільного права

Калітенко О.М.

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ: ЗАХИСТ ЧИ ЗАГРОЗА?

Інтеграція штучного інтелекту в системи кібербезпеки відкриває нові можливості для ефективного захисту даних та інформаційних інфраструктур у сучасному цифровому світі, де кіберзагрози стають дедалі складнішими та більш витонченими. З огляду на зростаючу складність і динамічність кіберзагроз, традиційні методи захисту виявляються недостатньо ефективними, що зумовлює необхідність пошуку нових підходів.

Штучний інтелект (ШІ) має потенціал значно підвищити ефективність систем кібербезпеки, забезпечуючи автоматизацію процесів виявлення загроз, аналіз аномалій, прогнозування можливих атак та адаптацію захисних механізмів у режимі реального часу. Це стає можливим завдяки здатності ШІ обробляти великі масиви даних, виявляти складні закономірності та взаємозв'язки, які можуть залишитися непомітними для людини. Проте, інтеграція ШІ в кібербезпеку супроводжується низкою викликів. Основними проблемами є забезпечення точності та надійності роботи ШІ, оскільки помилкові спрацювання можуть призвести до збоїв у системі захисту або навіть спричинити помилкове блокування ле-

гітимної активності. Крім того, алгоритми ШІ можуть стати об'єктом атак, що вимагає розробки заходів захисту самих алгоритмів від маніпуляцій та втручання. Існує також питання етичності та прозорості прийняття рішень штучним інтелектом у контексті конфіденційності даних та потенційних обмежень доступу до критично важливої інформації.

У наукових працях зазначається, що методи і стратегії кібербезпеки на основі ШІ можуть забезпечити надійніший захист від сучасних загроз. Дослідження, що фокусуються на огляді цих методів, зокрема аналізують, як ШІ допомагає виявляти нові види атак і адаптуватися до швидко змінюваного кіберсередовища [1, 2]. Наприклад, розглядаються системи, що використовують штучний інтелект для аналізу поведінкових аномалій, що дозволяє виявляти кіберзлочини на ранніх етапах.

Інший напрямок досліджень фокусується на питаннях забезпечення кібербезпеки в самих системах штучного інтелекту, зокрема на аналізі їхніх вразливостей і контрзаходів, необхідних для протидії цим уразливостям. У цих публікаціях підкреслюється, що кібербезпека систем, які використовують ШІ, потребує унікального підходу, оскільки вони схильні до атак типу «отруєння даних» та інших маніпуляцій, що можуть змінити результати моделі [3]. Зокрема, аналізуються типи атак і заходи для їхнього попередження, що мають критичне значення у безпеці автоматизованих систем [4].

Інноваційні рішення для бізнесу, особливо в електронному комерційному середовищі, також активно обговорюються в публікаціях. Дослідники підкреслюють, що використання ШІ у бізнесових структурах є одночасно перспективним і ризикованим, оскільки тут необхідно не лише враховувати технічні аспекти, але й забезпечувати постійний моніторинг та оперативне реагування на нові види загроз [5]. Етичні аспекти застосування штучного інтелекту в кібербезпеці стають дедалі важливішими, оскільки використання автоматизованих систем для захисту інформації та даних впливає на базові права користувачів і піднімає складні питання відповідальності та прозорості. Одним із ключових етичних викликів є

забезпечення конфіденційності даних. Алгоритми ШІ обробляють великі обсяги інформації, включаючи персональні та конфіденційні дані, що створює ризики несанкціонованого доступу або неналежного використання цих даних. Водночас організації повинні гарантувати, що інформація зберігається та обробляється відповідно до принципів захисту персональних даних і забезпечення конфіденційності, щоб уникнути порушення прав користувачів.

Прозорість рішень, що приймаються алгоритмами штучного інтелекту, також є важливим аспектом у сфері кібербезпеки. У більшості випадків алгоритми, зокрема алгоритми глибинного навчання, функціонують як «чорні ящики», що ускладнює розуміння процесу прийняття рішень та причини конкретних дій системи. Це може викликати сумніви щодо об'єктивності та справедливості рішень, особливо коли йдеться про автоматичне блокування доступу до даних або виявлення підозрілої поведінки. Прозорість рішень важлива не тільки для довіри користувачів, але й для забезпечення підзвітності.

