СОЦІАЛЬНА СПРАВЕДЛИВІСТЬ ТА ЦИФРОВА ЕКОНОМІКА. 2025

ЗБІРНИК МАТЕРІАЛІВ МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

SOCIAL JUSTICE AND DIGITAL ECONOMY. 2025

PUBLICATION OF MATERIALS OF THE INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE

The Clark Foundation *for Legal Education*

UKRAINIAN NATIONAL BAR ASSOCIATION

Cyber Scotland Week

AIEi

Ukrainian Modern Digital Science

Державна установа «Інститут економіко-правових досліджень
імені В.К. Мамутова Національної академії наук України»

State Institution "V.K. Mamutov Institute of Economic
and Legal Research of the National Academy of Sciences of Ukraine"

СОЦІАЛЬНА СПРАВЕДЛИВІСТЬ ТА ЦИФРОВА ЕКОНОМІКА. 2025

**ЗБІРНИК МАТЕРІАЛІВ
МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ
КОНФЕРЕНЦІЇ**

SOCIAL JUSTICE AND DIGITAL ECONOMY. 2025

**PUBLICATION OF MATERIALS
OF THE INTERNATIONAL
SCIENTIFIC AND PRACTICAL
CONFERENCE**

КИЇВ
АКАДЕМПЕРІОДИКА
2025

https://doi.org/10.15407/akademperiodyka.545.100
УДК 346.3
С69

Соціальна справедливість та цифрова економіка. 2025: С69 зб. матеріалів Міжнарод. наук.-практ. конф. (28.02.2025, Київ) / ДУ «Інститут економіко-правових досліджень імені В.К. Мамутова Національної академії наук України». — Київ: Академперіодика, 2025. — 100 с.

ISBN 978-966-360-545-6

У збірнику оприлюднено матеріали, представлені під час міжнародної конференції «Соціальна справедливість та цифрова економіка. 2025», присвяченої обговоренню викликів цифрової економіки. Конференція об'єднала експертів у сферах цифрових фінансів, криптовалют, санкційної політики та штучного інтелекту, адже нині Україна потребує сучасних правових механізмів регулювання цифрової економіки (криптоактивів, штучого інтелекту зокрема), що сприятиме не лише економічній стабільності, а й підвищенню довіри до національного фінансового ринку в умовах глобальних економічних змін.

Для фахівців з цифрової економіки та міжнародного права, зацікавлених у процесах цифрової трансформації суспільства і застосуванні для цього сучасних технологій.

УДК 346.3

ISBN 978-966-360-545-6

https://doi.org/10.15407/akademperiodyka.545.003

АНДРІЄНКО ОЛЕНА
кандидат психологічних наук, адвокат,
заступник директора з правових питань
ДП «ССМ» (Publicis Groupe Ukraine),
член Експертно-консультаційного комітету
з питань розвитку сфери ШІ в Україні
при Міністерстві цифрової трансформації України,
м. Київ, Україна

ВАЖКА ПРОБЛЕМА (ПІД)СВІДОМОСТІ: ПРАВОВИЙ ЗАХИСТ СПОЖИВАЧІВ ВІД МАНІПУЛЯЦІЙ З ВИКОРИСТАННЯМ СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ

Вступ. Стрімкий розвиток штучного інтелекту (далі — ШІ) та його трансформуючий вплив на всі сфери економіки актуалізує низку фундаментальних питань (як-то дефініція свідомості та поняття свободи волі), які отримують цілком прикладне значення. Зокрема, використання систем ШІ для аналізу поведінки споживачів, персоналізації рекламного контенту і нейромаркетингу ставить питання про межу між свідомим та несвідомим у різних його проявах і відповідно про правовий захист споживача в умовах інформаційної асиметрії [5], яка мультиплікується через використання ШІ.

Використання ШІ у рекламі: полонити увагу й зачепити емоції. Як зазначається у Рекомендаціях з

Cite: Andrienko Olena. A serious problem of (sub)consciousness — legal protection of consumers against manipulation using artifical intelligence systems. https://doi.org/10.15407/akademperiodyka.545.003

відповідального використання ШІ у сфері реклами та маркетингових комунікацій [3], ШІ у рекламі застовується для різних цілей: від аналітики й створення контенту до мікротаргетування.

В умовах економіки уваги [7, 11] ефективність маркетингової чи рекламної кампанії визначається передусім здатністю емоційно зачепити споживача, спонукаючи до бажаної дії або вибору. Тож такі кампанії розгортаються на межі між свідомим та підсвідомим / раціональним і емоційним / індивідуальним та колективним вибором. Водночас ШІ може значно покращити ефективність кампанії, на що вказують численні дослідження. Серед прикладів: вивчення готовності споживачів приймати рекламу, згенеровану ШІ [9]; дослідження впливу розкриття факту використання ШІ для створення реклами на емоційне сприймання бренду [10] та поведінку споживачів (намір придбати продукт) [6]; вивчення ролі ШІ для *технологічно обґрунтованого маркетингу та підсвідомого брендингу* [14], нейромаркетингу та емоційного впливу [13].

Можна виділити такі напрямки використання ШІ для підвищення ефективності реклами на межі свідомого сприймання:

- **емоційний вплив**: ШІ дає можливість виявляти *колективні емоційні настрої*, домінуючі у конкретний момент часу (наприклад, реакцію на соціально значущу подію) та *індивідуальні емоційні реакції*, використовуючи цю інформацію для генерування реклами, сфокусованої на виявленій емоції;
- **підсвідомі тригери та упередження**: аналіз великих даних для виявлення підсвідомих тригерів, які впливають на рішення споживачів (зокрема, кольори, звуки, образи, інші елементи, які викликають певні емоції та асоціації), виявляти та експлуатувати *упередження*;
- **ефект повторення**: ШІ автоматизує процес повторення рекламних повідомлень, що сприяє їх закріпленню в імпліцитній пам'яті споживачів та підвищенню лояльності останніх через ефект знайомості;

- **маніпуляція сприйняттям**: використання ШІ для створення ілюзії (зокрема, ілюзії вибору) або підштовхування споживачів до певних дій без їхнього достатнього усвідомлення;
- **смислові та ціннісні впливи**: аналіз відкритих даних для виявлення домінуючих колективних та індивідуальних цінностей і смислів для побудови на їхній основі рекламних та маркетингових стратегій;
- **персоналізація**: створення персоналізованих рекламних повідомлень, які враховують індивідуальні особливості споживачів, їхні емоційні реакції, цінності, смисли, специфіку сприймання, поведінкові патерни тощо;
- **соціальні докази та вплив групи**: аналіз соціальної мережі та інших джерел даних для виявлення значимих осіб і референтних груп задля подальшого використання у рекламі через вплив групової динаміки.

Усі описані напрямки використання ШІ можуть призводити до маніпуляції емоціями, сприйняттям та поведінкою споживачів, що викликає не лише етичні, а й психологічні та правові питання, про що йтиметься далі.

Фундаментальні психологічні питання: свідомість і свобода вибору. Аналіз використання ШІ в рекламі, а також застосовний у нормативних документах понятійний апарат (про що мова буде іти нижче) дає можливість виокремити психологічні питання, які потребують розробки прикладних критеріїв для розмежування етично та/або юридично прийнятного і недопустимого:

- **континуум свідоме — несвідоме**. З огляду на «*тяжке питання свідомості*» [8], у законодавстві відсутня *дефініція підсвідомості*. Водночас ці поняття є полюсами широкого континууму, а не бінарною шкалою «1 або 0». Тож розвиток ШІ висуває вимогу у напрацюванні набору критеріїв для оцінки, який вплив вважатиметься підсвідомим;
- **емоційна сфера**. На нейрофізіологічному рівні надмірна активність відповідальної за емоції лімбічної системи гальмує

активність префронтальної кори великих півкуль, яку асоціюють зі здатністю до критичного мислення, планування та вольового контролю поведінки. Разом із тим недостатність функціонування лімбічної кори зумовлює неспроможність людини приймати рішення [12]. Тож психологічне благополуччя людини потребує оптимальної активації лімбічної (емоційної) системи. Також індивідуальна емоційна сфера містить *чутливі до тригерів вразливості* (зумовлені, зокрема, пережитими травмами — індивідуальними, родинними і колективними), може мати схильність до формування *залежностей* (які експлуатує адиктивний дизайн) і є *чутливою до домінуючих колективних (масових) емоцій*;