Організації повинні мати можливість пояснити, чому алгоритм прийняв певне рішення, особливо якщо це стосується дій, що мають серйозні наслідки для безпеки чи приватності.

Адаптивні можливості систем кібербезпеки на базі штучного інтелекту вже демонструють високу ефективність у різних галузях, таких як банківський сектор, корпоративні мережі та хмарні платформи. Наприклад, у банківському секторі використовується автоматичне налаштування ШІ для виявлення підозрілих транзакцій у реальному часі. Якщо система виявляє аномалії у поведінці користувача, такі як спроба входу з незвичних геолокацій або нетипові суми переказів, вона автоматично блокує операцію та сповіщає клієнта. Це значно підвищує рівень безпеки та запобігає потенційному шахрайству.

Ще одним практичним прикладом є застосування ШІ в електронній пошті для захисту від фішингових атак. Система аналізує нові вхідні повідомлення, порівнюючи їхній стиль та вміст із відомими фішинговими шаблонами, і адаптується до нових методів

обману, які зловмисники використовують для обходу традиційних захисних фільтрів. Коли з'являються нові методи фішингу, система самостійно оновлює свої алгоритми для точнішого розпізнавання загроз, що мінімізує ризик несанкціонованого доступу через електронну пошту.

Крім того, для підтримання гнучкості кіберсистем доцільно запровадити комплексний план навчання персоналу, що включає не тільки технічні знання, але й етичні принципи роботи з ШІ та кібербезпекою. Це дозволяє співробітникам діяти відповідно до стандартів та знижує ймовірність помилок при експлуатації ШІ-систем. Подібні навчальні програми мають бути постійно актуалізованими з урахуванням нових загроз і тенденцій у сфері кібербезпеки.

Ці практичні рекомендації, що включають управління доступом до даних, розвиток міждисциплінарної співпраці, регулярні аудити алгоритмів та навчання персоналу, формують основу для ефективного і відповідального використання штучного інтелекту в кібербезпеці.

На основі проведеного дослідження встановлено, що інтеграція штучного інтелекту в системи кібербезпеки має значний потенціал для підвищення рівня захисту інформаційних інфраструктур завдяки здатності ШІ-алгоритмів виявляти нові загрози, аналізувати аномалії та прогнозувати потенційні атаки. Основними проблемами при впровадженні ШІ в кібербезпеку є забезпечення точності алгоритмів та їхньої стійкості до зовнішніх втручань, а також етичні виклики, пов'язані з конфіденційністю даних і прозорістю рішень.

Суттєвою перешкодою залишається потреба у висококваліфікованих кадрах і значні фінансові витрати на впровадження та підтримку ШІ-систем.

ЛІТЕРАТУРА:

1. Лунгол О. Огляд методів та стратегій кібербезпеки засобами штучного інтелекту. «Кібербезпека: освіта, наука, техніка». 2024. № 1.25. С. 379–389. DOI: <https://doi.org/10.28925/2663–4023.2024.25.379389>

2. Онищенко Ю., Каланча А., Гельдт С. Застосування штучного інтелекту у сфері кібербезпеки. Trends, theories and ways of improving science:

The 8th International scientific and practical conference Madrid, Spain: International Science Group. 2023. С. 544. URL: <http://surl.li/urooxa>

3. Неретін О., Харченко В. Забезпечення кібербезпеки систем штучного інтелекту: аналіз вразливостей, атак і контрзаходів. *Information Systems And Networks*. 2022. № 12. С. 7–20.

4. Черевко К. О. Штучний інтелект як інструмент протидії злочинності. *Вісник Кримінологічної асоціації України*. 2023. № 28.1. С. 124–133.

5. Шкоденко Т. Роль штучного інтелекту в сучасних стратегіях кібербезпеки: аналіз потенційних загроз для електронного бізнесу. *Graill of Science*. 2024. № 37. С. 239–240. URL: <https://archive.journal-grail.science/index.php/2710-3056/article/view/2158>

Фасій Анастасія Володимирівна,

студентка 2-го курсу факультету цивільної та господарської юстиції

Національного університету «Одеська юридична академія».

Науковий керівник: к.ю.н., доц., доц. кафедри цивільного права

Завальнюк С. В.