- **цінності та смисли**. Вони, як емоції, потреби й почуття, належать до диспозитивного ядра (яке виконує роль двигуна особистості), проте на фундаментальнішому рівні. Через таку приналежність апелювання до них є набагато ефективнішим у довгостроковій маркетинговій перспективі для формування лояльності споживачів. Водночас робота з цінностями й смислами — це складна багаторівнева задача, яка передбачає роботу з комплексом свідомих переконань та підсвідомих установок з використанням як емоційного, так і раціонального впливу;
- **когнітивна сфера** охоплює низку проблемних питань: сприймання підпорогових стимулів, імпліцитну пам'ять, мимовільну увагу, упередження, розвинутість інтелекту (як характеристики швидкості, глибини та якості обробки потоку інформації у її певній формі) та мислення, зокрема абстрактного. У підсумку йдеться про *когнітивну спроможність*, яка безпосередньо впливає на те, щоб визнавати певне рішення споживача поінформованим;
- **поведінкова сфера**. На операційному рівні ідеться передусім про усвідомлений вибір та відмову від надмірної експлуатації імпульсивної поведінки. На рівні поведінкової економіки виникає питання про співвідношення *свободи вибору та підштовхування* (nudge) [15], яке не повинно перетворюватися

на *маніпуляцію чи тиск*. А на загальнолюдському рівні — про *людську суб'єктність та агентність*, особливо у контексті стрімкого поширення ШІ-агентів;

- **соціальний тиск, маніпуляція та переконання**. Соціальна психологія розрізняє чотири форми впливу: переконання, навіювання (сугестію), емоційне зараження, наслідування. Перше має найістотніший когнітивний складник і відповідно ступінь усвідомленості й здатності керувати вибором. Решта ж переважно орієнтовані на активізацію лімбічної системи та дзеркальних нейронів, підсилюючи соціальний тиск і спонукаючи до дій, що можуть суперечити особистим інтересам;
- **дипфейки**. Можна виділити в окрему категорію через їхній руйнівний потенціал, спрямований на введення в оману на всіх рівнях психіки: від сенсорного та когнітивного — до потужного емоційного впливу й експлуатації відданості людини певним цінностям та смислам;
- **стрес, дистрес та рівень суб'єктивного благополуччя** (well-being). Визначаються рівнем потужності стимулів будь-якої природи та спрямованості. Будь-яка жива істота потребує стимуляції у певних межах, які у фізиці називають «поясом Золотоволоски». Якщо ж стимуляція або надмірно слабка (десенсибілізація), або надмірно інтенсивна (гіперстимуляція), це викликає дискомфорт, що у контексті рекламної комунікації може призводити до зниження ефективності.

Наведений аналіз показує, що для благополуччя людини важливим є збалансоване функціонування всіх психологічних процесів та систем, і відповідно етичне використання ШІ у рекламно-маркетинговій комунікації передбачає врахування такого балансу й відмову від експлуатації вразливостей.

Право на свідоме рішення та свободу волі. У законодавстві України немає визначення свідомості та підсвідомості, свідомого вибору, поінформованого рішення чи свободи волі. Загалом цей перелік може визначатися поняттям *гідності* як «усвідомлення людиною своєї громадської ваги, громадського

обов'язку» [1, с. [236], що в Україні є найвищою соціальної цінністю (ст. 3, 21, 28, 68 Конституції України) та особистим немайновим благом (ст. 201 Цивільного кодексу України). Згідно зі ст. 7 *Рамкової Конвенції Ради Європи про ШІ та права людини, демократію і верховенство права* повага до людської гідності та автономності людини є одним із семи принципів, яким повинні відповідати системи ШІ впродовж життєвого циклу.

Водночас ст. 8 Закону України «Про рекламу» *забороняє* використовувати засоби і технології, які *впливають на підсвідомість споживачів реклами* (така ж заборона є в ст. 100 Закону «Про всеукраїнський референдум»); ст. 15 Закону «Про захист прав споживачів» закріплює право споживача на одержання необхідної, доступної, достовірної та своєчасної інформації про продукцію, що забезпечує можливість її *свідомого і компетентного вибору*; ст. 15-1 Закону «Про захист від недобросовісної конкуренції» забороняє поширення інформації, що вводить *в оману*, через повідомлення, наприклад у рекламі, неповних, неточних, неправдивих відомостях, зокрема *внаслідок обраного способу їх викладення*, замовчування окремих фактів чи нечіткості формулювань, що вплинули або можуть вплинути на наміри споживачів щодо придбання чи реалізації товарів, робіт, послуг.

Що стосується правозастовування, то аналіз судових рішень показує: хоча наглядові органи регулярно апелюють, що «дії позивача були *направлені саме на підсвідомість споживача*, що безпосередньо привертало увагу останнього на продукцію конкретної торговельної марки» [4], проте не наводять доказів такого впливу, який часто призводить до скасування судом рішень таких органів про накладення штрафних санкцій. (Також існує чимала кількість рішень, де суд посилається на *підсвідомість замість правосвідомості*: «За змістом ст. 252 КпАП України, оцінка доказів здійснюється органом <…> за своїм внутрішнім переконанням, <…>, керуючись законом і підсвідомістю» [2].)

Законодавство ж ЄС наразі перебуває на якісно іншому рівні розвитку щодо захисту споживачів від так званих «темних патернів». У цьому контексті можна згадати такі документи:

- **The Digital Services Act**, п. 67 преамбули якого визначає темні патерни як «практики, які суттєво спотворюють або погіршують, навмисно чи фактично, здатність одержувачів послуги приймати самостійні та усвідомлені вибори чи рішення», а ст. 25 забороняє їх використання;
- **The Unfair Commercial Practices Directive** — зокрема, ст. 8;
- **The Digital Markets Act (DMA) —** ст. 13;
- **The Data Act** — п. 38 преамбули;
- **The Consumer Rights Directive** (CRD) — заборона темних патернів для фінансових послуг;
- European Parliament resolution of 12.12.2023 **on addictive design** of online services and consumer protection in the EU single market (2023/2043(INI)).

Проте найповніший на сьогодні правовий концепт захисту від впливу систем ШІ на підсвідомість споживачів подано у **The Guidelines on prohibited AI practice**, опублікованих 04.02.2025 на виконання, зокрема ст. 5 (1) (a), (b), (f) **AI Act**. Дана стаття визначає використання систем ШІ як високоризикові та забороняє їх, оскільки вважає, що вони впливають на підсвідомість, використовують маніпулятивні та оманливі техніки, експлуатують вразливості, а також розпізнають емоції. Слід підкреслити, що подібна заборона поширюється за умови завдання чи обґрунтованої ймовірності завдання істотної шкоди споживачам, залежить від ситуації використання системи ШІ, а для систем ШІ, які розпізнають емоції, — ще й від джерела даних: використання біометричних даних заборонено, а от семантичний аналіз наразі дозволений. Разом із тим у будь-якому випадку наголошується на індивідуальній оцінці кожного випадку.

Висновки: перспективи та рекомендації. З огляду на євроінтеграційний процес, наведені нормативно-правові акти ЄС є істотним орієнтиром для *розвитку законодавства* України

щодо захисту споживачів від впливу на підсвідомість та маніпуляцій з використанням ШІ. Зауважимо, що даий розвиток потребує *дослідження психологічних феноменів і розробки практичних методик* оцінювання такого впливу, а також запровадження стандартів щодо його допустимих меж.

Водночас уже сьогодні важливо формувати культуру відповідального використання систем ШІ, яка передбачає, зокрема, дотримання принципу «етика за проєктуванням» та поваги до права людини на автономність, свідомі рішення і захист від маніпуляції. Це означає:

1) відмову від використання дипфейків;

2) відмову від використання ШІ для надмірного втручання у сенсорний та емоційний простір споживачів і маркування реклами, виготовлення чи розповсюдження якої використовує методи нейромаркетингу;

3) відмову від використання ШІ для перешкоджання у прийнятті споживачем зважених та поінформованих рішень;

4) інформування споживачів про персоналізацію контенту й використання систем ШІ як під час створення, так і під час розповсюдження реклами, на чому наголошує низка розроблених в Україні рекомендацій з відповідального використання ШІ [2].

Тож саме баланс між захистом прав споживачів та розвитком індустрії є індикатором культури відповідального використання ШІ у рекламі.

ЛІТЕРАТУРА

1. Великий тлумачний словник сучасної української мови. Київ; Ірпінь: Перун, 2007.
2. Постанова Першотравневого районного суду м. Чернівці по справі від 17.02.2025 № 725/549/25. URL: https://reyestr.court.gov.ua/Review/125280257 (дата звернення: 03.02.2025).
3. Рекомендації з відповідального використання ШІ у сфері реклами та маркетингових комунікацій. URL: https://webportal.nrada.gov.ua/

wp-content/uploads/2024/08/rekomendatsiyi_SHIreklama_2024.pdf (дата звернення: 03.02.2025).
4. Рішення Львівського окружного адміністративного суду по справі від 20.02.2025 № 380/7925/24. URL: https://reyestr.court.gov.ua/Review/125336078
5. Akerlof G.A. The Market for 'Lemons': Quality Uncertainty and the Market Mechanism. *Quarterly Journal of Economics*. Vol. 84, No. 3. The MIT Press, 1970. P. 488—500. https://doi.org/10.2307/1879431
6. Andersson L., Pettersson M. AI vs. Human: Ad Creator Influence. *Journal of Advertising Research*. 2024. Vol. 64, No. 4. P. 345—359.
7. Brynjolfsson E., Kim S.T., Oh J.H. The Attention Economy: Measuring the Value of Free Goods on the Internet. *Information Systems Research*. 2023. Vol. 35, No. 3. P. 978—991. https://doi.org/10.1287/isre.2021.0153
8. Chalmers D. Facing up to the problem of consciousness. *Journal of Consciousness Studies.* 1995. Vol. 2, No. 3. P. 200—219.
9. Li Y., Huang J. Exploring Consumer Acceptance of AI-Generated Advertisements. *Journal of Theoretical and Applied Electronic Commerce Research*. 2024. Vol. 19, No. 3. P. 108—123.
10. Massop J. How AI Disclosures Influence Consumers. *Journal of Consumer Psychology*. 2024. Vol. 30, No. 2. P. 210—225.
11. New Economics For Sustainable Development: Attention Economy. *United Nations*. United Nations Economist Network. 2024. Dec. 10.
12. Research and Perspectives in Neurosciences / eds: A. Damasio, H. Damasio. Springer Science & Business Media, 2012.
13. Rossi P. Neuromarketing: Neuroscience and AI Decode Consumer Emotions. *Journal of Neuromarketing Research*. 2025. Vol. 8, No. 1. P. 15—27.
14. Sharma S. Subconscious Branding: The Role of Artificial Intelligence in Marketing. *International Journal of Marketing Studies*. 2023. Vol. 15, No. 2. P. 45—56.
15. Thaler R.H., Sunstein C.R. Nudge: Improving decisions about health, wealth, and happiness. Yale University Press, 2008.

https://doi.org./10.15407/akademperiodyka.545.012

BULGAKOVA DARIA
PhD in International Law, An advocate,
Kryvyi Rih, Ukraine
dariabulgakova@yahoo.com
https://orcid.org/ 0000-0002-8640-3622

DATA SHARING IN CLOUD SERVICES

Users are typically only aware of the service they directly interact with, not the various sub-services that could be hosted on other cloud providers, such as those for advertising or data processing. Anyway, the GDPR requires cloud providers to obtain explicit user consent before performing these actions. When it comes to logistics, the pressure from new legislation about data sharing is not as clear [1]. The challenge for the automotive industry, for example, is that an autonomous vehicle can only collect personal data based on balancing interests because it is not doable to work with consent [1].

Taking into consideration a European Data Strategy of European Commission given to the public in Brussels on 19 February 2020 the compliance problem lay down due to the view that EU-based cloud providers have only a small share of the cloud market, which makes the EU highly dependent on external providers, vulnerable to external data threats and subject to a loss of investment potential for the European digital industry in the data processing market [3]. Therefore, to

Cite: Bulgakova Daria. Data sharing in cloud services. https://doi.org/10.15407/akademperiodyka.545.012

mitigate this risk, on the view of the study, it is proposed look into personal data stores (PDSs). Many PDSs seek to allow the computation (including analytics) to be 'brought' to the data [4, p. 359]. This contrasts with today's common approach where data are transferred to remote, third-party operated servers for computation to occur [Ibid]. PDS technology is beneficial for EU data protection law since it lets app designers specify data access and accounting, and at the same time, users can set impediments to app manners, for example, confining data access. These controls are executed by the PDS's technical configuration and smart agreements onsite of the app when users agree to the app's functionality and data transfers with legal terms that bind developers and platforms. PDSs also facilitate large-scale data processing, where computation occurs on user devices, with only results transferred to institutions, offering users control over data processing while reducing institutions' accountability for raw user data.

The safe and widespread use of data-fuelled products and services also depend on the highest cybersecurity standards [3]. The EU Cybersecurity Certification Framework and the EU Agency for Cybersecurity (ENISA) are play an important role towards that endeavour [3]. In this regard it is useful a Blockchain-based architecture that supports GDPR compliance verification (especially in the context of such a service chain) for enhancing the data privacy of cloud users [2]. The architecture supports a factory of smart contracts, including user consent, GDPR compliance, container, and verification, each of which is activated by an actor within a cloud environment [2].

The solutions are on the table. However, the study supports the idea of Swedish researcher Andersson Kristina [1] on data sharing regulations that have intersectoral impact, likewise, horizontal ones. It is explained on the next point of view. Data sharing — the trade of data between different actors — is a central feature of the development of a data economy. Today, data is conveyed business-to-business (B2B) predominantly from the perspective that the data is

controlled by someone, and that the data has value from a civil law perspective. Compared to many other phenomena, B2B data sharing is relatively unregulated. Data sharing between different companies occurs primarily through agreements and it is up to a company to decide how, when, what, who, and at what price the company wants to share. Another thing that is important to agree on when sharing data is the format of the data standard that you want to share with each other. The EU sees that there is a risk of too much data being collected by a company, which in turn makes the free flow of data more difficult, therefore, need to prevent monopolies from being created. The risk with this is that horizontal (general) legislation is used to solve a problem in one vertical sector but can have unexpected serious consequences for another vertical sector, likewise, preventing an intended business model. It is therefore important to understand what is happening with the regulations for data sharing at the general / horizontal level since it can have a major impact on a certain individual sector vertically.

REFERENCES

1. Andersson K. Regelverk för datadelning inom citylogistik: nulägesanalys. 2022.
2. Barati M., Rana O. Checking GDPR Compliance for Cloud-based Services. *2021 IEEE World Congress on Services (SERVICES)*. 2021. https://doi.org/10.1109/SERVICES51467.2021.00013
3. Communication from the commission to the european parliament, the council, the european economic and social committee and the committee of the regions. *A European strategy for data, COM/2020/66 final*. URL: https://eur-lex.europa.eu/legacontent/EN/TXT/?uri=CELEX:52020DC0066 (last accessed: 03.02.2025).
4. Janssen H., Cobbe J., Norval C., Singh J. Decentralized data processing: personal data stores and the gdpr. *International Data Privacy Law*. 2020. Vol. 10. No. 4. P. 356—384.

https://doi.org/10.15407/akademperiodyka.545.015

БУРЛАЙ ТЕТЯНА
доктор економічних наук, доцент,
провідний науковий співробітник
відділу економічної теорії,
Державна установа «Інститут економіки та прогнозування
Національної академії наук України»,
м. Київ, Україна
https://orcid.org/0000-0003-4530-9151

СОЦІАЛЬНА СПРАВЕДЛИВІСТЬ ТА СОЦІАЛЬНІ ВИКЛИКИ У ХОДІ ЦИФРОВІЗАЦІЇ СУЧАСНИХ ЕКОНОМІК І СУСПІЛЬСТВ

Примітною особливістю сьогодення стало глобальне прискорення процесів цифровізації, яка передбачає створення, поширення, впровадження та використання цифрових і новітніх технологій, включаючи штучний інтелект (ШІ), технології віртуальної та доповненої реальності й інші. За оцінними даними, станом на початок 2025 р. до цифровізації та участі у різних цифрових ініціативах залучено понад 94 % фірм, установ і організацій у всіх секторах світової економіки. На вказану дату глобальні прямі інвестиції у цифрову трансформацію прогнозовано сягнуть 8,5 трлн дол. США, зростаючи протягом 2020—2024 рр. у середньому на 19 % щорічно.

Cite: Burlai Tetiana. Social justice and social challenges during digitalisation of modern economies and societies. https://doi.org/10.15407/akademperiodyka.545.015

Зрештою, це сприятиме тому, що за підсумками 2024 р. на охоплені цифровізацією бізнесові та інші структури припадатиме понад 55 % світового обсягу ВВП, тобто 60 трлн дол. США [15].