ДО ПИТАННЯ ПРО ПРАВОВЕ РЕГУЛЮВАННЯ РЕКЛАМИ В СОЦІАЛЬНИХ МЕРЕЖАХ

Розвиток цифрових технологій став ключовим фактором інформаційної революції, що призвела до формування глобального інформаційного середовища. Онлайн-простір став універсальним засобом обміну даними, що відкриває нові можливості для реклами.

Новий рівень громадянського суспільства в інформаційну епоху пов'язаний із появою соцмереж. Соціальні мережі стали платформою для комунікації, обговорення та інтеграції суспільства.[1, с. 20]

На сьогодні популярність інтернет-реклами в соцмережах зростає разом із кількістю користувачів. Серед них більшість – це молодь, яка має найвищу споживчу спроможність. Популярними платформами для розміщення реклами в Україні є Instagram, Facebook, Telegram та інше.

Реклама на платформах соціальних мереж є одним із найбільш результативних методів донесення інформації до споживачів. Од-

нак компаніям слід враховувати, що дія Закону України «Про рекламу» поширюється й на цей вид реклами.

У статті 1 Закону України «Про рекламу» визначається термін «реклама», за яким можна виділити такі ключові ознаки реклами:

- 1) інформація стосується особи чи товару;
- 2) поширена на комерційній основі або для власного просування;
- 3) розповсюджена в будь-якій формі та в будь-який спосіб;
- 4) призначена для створення чи підтримки інтересу та обізнаності споживачів [2, с. 66].

Зміни до Закону України «Про рекламу», ухвалені Верховною Радою наприкінці травня 2023 року, встановлюють нові правила для рекламної діяльності в Україні. Відтепер, рекламна діяльність в Україні регулюється відповідно до стандартів ЄС. Нововведення охоплюють цифрову рекламу, телевізійну рекламу, e-mail розсилки, чат-боти та активність блогерів у соцмережах. Метою змін є досягнення прозорості, відповідальності та захисту прав споживачів, а також забезпечення справедливого рекламного ринку в умовах технологічного процесу [3].

Зміни до закону передбачають нові вимоги для таргетованої реклами, розширює соціальну рекламу, заборону продакт-плейсменту та обмеження реклами заборонених товарів. Також встановлені обмеження для реклами лікарських засобів, тютюнових виробів та заборонених товарів.

Закон щодо регулювання реклами встановлює вимоги для платформ відео- та інформаційного контенту (Facebook, Instagram, YouTube тощо) в Україні. Провайдери можуть самостійно встановлювати обсяг реклами, проте вона повинна відповідати законодавчим вимогам щодо конкуренції та захисту прав споживачів.

Нове законодавство про рекламу включає термін «користувацький контент». Простіше кажучи, користувацький контент – це матеріали, як-от пости та відео, які ми щодня переглядаємо в соцмережах. Реклама тепер охоплює просування товару чи послуги як за гроші, так і за інші винагороди. Також законом заборонено

розповсюдження реклами у формі спаму та регулює її розсилку через електронну пошту, повідомлення, веб-сайти й чат-боти. Спам-реклама дозволена лише за письмовою згодою споживача.

Усі ці зміни спрямовані на формування прозорого та справедливого рекламного ринку в Україні, що відповідає сучасним реаліям та технологічним тенденціям [3].

Відповідно до ст. 27 Закону України «Про рекламу», відповідальність за порушення рекламного законодавства можуть нести три категорії суб'єктів: рекламодавці; виробники реклами; розповсюджувачі реклами.

Відповідальність за правопорушення виробник реклами несе у разі доведення його вини. Суб'єкти можуть бути притягнуті до відповідальності як індивідуально, так і спільно.

Також у Законі України «Про рекламу» визначено поняття недобросовісної реклами, яку можна охарактеризувати як таку, що вводить споживачів в оману, містить неправдиві або неповні відомості та дискредитує інших виробників [4]. Основні риси недобросовісної реклами:

- вводить в оману, копіюючи оформлення, текст чи звукові ефекти інших реклам, використовуючи недосвідченість споживачів;
- дискредитує осіб, які не обирають рекламний товар;
- порушує встановлені вимоги до часу, місця та способу поширення;
- містить некоректні висловлювання, які принижують або дискредитують конкурентів, завдаючи шкоди їхній репутації;
- характеризується наявністю неточностей, двозначностей, недостовірності та перебільшень.