Цифровізація має двоїстий і суперечливий характер, створюючи як нові значні можливості, так і дуже серйозні ризики для соціально-економічного та суспільного розвитку. Це, зокрема, зазначає Світовий банк у своєму «Звіті про цифровий прогрес і тренди» за 2023 р., указавши, що цифровізація вирішальним чином впливає на вирішення інноваційними чи більш ефективними способами низки глобальних викликів, а саме: формування стійкості до зміни клімату; запобігання надзвичайним ситуаціям у сфері охорони здоров'я; гендерна та інших видів нерівність; готовність і реагування на надзвичайні ситуації; нестабільність, конфлікти та насильство. Водночас Світовий банк об'єктивно констатує, що зростаючий цифровий розрив загострює розрив у рівнях бідності та продуктивності між багатшими та біднішими економіками. У той час як 2022 р. у країнах з високим рівнем доходу інтернетом користувалися понад 90 % населення, у країнах з низьким рівнем доходу — лише 25 %. Цей та інші відповідні факти дали можливість дійти незаперечного висновку, що «без доступу до Інтернету та навичок ефективного використання цифрових технологій мільярди людей залишаються поза межами сучасного світу» [6]. Шанс змінити цю ситуацію, на думку Світового банку, дає форсування процесів цифровізації, яке інколи зумовлюється форс-мажорними обставинами. Так, пандемія COVID-19 призвела до безпрецедентного прискорення цифрової трансформації в усьому світі — з могутнім зростанням трафіку даних, використання застосунків, зростання ІТ-сектора, стійкості цифрового бізнесу, затребуваності ШІ тощо [6].

Прискорена динаміка та масштаби процесів цифровізації обумовили необхідність вироблення та імплементації спільного на глобальному рівні бачення щодо регулювання як самих процесів, так і їхніх довгострокових наслідків. Визнаючи

цю необхідність і беручи до уваги рішення Всесвітньої зустрічі на найвищому рівні з питань інформаційного суспільства (2003 і 2005 рр.), Генеральна Асамблея ООН своєю резолюцією від 22 вересня 2024 р. ухвалила Пакт в ім'я майбутнього, включаючи його додаток — Глобальний цифровий договір (Global Digital Compact). У цьому документі встановлено завдання, принципи, зобов'язання та дії, які взялася здійснити світова спільнота, маючи на меті забезпечити «інклюзивне, відкрите, стале, справедливе, безпечне та надійне цифрове майбутнє для всіх» у невійськовій сфері [8].

Декларуване у вказаному Договорі прагнення до справедливості передусім стосується її соціального виміру. Прямою відповіддю на необхідність подолання глобального дефіциту соціальної справедливості стало у листопаді 2023 р. створення Адміністративною радою МОП Глобальної коаліції за соціальну справедливість, що є «платформою для формування політичних зобов'язань, інвестицій і конкретних дій, які підтримують соціальну справедливість у відповідності з національними пріоритетами». Свою діяльність Коаліція будує згідно з такими першочерговими тематичними пріоритетами:

- подолання нерівності, дискримінації та відчуження;
- реалізація трудових прав як прав людини, забезпечення людської гідності та задоволення основних потреб;
- розширення доступу й можливостей для продуктивної та вільно обраної роботи і стійких підприємств;
- забезпечення соціального захисту та формування стійкості;
- зміцнення справедливого переходу і соціального виміру сталого розвитку, торгівлі та інвестицій;
- зміцнення інститутів соціального діалогу [3].

Вагомим внеском у Глобальну коаліцію за соціальну справедливість стало спільне проведення МОП та Європейським економічним і соціальним комітетом конференції високого рівня «Соціальна справедливість цифрової ери: вплив штучного інтелекту на працю та суспільство» у лютому 2025 р. У документах цього

заходу було підкреслено нагальну потребу в людиноцентричному підході до ШІ, який не повинен бути джерелом розколу чи ексклюзії, а бути рушієм можливостей, інновацій та справедливості, зокрема гендерної, у світі праці [10]. У даному контексті управлінцям особливу увагу слід приділяти ризикам і загрозам, генерованим у ході цифрової трансформації, що перешкоджають скороченню соціальної несправедливості, або й посилюють її.

Недарма у Глобальному цифровому договорі акцентовано, що цифрові та новітні технології, кардинально перетворюючи наш світ, дають дуже значні потенційні переваги для забезпечення добробуту й розвитку людей і суспільств, але разом із тим формують нові виклики [8]. Серед них одними з найсерйозніших є виклики соціального характеру.

Зважаючи на результати тематичних досліджень і враховуючи завдання, визначені, зокрема, Глобальним цифровим договором (2024), Європейською декларацією про цифрові права та принципи Цифрового десятиліття (2024), рекомендаціями Ради ОЕСР щодо управління ризиками цифрової безпеки для економічного та соціального процвітання (2015) і щодо штучного інтелекту (2017), а також дані звітів Адміністративної ради МОП (Робоча група з питань соціального виміру глобалізації) (2024) [4] та Всесвітнього економічного форуму (ВЕФ) (2025) [14], доцільно виокремити такі ключові соціальні виклики цифровізації сучасних економік і суспільств:

Загострення проблем зайнятості та розбалансування ринків праці. Дослідження Європейського фонду покращення умов життя та праці [7] обґрунтовує три головні вектори цифровізації з потенціалом фундаментальних технологічних і соціальних змін у сфері зайнятості: автоматизація праці, оцифрування економічних процесів (на основі таких трьох ключових технологій, як інтернет речей (IoT), 3D-друк, а також віртуальна та доповнена реальність) і цифрова платформізація. Саме ці вектори сьогодні визначають динаміку скорочення та створення робочих місць, проте експерти розходяться в прогнозах

щодо їхнього кінцевого впливу на кількісні й структурні зміни ринків праці. Так, у звіті ВЕФ за 2025 р. «Майбутнє робочих місць», за спільними з МОП оцінками, протягом 2025—2030 рр. під дією тренду цифровізації у світі може бути створено 170 млн робочих місць або, за еквівалентом повної зайнятості, 14 % їх глобальної кількості. У той же час буде скорочено 92 млн робочих місць (8 %), тобто щороку в середньому 18,4 млн [14]. Разом із тим за результатами дослідження Глобального інституту McKinsey [11], у період 2016—2030 рр. через цифровізацію, враховуючи ШІ та робототехніку, скорочення потенційно сягне від 400 до 800 млн робочих місць або від 28,6 до 57,1 млн щорічно. Вочевидь, інтенсивність впливу технологій на сферу зайнятості залежить від багатьох чинників, але одним із визначальних лишається ефективність національних стратегій цифровізації [13].

Необхідність трансформації освітніх систем і їх високої адаптації до потреб сучасних ринків праці. Набуття конкурентних переваг у цифровій економіці сьогодні значною мірою детермінується рівнем цифрових навичок і компетенцій її учасників. Саме тому, за оцінкою ВЕФ, інвестування у розвиток людського капіталу, у тому числі через програми безперервного навчання, підвищення кваліфікації та перекваліфікації робочої сили, а також цифрової грамотності населення, є пріоритетним завданням для національних урядів і бізнесу поряд із завданням синхронізації можливостей освітніх систем із потребами ринку праці. Зважаючи, що за 2025—2030 рр., імовірно, зміняться 39 % ключових навичок, на сьогодні необхідних для конкурентоспроможності на ринку праці, а наявність цифрових навичок у працівників стане першочерговою обов'язковою вимогою роботодавців. Так, за критерієм затребуваності ключових навичок на ринку праці у найближчі п'ять років, на трьох перших позиціях глобального рейтингу, складеного експертами ВЕФ, знаходяться: вміння застосовувати штучний інтелект (ШІ) та великі дані (Big Data); навички роботи з інформаційно-цифровими мережами й забезпечення кібербезпеки; технологічна грамотність [14].

З метою пом'якшення потенційних негативних наслідків цифровізації для національних ринків праці та сфери зайнятості, пріоритетним завданням урядів і бізнесу стає побудова ефективних систем професійної підготовки, підвищення кваліфікації та перепідготовки для працівників, охоплених видами діяльності, що зазнають впливу цифрових і новітніх технологій.

Прискорення процесів прекаризації суспільств внаслідок поширення платформної зайнятості та недосконалості (відсутності) її законодавчо-правового регулювання. Одним із джерел, генеруючих нині соціальні ризики, є стрімке — з часів поширення «коронакризи» у 2020 р. — масштабування зайнятості на цифрових платформах. За даними Світового банку, сьогодні на онлайнову платформну зайнятість припадає чимала та постійно зростаюча частка глобального ринку праці, що становить від 4,4 до 12,5 % світової робочої сили, тобто від 154 до 435 млн осіб [5]. Соціальна небезпека цих процесів полягає в тому, що платформи акумулюють різноманітні форми нестандартної зайнятості з надвисоким потенціалом прекарності, що й пояснює поширення низки ризиків, а саме: мінімізації соціального захисту платформних працівників і їх багатовимірної дискримінації; поширення їх вразливості щодо оплати, безпеки та інших умов праці; недоотримання державою та фондами соціального страхування податків, обов'язкових платежів і соціальних внесків; зниження фіскальної спроможності держави та зростання податкового тиску на офіційно працевлаштованих громадян. Хоча платформна економіка активно розвивається вже понад два десятиріччя, наразі переважна більшість країн світу перебуває лише на початковому етапі формування національної законодавчо-правової бази для регулювання платформної зайнятості та захисту соціально-трудових прав працівників цифрових платформ. Позаяк станом на березень 2025 р. в Україні така база практично відсутня, нагальним завданням є розробка вітчизняних актів законодавчо-правового регулювання платформної зайнятості, спрямованих на мінімізацію її прекаризаційного потенціалу [1; 12].

Посилення цифрової та соціальної нерівності через обмежений доступ до цифрових суспільних благ і цифрової суспільної інфраструктури. У 2024 р. Генеральною Асамблеєю ООН до переліку цифрових суспільних благ було віднесено: програмне забезпечення з відкритим вихідним кодом; відкриті дані; відкриті моделі ШІ; відкриті стандарти; відкритий контент, за умови, що вони відповідатимуть нормам конфіденційності та іншим застосовним міжнародним законам, стандартам і передовій практиці, а також не завдадуть шкоди в галузі сталого розвитку й зможуть сприяти здійсненню співробітництва та інвестицій у цифровій сфері [8]. За відсутності чи обмеженості доступу громадян, бізнесу, інституцій тощо до вказаних цифрових суспільних благ та цифрової суспільної інфраструктури зростають «цифрові розриви», що веде до посилення цифрової та соціальної нерівності.

Загострення проблем безпеки у цифровому середовищі (кібербезпеки) — ще один із нових соціальних викликів, обумовлених цифровізацією. З метою їх вирішення в частині забезпечення людської (персональної) кібербезпеки, Глобальним цифровим договором передбачено на рівні національних і міжнародних структур протидіяти всім формам насильства, включаючи сексуальне та гендерне, яке вчиняється з використанням цифрових технологій або посилюється внаслідок їх застосування, всім формам ненависницьких висловлювань і дискримінації, поширення хибної інформації та дезінформації, цькування в інтернеті тощо. Також передбачено розробку та реалізацію надійних заходів щодо зменшення ризиків, забезпечення захисту конфіденційності й свободи вираження поглядів у кіберпросторі.

Посилення загроз, що пов'язані з соціалізацією людини та потенційно ведуть до її соціальної деструкції. До таких загроз належать: відмова від соціальних відносин чи спільнот — наслідком стає соціальна ексклюзія; заміна соціальних відносин чи спільнот менш цінними альтернативами; деградація

соціальних відносин унаслідок використання інтернету, соціальних мереж, що проявляється у соціальній ізоляції, збідненому спілкуванні, безкультур'ї та агресивності, зловмисній соціальній поведінці в цифровому просторі (кіберпереслідування, кібердомагання, кіберзалякування тощо) [2].

Резюмуючи, зазначимо, що у цифрову епоху важливим завданням для міжнародних структур і національних урядів є сприяння посиленню соціальної справедливості та ефективне реагування на соціальні виклики цифровізації економік і суспільств. Дієвим підґрунтям для формування необхідних регуляторних механізмів, зокрема, можуть стати розроблені ОЕСР Рамкові основи впровадження цифрової інтегрованої політики (2020), у яких вміщено сім взаємопов'язаних напрямів дій: 1) доступ до комунікаційної інфраструктури, послуг і даних; 2) ефективне використання цифрових технологій і даних; 3) цифрові інновації та інновації, керовані даними; 4) гідна робота для всіх; 5) соціальне процвітання та інклюзія; 6) довіра до цифрової епохи; 7) відкритість ринку в цифровому бізнес-середовищі [9]. У випадку країн, що охоплені повномасштабною війною, зокрема України, і постконфліктних країн, зазначені вище підходи мають коригуватися з урахуванням відповідно реалій воєнного стану та завдань повоєнного відновлення.

ЛІТЕРАТУРА

1. Близнюк В.В., Бурлай Т.В., Гук Л.П. Законодавчо-правове регулювання платформної зайнятості у контексті соціальної стійкості держави. *Економічна теорія*. 2024. № 4. С. 49—84. https://doi.org/10.15407/etet2024.04.049
2. Гриценко А.А., Бурлай Т.В. Вплив цифровізації на соціальний розвиток. *Економічна теорія*. 2020. № 3. С. 24—51. https://doi.org/10.15407/etet2020.03.024
3. Advancing social justice for everyone, everywhere. *Global Coalition for Social Justice*. 2024. URL: https://social-justice-coalition.ilo.org/ (дата звернення: 03.02.2025).

4. Challenges and Opportunities of Digitalization. ILO Governing Body, 350th session — High-Level Section. *ILO*. 2024. March. 13 p. URL: https://www.ilo.org/resource/gb/350/challenges-and-opportunities-digitalization-0 (дата звернення: 03.02.2025).
5. Datta N., Chen R., et al. Working without Borders: The Promise and Peril of Online Gig Work. *World Bank*. 2023. 301 p. URL: https://openknowledge.worldbank.org/handle/10986/40066 (дата звернення: 03.02.2025).
6. Digital Progress and Trends Report 2023. *World Bank*. 2024. March. 149 p. URL: https://openknowledge.worldbank.org/handle/10986/40970 (дата звернення: 03.02.2025).
7. Fernández-Macías E. Automation, Digitisation and Platforms: Implications for Work and Employment. *Eurofound*. 2018. 26 p. https://doi.org/10.2806/090974
8. Global Digital Compact: An Open, Safe & Secure Digital Future for All. *United Nations Office for Digital and Emerging Technologies*. 2024. URL: https://www.un.org/digital-emerging-technologies/content/gdc-resources (дата звернення: 03.02.2025).
9. Going Digital Integrated Policy Framework. *OECD Digital Economy Papers*. 2020. No. 292. 66 p. https://doi.org/10.1787/dc930adc-en
10. ILO and EESC join forces to shape a fair and inclusive AI-driven future at high-level conference. *ILO.* 2025. February 3. URL: https://www.ilo.org/resource/news/ilo-and-eesc-join-forces-shape-fair-and-inclusive-ai-driven-future-high (дата звернення: 03.02.2025).
11. Jobs Lost, Jobs Gained: Workforce Transitions in a Time of Automation. *McKinsey Global Institute*. 2017. December. 148 p. URL: www.mckinsey.com/mgi (дата звернення: 03.02.2025).
12. Kolot A., Herasymenko O., Shevchenko A., Ryabokon I. Employment in the Coordinates of Digital Economy: Current Trends and Foresight Trajectories. *Neuro-Fuzzy Modeling Techniques in Economics*. 2022. No. 11. P. 78—123. http://doi.org/10.33111/nfmte.2022.078
13. OECD Digital Economy Outlook 2024 (Vol. 2): Strengthening Connectivity, Innovation and Trust. *OECD*. 2024. 220 p. https://doi.org/10.1787/3adf705b-en
14. The Future of Jobs Report 2025. *World Economic Forum*. 2025. January. 289 p. URL: https://www.weforum.org/reports/the-future-of-jobs-report-2025/ (дата звернення: 03.02.2025).
15. Top 10 Digital Transformation Trends for 2025 and Further. *Veritis Group Inc. [*2025. URL: https://www.veritis.com/blog/top-10-digital-transformation-trends/ (дата звернення: 03.02.2025).

https://doi.org/10.15407/akademperiodyka.545.024

ДМИТРЕНКО ТЕТЯНА
кандидат економічних наук, старший дослідник,
завідувач відділу міжнародних фінансів та фінансової безпеки відділення глобальної економіки і міжнародних фінансів,
НДФІ ДННУ «Академія фінансового управління»
м. Київ, Україна

ВОЛКОВА ВАЛЕРІЯ
аспірант, НДФІ ДННУ «Академія фінансового управління»
м. Київ, Україна

РЕГУЛЯТОРНИЙ ПІДХІД ДО ОЦІНКИ ТА УПРАВЛІННЯ РИЗИКАМИ ВИКОРИСТАННЯ DeFi В ЛЕГАЛІЗАЦІЙНИХ ОПЕРАЦІЯХ ЩОДО ВІДМИВАННЯ КОШТІВ, ОТРИМАНИХ ЗЛОЧИННИМ ШЛЯХОМ

Децентралізовані фінанси (DeFi) надають необмежені можливості для розвитку фінансових послуг у публічних блокчейнах без необхідності отримання дозволу та з використанням смартконтрактів. Однак це створює певні проблеми для регуляторних органів у боротьбі з певними викликами: забезпеченням захисту споживачів, фінансовою стабільністю та запобіганню незаконним діям, таким як відмивання грошей.