Недобросовісна реклама є забороненою, а за її порушення відповідає винна особа.

Підсумовуючи вищесказане, слід зауважити, що, попри зміни в Законі України «Про рекламу», правове регулювання реклами

в соціальних мережах все ще залишається недосконалим. Правове регулювання реклами в соціальних мережах є важливою і актуальною темою, яка потребує постійної уваги. Постійні зміни та інновації на платформах соцмереж потребують постійного оновлення законодавства для усунення виникаючих прогалин.

ЛІТЕРАТУРА:

1. IT-право – теорія та практика: посібник. авт. кол.; за ред. д.ю.н., проф. Є. О. Харитонов. Одеса, Фенікс, 2017. 472 с.
2. Фасій Б.В., Матвійчук А. В. Реклама в соціальних мережах: проблема регулювання. *Часопис цивілістики*. 2018. № 30. С. 66–70.
3. Закон про рекламу в Україні оновили: що змінилось. URL: <https://www.rivneprod.gov.ua/2023/10/10/zakon-pro-reklamu-v-ukrayini-onovyly-shho-zminylos/>
4. Про рекламу: Закон України. Відомості Верховної Ради України. 1996. № 39. Ст. 181. URL: <http://zakon4.rada.gov.ua/laws/show/270/96-вр>

ВИСНОВКИ

Шановні учасники круглого столу!

Підсумовуючи нашу дискусію, варто наголосити: в умовах гібридної війни інформаційні технології перетворилися на стратегічний ресурс, який одночасно є інструментом розвитку і полем для нових загроз. Російсько-українська війна яскраво продемонструвала, наскільки важливою є надійна кібербезпека як на рівні держави, так і на рівні кожного громадянина.

У таких реаліях ІТ-право має швидко реагувати на виклики цифрової доби: забезпечувати правовий захист цифрової особистості, регулювати застосування штучного інтелекту, захищати критичну інфраструктуру, боротися з інформаційними атаками та кіберзлочинністю.

Особливої уваги потребує захист вразливих категорій населення, зокрема людей похилого віку, дітей, а також регулювання питань спадкування цифрових активів, використання автоматизованих систем на полі бою та відповідальності за фейки і дезінформацію у соціальних мережах.

Сьогодні ІТ-право – це не просто сфера юридичної практики. Це один із головних чинників національної безпеки, захисту прав людини й розвитку сучасної держави. В процесі наукової дискусії були сформульовані наступні висновки:

Штучний інтелект у війні: Використання ШІ у російсько-українській війні підкреслило потребу розробки чітких міжнародно-правових стандартів щодо використання автономних систем у збройних конфліктах та гарантування дотримання гуманітарного права.

Цифрові аватари: Відсутність визначеного правового статусу цифрових аватарів ускладнює їх правове регулювання. Необхідно розробити критерії для класифікації їх як об'єктів або суб'єктів права.

Смарт-контракти та ІІІ: Застосування штучного інтелекту для укладання смарт-контрактів потребує нормативного врегулювання, зокрема щодо валідності угод, розподілу ризиків та механізмів відповідальності.

Поняття штучного інтелекту: Наразі відсутнє уніфіковане визначення поняття ІІ, що ускладнює його регулювання у різних сферах права. Потрібна гармонізація термінології на міжнародному та національному рівнях.

Право на освіту під час війни: Цифровізація освіти є важливим інструментом забезпечення права дітей на освіту в умовах гібридної війни, але потребує гарантій рівного доступу та захисту персональних даних.

Шлюбні правовідносини у цифрову добу: Під впливом цифровізації шлюбні правовідносини змінюються, що вимагає оновлення нормативних актів щодо укладення та розірвання шлюбу через електронні сервіси.

Інформаційне середовище у гібридних конфліктах: Інформаційні ресурси стали стратегічним фактором у веденні гібридних війн, що вимагає створення ефективних систем кібербезпеки та інформаційної протидії.

Страховання відповідальності ІТ-компаній: Професійна відповідальність у сфері ІТ потребує спеціального страхового регулювання для мінімізації ризиків технічних збоїв і витоку даних.

ІТ в охороні здоров'я: Впровадження інформаційних технологій у систему охорони здоров'я має супроводжуватися посиленням правового захисту пацієнтів і медичних даних.