Cite: Dmytrenko Tetiana, Volkova Valeria. Regulatory approach to assessment and management of the risks of using DeFi in legalisation operations related to money laundering, obtained by criminal means. https://doi.org/10.15407/akademperiodyka.545.024

Міжнародні організації — Міжнародний валютний фонд (МВФ) [3] і Група розробки фінансових заходів протидії відмиванню грошей (FATF) [2] — відіграють важливу роль у встановленні глобальних стандартів щодо регулювання криптоактивів. Вони надають комплексні рекомендації, щоб зменшити ризики відмивання грошей та фінансування тероризму (ПВК/ФТ).

Функціональний підхід FATF до регулювання сфери віртуальних активів зосереджений на діяльності компаній та платформ постачальників послуг, пов'язаних з оборотом віртуальних активів (ППВА) залежно від наданих ними послуг, а не їхньою технологічною реалізацією. Тобто, якщо сервіс виконує функції, що відповідають визначенню ППВА, він зобов'язаний дотримуватися стандартів ПВК/ФТ [4].

У жовтні 2021 р. FATF вперше включила DeFi у свої рекомендації для регулювання діяльності ППВА, наголошуючи на необхідності регулювання цього сектора [4].

Керівництво FATF розглядало можливість віднесення децентралізованих додатків (DApps), їхніх власників, операторів/розробників до категорій ППВА в тому випадку, якщо вони сприяють або фактично обмінюють чи переказують цифрові активи. Проте дане роз'яснення викликало багато обговорень серед державних регуляторів і безпосередньо учасників ринку.

У новому керівництві FATF «Міжнародні стандарти боротьби з відмиванням коштів та фінансуванням тероризму» розширено підхід до визначення децентралізованих фінансових послуг (DeFi) та їх регулювання. Особливу увагу зосереджено на визначенні відмінностей між децентралізованими серверклієнтськими додатками (DApps) і фізичними та юридичними особами, що належать або управляють фінансовими послугами через ці додатки [1].

Відповідно до положень Керівництва FATF розробники або оператори DeFi-платформ, які класифікуються як ППВА, повинні відповідати вимогам щодо комплаєнсу, зокрема політики «Знай свого клієнта» (англ. Know you client, (KYC)), і

процедур ПВК/ФТ. Децентралізовані автономні організації управління DeFi-протоколами можуть попасти під регулювання в разі наявності достатнього контролю або впливу на ці протоколи. Встановлені протоколи, які повністю функціонують автономно, без постійного контролю та втручання з боку розробників або операторів, з меншою вірогідністю підпадуть під визначення ППВА. В іншому випадку, можуть нести відповідальність за зберігання контролю після його запуску.

Аналізуючи зростаючу роль DeFi та їх інтеграцію в діяльність традиційних фінансових ринків, яка розглядається у звіті Організації економічного співробітництва та розвитку (ОЕСР) від 19 січня 2022 р. «Чому децентралізовані фінанси (DeFi) важливі та які це має політичні наслідки» [8], можна зробити висновок, що водночас DeFi має такі безумовні переваги у сфері розвитку інновацій та фінансової інклюзії, з іншого боку, беруться до уваги ризики використання DeFi технологій, зокрема відсутність регулювання, що є загрозою в діяльності фінансового ринку. ОЕСР акцентує увагу на розробці політик, які поєднують стимулювання інновацій із заходами безпеки.

Звіт Банку міжнародних розрахунків (BIS) свідчить про стрімке зростання вартості криптоактивів у DeFi-додатках на блокчейні Ethereum: з менш ніж 2 млд доларів у липні 2020 р. до 100 млд доларів у листопаді 2021 р., що демонструє 50-кратне збільшення їхньої капіталізації. [6] Це, безумовно, свідчить про те, що DeFi є значним сегментом фінансового ринку, перспективною сферою його діяльності та, враховуючи виклики, пов'язані з безпекою та управлінням ризиками, потребує більш ретельної уваги з боку державних регуляторів.

Також у звіті BIS зазначено, що платформи та додатки DeFi створюють низку ризиків, які притаманні самій технології розподіленого реєстру (DLT), інші — через інновації в архітектурі й роботі таких платформ і додатків. Слід зауважити, що поставлений і акцент на волатильності цін на криптоактиви, що посилює вразливість ринку DeFi до використання його в

злочинних цілях. Так, у 2021 р. із DeFi-протоколів було втрачено близько 1,4 млд доларів через комп'ютерні програми (експлойти) та помилки у смартконтрактах. Тому посилення заходів безпеки, впровадження аудиту смартконтрактів для зменшення ризиків є актуальними й необхідними кроками в розвитку прозорої діяльності DeFi.

Враховуючи посилення глобалізації діяльності DeFi, OECD та BIS підкреслюють важливість міжнародного співробітництва й визначення юрисдикцій розробки та здійснення діяльності цих платформ і додатків для забезпечення ефективного контролю над DeFi. Звіти вказують на те, що потрібно залучити розробників програмного забезпечення до обговорення створення регуляторних політик, як і регуляторний контроль архітектури DLT-систем. Також іхні рекомендації спрямовані на усунення нормативних прогалин і мінімізацію транскордонного регуляторного арбітражу за допомогою узгодженої політики стандартів та співпраці.

Регламент MiCA [5] стосується переважно централізованих платформ у криптовалютній індустрії, а щодо DeFi — то його вплив обмежений. У поточній версії MiCA децентралізовані фінанси не входять у сферу державного регулювання, але розробники та оператори DeFi-платформ можуть підпадати під регулювання, якщо вони контролюють відповідні протоколи або надають відповідні фінансові послуги.

Основні аспекти розширення сфери регулювання MiCA для DeFi — розробка вимог щодо прозорості та звітності платформ, які можуть діяти як ППВА, регуляція обігу стейблкоїнів (вплив на DeFi-протоколи, що інтегрують стейблкоїни). Засади, розкриті в MiCA, створюють базу для можливості подальшого дослідження у сфері регуляції DeFi та передбачають моніторинг DeFi для оцінки ризиків і можливого впровадження регулювання ними у майбутньому.

Враховуючи те, що багато DeFi-платформ усе-таки керуються за допомогою автономних організацій (DAO), виникають

складнощі в ідентифікації та визначенні відповідальних осіб, що впливає на процес розробки ефективних регуляторних механізмів. Швидкий темп розвитку й нові фінансові продукти ускладнюють розробку та прийняття ефективних регуляторних механізмів.

В опублікованому документі Міжнародний валютний фонд (МВФ) «Віртуальні активи та боротьба з відмиванням грошей і фінансуванням тероризму: деякі юридичні та практичні міркування» [3] зосереджується увага на ризиках використання фінансових технологій у відмиванні грошей, фінансуванні тероризму і розповсюдженні зброї масового ураження [7]. Документ охоплює юридичні та операційні аспекти, спрямовані на посилення регуляторного нагляду.

Для гарантування дотримання вимог ПВК/ФТ у цифрових середовищах, таких як DeFi, необхідно впровадити ефективні регуляторні рішення: зокрема, використання блокчейну — для надання безпечної та прозорої перевірки особи; запис транзакцій у DLT-реєстр — для підвищення прозорості діяльності учасників DeFi; запобігання шахрайству, партнерства між платформами, регуляторами та експертами — для розробки стандартів саморегулювання і обміну інформацією.

Регулювання в галузі DeFi є необхідним для вирішення питань правового захисту учасників ринку. Без належного контролю в умовах відсутності юридичного захисту конфлікти між учасниками цих платформ є складними для врегулювання.