Правова охорона творчих результатів ІІІ: Продукти, створені за допомогою штучного інтелекту, потребують спеціального підходу до захисту авторських прав та врегулювання питань авторства.

Спадкування цифрових речей: Необхідно розробити законодавчі механізми спадкування цифрового майна, зокрема щодо доступу до акаунтів, цифрових активів та віртуальної власності.

Цивільно-правові відносини в Інтернеті: Складність таких відносин вимагає розробки гнучких правових норм, що враховуватимуть специфіку онлайн-середовища.

Правовий статус стартапу: Стартапи як суб'єкти ІТ-відносин потребують спеціального правового регулювання, що сприятиме розвитку інновацій та венчурного інвестування.

Емоційні фейки у соцмережах: Поширення фейкової інформації, що викликає емоційні реакції, вимагає посилення юридичної відповідальності та заходів боротьби з дезінформацією.

Цифрова ідентичність у соцмережах: Питання захисту цифрової ідентичності набуває особливої актуальності та потребує розробки правових механізмів її охорони.

Кібербезпека літніх людей: В умовах гібридної війни особливої уваги потребує захист людей похилого віку від кіберзагроз та інформаційних атак.

Дякуємо всім учасникам за активну роботу, зацікавленість і фахову дискусію. Переконали, що спільними зусиллями ми зможемо розробити ефективні правові механізми, які відповідатимуть реаліям гібридної війни і захищатимуть Україну у цифровому просторі.

Слава Україні!

Євген Харитонов

*доктор юридичних наук, професор,
член-кореспондент НАПрН України*

Юлія Кривенко

кандидатка юридичних наук, доцентка

Зміст

ПЕРЕДМОВА	4
Харитонов Євген Олегович ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ У РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ: ПРАВОВІ ПРОБЛЕМИ	6
Булеца Сібілла Богданівна ЦИФРОВІ АВАТАРИ: ОБ'ЄКТИ ЧИ СУБ'ЄКТИ ПРИВАТНОГО ПРАВА	10
Голубєва Неллі Юрійвна РОЗВИТОК CROSS BORDER E-COMMERCE В УКРАЇНІ	16
Давидова Ірина Віталівна ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ УКЛАДАННЯ СМАРТ-КОНТРАКТІВ	20
Менджул Марія Василівна ЦИФРОВІЗАЦІЯ ЯК ІНСТРУМЕНТ РЕАЛІЗАЦІЇ ПРАВА НА ОСВІТУ ДІТЕЙ В УМОВАХ ВІЙНИ	24
Самойленко Георгій Валерійович ДО ПИТАННЯ ВИЗНАЧЕННЯ ПРАВОВОЇ ПРИРОДИ СТАРТАПУ	27
Сафончик Оксана Іванівна ДЕЯКІ ПИТАННЯ ШЛЮБНИХ ПРАВОВІДНОСИН В ЦИФРОВУ ДОБУ В УМОВАХ ГІБРИДНОЇ ВІЙНИ	31
Харитонova Олена Іванівна БАГАТОАСПЕКТНІСТЬ РОЗУМІННЯ «ШТУЧНОГО ІНТЕЛЕКТУ»	35
Берназ-Лукавецька Олена Михайлівна ОСОБЛИВОСТІ СТРАХУВАННЯ ПРОФЕСІЙНОЇ ВІДПОВІДАЛЬНОСТІ ІТ КОМПАНІЙ	40
Василевська Надія Станіславівна ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В СИСТЕМІ ОХОРОНИ ЗДОРОВ'Я	43
Галупова Лариса Ігорівна КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ПРАВОВОЇ ОХОРОНИ РЕЗУЛЬТАТІВ ТВОРЧОЇ ДІЯЛЬНОСТІ, СТВОРЕНИХ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ	47
Калітенко Оксана Михайлівна ІНФОРМАЦІЙНЕ СЕРЕДОВИЩЕ, ЯК СТРАТЕГІЧНИЙ РЕСУРС У ГІБРИДНИХ КОНФЛІКТАХ	52
Кривенко Юлія Василівна ДО ПИТАННЯ СПАДКУВАННЯ ЦИФРОВОЇ РЕЧІ	55
Маковій Віктор Петрович ПРАВОВИЙ СТАТУС СТАРТАПУ ЯК СУБ'ЄКТА ІТ-ВІДНОСИН	59
Омельчук Олександр Сергійович ПОТЕНЦІАЛ ТА ПРОБЛЕМИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ НА ДЕЙТИНГ-ПЛАТФОРМАХ	64