Загалом DeFi може підвищити ефективність діяльності фінансової системи за умови його сталого розвитку та впровадження відповідних регуляторних заходів. Доказом цього є оновлення керівництв FATF щодо діяльності ППВА шляхом розширення стандартів ПКВ/ФТ на сферу децентралізованих фінансів. Важливим кроком до розвитку діяльності DeFi у глобальній фінансовій системі є урахування унікальних характеристик DeFi та з збереження балансу між інноваціями й регуляторними вимогами.

ЛІТЕРАТУРА

1. Міжнародні стандарти щодо боротьби з відмиванням коштів, фінансуванням тероризму та розповсюдження зброї масового знищення. *Рекомендації FATF. Держфінмоніторинг*. 2023. Листоп. URL: https://surl.li/xaufgb (дата звернення: 23.01.2025).
2. Можливості та виклики нових технологій для ПВК/ФТ. *FATF*. 2021. Лип. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/translations/guidance/Ukranian-Opportunities-Challenges-New-Technologies-AML-CFT.pdf (дата звернення: 23.01.2025).
3. Хуторна М., Ткаченко. Ю. Світові моделі регулювання цифрових валют і сучасні ініціативи центральних банків. *Socio-Economic Relations in the Digital Society*. 2021. Т. 1, № 40. С. 42—49. https://doi.org/10.18371/2221-755X1(40)2021237578
4. Guidance for a Risk-Based Approach for VirtualAssets and Virtual Asset Service Providers. *FATF*. 2021. URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf (дата звернення: 23.01.2025).
5. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) N 1093/2010 and (EU) N 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance). *EUR-Lex*. URL: https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng (дата звернення: 23.01.2025).
6. The Technology of Decentralized Finance (DeFi). *BIS Working Papers*. No. 1066. 2023. URL: https://www.bis.org/publ/work1066.pdf (дата звернення: 23.01.2025).
7. Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism: Some Legal and Practical Considerations. *IMF, Fintech notes*. 2021. October 14. URL: https://www.imf.org/en/Publications/fintech-notes/Issues/2021/10/14/Virtual-Assets-and-Anti-Money-Laundering-and-Combating-the-Financing-of-Terrorism-1-463654 (дата звернення: 23.01.2025).
8. Why Decentralised Finance (DeFi) Matters and the Policy Implications. *OECD*. URL: https://www.oecd.org/en/publications/why-decentralised-finance-defi-matters-and-the-policy-implications_109084ae-en.html?utm (дата звернення: 23.01.2025).

https://doi.org/10.15407/akademperiodyka.545.030

ZHDANKINA LARYSA
Doctor of the University of Glasgow,
Scotland, UK
https://orcid.org/0000-0002-8215-7815

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON HUMAN RIGHTS: A FOCUS ON DIGNITY

Introduction. In the era of quick technological expansion, artificial intelligence (hereinafter AI) has emerged as a transformative force, reshaping social, economic, and political landscapes. While AI-driven innovations hold immense potential to enhance efficiency and progress, they also challenge fundamental human rights, particularly equality and human dignity. Human rights protection is a cornerstone of international law, rooted in the recognition that every human being, regardless of nationality, socioeconomic status, or geographical location, deserves to be treated with fairness, respect, and autonomy. However, as AI systems become increasingly embedded in decision-making processes, concerns regarding algorithmic bias, data privacy, and the undermining of human agency have intensified, notably in the developing world, where regulatory frameworks and digital literacy may be less robust.

At the heart of global legal and ethical discourse lies the principle that, on the one hand, human beings must remain the central focus of technological progress, and

Cite: Zhdankina Larysa. The impact of artificial intelligence on human rights: a focus on dignity. https://doi.org/10.15407/akademperiodyka.545.030

on the other hand, AI should serve humanity rather than dictate the conditions of human existence. Moreover, in spheres such as access to employment, social services, or justice, the risk of AI-driven discrimination raises pressing concerns about the aggravation of existing inequalities. Vulnerable populations, mostly in regions with limited institutional safeguards, face a high risk of being sidelined if AI is deployed without adequate oversight or human-centred design principles. Moreover, the necessity of ensuring that individuals are not only protected from potential abuses of AI but also equipped with the knowledge and legal mechanisms to navigate this growing landscape is crucial.

The explosion of AI technologies presents profound implications for the protection and enrichment of fundamental human rights. This article examines the dialectical relationship between AI and human rights, such as equality and human dignity, as foundational principles within international human rights law. The analysis compares the potential of these technologies against their capacity to establish or intensify existing inequalities, contextualising this discussion within the evolving international legal framework. Through a critical analysis of this technological paradigm shift, this article argues for a rights-based approach to AI governance that prioritises human dignity and equality as unshakeable principles.

Human Dignity as a Cornerstone of Human Rights in the Age of AI. Human dignity is an essential characteristic of every individual and a fundamental value that must be protected. The Universal Declaration of Human Rights (hereinafter UDHR) (1948) [19] explicitly affirms this principle in Articles 1 and 5, stating that "all human beings are born free and equal in dignity and rights," gifted with reason and conscience, and should act towards one another in a spirit of brotherhood. Furthermore, it establishes a categorical prohibition against torture and cruel, inhuman, or degrading treatment or punishment, reinforcing the inviolability of human dignity.

The worth of dignity as a legal and ethical imperative has been further articulated in international human rights instruments. It is needed to stress that the International Covenant on Civil and Political

Rights (hereinafter ICCPR) (1966) [13] in Articles 7 and 10 prohibits torture and cruel, inhuman, or degrading treatment and mandates that all persons deprived of liberty be treated with humanity and with respect for the inherent dignity of the human person. Similarly, the Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (1984) [6] and the European Convention on Human Rights (hereinafter ECHR) (1950) [10] both enshrine human dignity as a protected principle, recognising that any violation of dignity constitutes an assault on the fundamental values of democratic societies.

The United Nations Charter (1945) [17], alongside the prohibition of ill-treatment, underscores the broader role of dignity in shaping global legal and political order. In essence, the Preamble explicitly commits member states "to reaffirm faith in fundamental human rights, in the dignity and worth of the human person, in the equal rights of men and women and of nations large and small." This commitment extends beyond the protection of individuals to the foundation of international relations, ensuring that human dignity remains a guiding principle in governance, diplomacy, and global justice.

In addition, the European Court of Human Rights (hereinafter ECtHR) has reinforced this understanding, consistently interpreting human dignity as a foundational right that underpins all other rights and freedoms enshrined in the ECHR. The Court has held that respect for human dignity and freedom forms the essence of the Convention, emphasising the principle of inviolability of human dignity, even when rights are subject to lawful limitations [15]. Taking into account the above, jurisprudence of the ECtHR has demonstrated that national restrictions on individual rights must always be assessed through the lens of dignity, ensuring that state actions do not undermine the intrinsic worth of the individual [7].

It is worth mentioning that, following Article 1 of the Charter of Fundamental Rights of the European Union (2000) [5], "Human dignity is inviolable. It must be respected and protected." It places dignity at the core of its legal framework. Furthermore, in the broader

European legal order, the principle of dignity has played a crucial role in the gradual development of a unified constitutional tradition.

Consequently, common constitutional values — including human dignity, human rights, and the rule of law — serve as the foundation for democratic governance and legal harmonisation across Europe. This approach aligns with the general European concept of freedom and democracy, which has been progressively shaped by shared constitutional traditions emphasising the primacy of the individual in legal and political structures.

AI and the Challenge to Human Dignity. Alongside the acceleration of technological innovations, new challenges arise concerning the preservation of human dignity in digital and automated environments. Human beings exist in a social framework where they contribute to and benefit from societal progress, expecting reciprocal guarantees for their protection and well-being. While fundamental aspects of human life remain constant, cutting-edge technologies introduce new ethical and legal dilemmas that require meticulous rethinking and careful scrutiny to prevent the undermining of dignity.

From the philosophical foundations of Aristotle and Platon to the theological doctrines of Augustine, John Chrysostom, and Thomas Aquinas, dignity has evolved into a well-defined legal and moral concept. The Renaissance and Reformation further reinforced the recognition of human worth, providing the intellectual basis for the ideas of Hobbes, Locke, Grotius, Montesquieu, and Rousseau, who viewed dignity as intrinsic to human existence. These historical developments laid the groundwork for the modern legal recognition of dignity, emphasising that states must view individuals not merely as instruments of policy but as autonomous beings with inherent worth [2].