Резніченко Семен Васильович НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ПЕРЕВЕЗЕНЬ ПАСАЖИРІВ АВТОБУСАМИ	67
Святошнюк Арина Леонідівна ЗМІСТ ЦИВІЛЬНО-ПРАВОВИХ ВІДНОСИН У МЕРЕЖІ ІНТЕРНЕТ	73
Спасова Катерина Іванівна ЦИВІЛЬНО-ПРАВОВІ АСПЕКТИ ЦИФРОВОЇ ІДЕНТИЧНОСТІ В СОЦІАЛЬНИХ МЕРЕЖАХ	75
Токарева Віра Олександрівна ДО ПИТАННЯ ВИКОРИСТАННЯ АВТОНОМНИХ СИСТЕМ У ЗБРОЙНОМУ КОНФЛІКТІ	78
Вовчок Руслан Володимирович ІНФОРМАТИЗАЦІЯ ТА ЦИФРОВІЗАЦІЯ СУСПІЛЬСТВА В ЕПОХУ СТІМКОГО РОЗВИТКУ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ	81
Кірсанов Олексій Володимирович ВЕРИФІКАЦІЯ БАНКІВСЬКИХ КАРТ КЛІЄНТА	85
Коштура Богдан Вячеславович ШТУЧНИЙ ІНТЕЛЕКТ ЯК УЧАСНИК ЕЛЕКТРОННИХ ПРАВОЧИНІВ	87
Романовський Денис Сергійович ІТ ПРАВА ТА КІБЕРБЕЗПЕКА ЛЮДЕЙ ПОХИЛОГО ВІКУ В УМОВАХ ГІБРИДНОЇ ВІЙНИ	91
Рябченко Вікторія Олександрівна ПРОБЛЕМИ ЗАХИСТУ НЕПОВНОЛІТНІХ ВІД ВЕРБУВАННЯ ФСБ У СОЦМЕРЕЖІ «ТЕЛЕГРАМ»	95
Балик Даша Вікторівна ОСОБЛИВОСТІ ЗДІЙСНЕННЯ ПРАВА ВЛАСНОСТІ НА ЦИФРОВІ РЕЧІ	99
Білошкурський Микола Миколайович ЦИВІЛЬНО-ПРАВОВИЙ СТАТУС ІГРОВОЇ ОНЛАЙН-РЕЧІ НА ПРИКЛАДІ СЕРВІСУ STEAM	104
Забудько Анастасія Сергіївна ОСОБЛИВОСТІ СПАДКУВАННЯ ЦИФРОВИХ АКТИВІВ	111
Костенко Олександр Сергійович АВТОРСЬКІ ПРАВА НА ОБ'ЄКТИ, СТВОРЕНІ ШТУЧНИМ ІНТЕЛЕКТОМ: ПРАВОВІ АСПЕКТИ РЕГУЛЮВАННЯ	115
Мурашева Катерина Василівна ПЕРСОНАЛЬНІ ДАНІ ТА ЇХ ЗАХИСТ: ЦИВІЛЬНО-ПРАВОВІ АСПЕКТИ В УМОВАХ КІБЕРЗАГРОЗ	119
Рогожа Валерія Василівна РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ: ЗАХИСТ ЧИ ЗАГРОЗА?	124
Фасій Анастасія Володимирівна ДО ПИТАННЯ ПРО ПРАВОВЕ РЕГУЛЮВАННЯ РЕКЛАМИ В СОЦІАЛЬНИХ МЕРЕЖАХ	128
ВИСНОВКИ	132

Наукове видання

ІТ-право та кібербезпека в умовах гібридної війни

МАТЕРІАЛИ

Всеукраїнського круглого столу

Одеса,

12 квітня 2025 року

За загальною редакцією

доктора юридичних наук, професора Євгенія Харитонова,
кандидатки юридичних наук, доцентки Юлії Кривенко

Упорядники-укладачі

Юлія Кривенко, Єлизавета Лешкова

Електронне видання

Формат 60x84/16. Ум-друк. арк. 8,0.
Зам. № 2505-05.

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