In this context, AI-driven decision-making systems present a dual challenge: (1) while they offer vast opportunities for innovation, they also (2) risk depreciating fundamental human rights by reinforcing inequality, enabling intrusive surveillance, and reducing individuals to mere data points in algorithmic processes. A purely instrumentalist approach to AI, where human beings are seen as objects of analysis

rather than subjects of rights, might lead to contradicting the core international law principles. Therefore, AI must be governed by ethical and legal frameworks, simultaneously prioritising human dignity, ensuring that technological progress does not come at the expense of fundamental freedoms.

The recognition of dignity in international law must be operationalised via concrete legal and social mechanisms. Merely defining dignity as a legal principle is insufficient. It requires robust mechanisms to prevent AI-driven violations, such as discriminatory algorithms, biased decision-making systems, and the commodification of personal data. Furthermore, key areas of concern have to be reviewed. Firstly, AI must be designed and implemented in a way that prevents racial, gender, and socioeconomic biases, ensuring equality in access to opportunities and resources. Secondly, AI must respect individuals' right to control their personal data, aligning with the General Data Protection Regulation (hereinafter GDPR) [11; 19] and other privacy laws. Thirdly, Legal frameworks must mandate clear decision-making processes in AI systems, ensuring individuals can challenge unfair or harmful outcomes. Finally, human rights impact assessments must be integrated into AI research and deployment, ensuring alignment with dignity-centred legal principles.

The Connection Between AI and Human Rights. AI offers unprecedented opportunities for advancing human rights through enhanced access to fundamental services and greater societal equity.

Firstly, when deployed with appropriate safeguards, AI systems can serve as powerful instruments for realising rights enshrined in the Universal Declaration of Human Rights (hereinafter UDHR) [19]. These technologies demonstrate certain promise in expanding access to essential services in healthcare, education, and legal assistance, thereby advancing the right to "a standard of living adequate for health and well-being" under Article 25 of the UDHR [19].

Moreover, properly calibrated algorithmic systems hold the potential to mitigate human biases that have historically undermined the principle of equality. Contrasting human decision-makers, AI

systems can be rigorously tested, audited, and continuously improved in order to minimise discriminatory outcomes. This capacity aligns with the United Nations Recommendations on the Ethics of Artificial Intelligence (2021), which stipulates that such systems must be "designed in a way that respects, protects and promotes human rights and fundamental freedoms" [18, p. 7]. In addition, the empowerment of marginalised communities represents another dimension of AI's emancipatory potential. Translation technologies that transcend linguistic barriers, assistive technologies that enhance accessibility for persons with disabilities, and data analytics that illuminate patterns of systemic discrimination collectively contribute to the realisation of Articles 19 and 27 of the UDHR, which protect freedom of expression and the right to participate in cultural life, respectively.

Secondly, despite these promising applications, the deployment of AI technologies raises significant human rights concerns. Algorithmic systems trained on historically biased data frequently reproduce and amplify existing social inequalities, constituting a direct contravention of Article 7 of the UDHR, which establishes equality before the law and equal protection against discrimination. Empirical evidence demonstrates that facial recognition systems exhibit significantly higher error rates for women and people with darker skin [3], while recruitment algorithms have been documented to systematically disadvantage certain demographic groups [9].

There is no doubt that the expansion of AI-enabled surveillance capabilities poses a substantial threat to the right to privacy enshrined in Article 12 of the UDHR and Article 8 of the European Convention on Human Rights [10]. The incorporation of facial recognition technologies in public spaces, predictive policing methodologies, and social scoring systems creates unprecedented environments of continuous monitoring that fundamentally undermine human dignity by violating autonomy and generating inadequate reactions to protected expression.

Furthermore, the opaqueness that characterises many AI systems — commonly referred to as the "black box" problem — raises

profound questions of procedural justice. The inscrutability of algorithmic decision-making processes contravenes the right to a fair and public hearing articulated in Article 10 of the UDHR by precluding individuals from effectively challenging determinations that affect their fundamental rights. The UN General Assembly resolution on rights and digital innovation (2021) addresses this concern, emphasising the necessity of explainability in AI systems that impact human rights.

Thirdly, the international community has increasingly recognised the necessity for specialised normative frameworks to address the human rights implications of AI technologies. Interestingly, the UNESCO Recommendation on the Ethics of Artificial Intelligence (2021) [18] represents the first global normative instrument in this domain, which contributes to establishing principles for ensuring that AI technologies advance human flourishing. These paramount provisions explicitly refer to human dignity and equality as unwavering values.

Furthermore, the European Union's proposed Artificial Intelligence Act [2] stipulates the most comprehensive regulatory framework for AI governance globally, adopting a risk-based approach that imposes tiered obligations based on an AI system's potential to adversely impact fundamental rights. This legislative initiative establishes stringent requirements for high-stakes applications, including robust documentation, transparency, and human oversight provisions.

Another crucial thing that should be mentioned is that the Council of Europe's modernised Convention 108+ [14] extends traditional data protection principles to address contemporary challenges posed by automated processing and algorithmic decision-making. Concurrently, the UN Guiding Principles on Business and Human Rights [16] establish that technology companies bear responsibility for respecting human rights and providing remedies for harmful impacts resulting from their operations.

Towards Rights-Based AI Governance. The necessity for rights-based AI governance has never been more noticeable. Given that these technologies continue to convert fundamental aspects of

social, economic, and political life, regulatory frameworks must centre human dignity and equality as non-negotiable principles. This requires a multifaceted approach involving robust legal protections, technical safeguards, and institutional oversight mechanisms.

First, legislative frameworks must establish clear boundaries regarding permissible applications of AI technologies, with particular scrutiny applied to high-stakes areas where fundamental rights may be jeopardised. This should (1) mandate algorithmic impact assessments before deployment, (2) establish meaningful transparency requirements, and (3) ensure effective remedies for rights violations.

Second, technical standards must evolve to embed human rights considerations throughout the AI extension growth. This includes (1) diverse and representative training data, (2) rigorous testing for discriminatory impacts, and (3) explainable architectures that facilitate meaningful human oversight and contestability.

Finally, institutional mechanisms must be strengthened to provide effective, meticulous control and enforcement. This includes (1) specialised regulatory bodies with appropriate technical expertise, (2) robust civil society participation, and (3) judicial capacity to adjudicate complex cases involving algorithmic harm.

Conclusion. The relationship between artificial intelligence and human rights presents one of the essential challenges of our era. While these technologies offer unprecedented opportunities to advance human dignity and equality, they simultaneously introduce novel threats to these fundamental principles. International legal frameworks have begun to address these challenges, though substantial gaps remain.

Although we navigate this technological transformation, we must insist upon governance frameworks that prioritise human flourishing above technical innovation for its own sake. The principles enshrined in international human rights law — notably equality and human dignity — must serve as non-negotiable foundations for AI development and deployment. Only through this rights-based approach can we harness the potential of AI while mitigating its capacity to undermine the very rights it might otherwise advance.

Human dignity, as recognised in international law and philosophical tradition, is not only a legal norm but a fundamental pillar of a democratic society. In the face of AI's rapid expansion, the legal system must guarantee the respect of dignity and inviolability. The processes of implementation and application of AI must reflect the principles embedded in the UDHR, ICCPR, ECHR, and the UN Charter, reinforcing the ECtHR's practice on the primacy of dignity. By implementing strong legal and ethical safeguards, societies can ensure that AI serves as a tool for human progress rather than a mechanism for exploitation and control. The ongoing challenge lies in balancing innovation with fundamental rights, ensuring that technological development correlates with the core values that define humanity itself.

REFERENCES

1. Yurovska H., Zhdankina L. Human Dignity and Gender Equality: Constitutional Metamorphoses. *Bulletin of the Constitutional Court of Ukraine*. 2021. No. 1. P. 103–119.
2. Artificial Intelligence Act. URL: https://artificialintelligenceact.eu/the-act/ (last accessed: 27.01.2025).
3. Buolamwini J., Gebru T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research*. 2018. Vol. 81. P. 77—91. URL: https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf (last accessed: 27.01.2025).
4. Buyse A. The Role of Human Dignity in the ECHR Case-Law. *ECHR Blog*. 2016. URL: http://echrblog.blogspot.com/2016/10/the-role-of-human-dignity-in-echr-case.html (last accessed: 27.01.2025).
5. Charter of Fundamental Rights of the European Union. 2000. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT (last accessed: 27.01.2025).
6. Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment. 1984. URL: https://legal.un.org/avl/ha/catcidtp/catcidtp.html (last accessed: 27.01.2025).
7. Costa J.-P. Human Dignity in the Jurisprudence of the European Court of Human Rights; ed. C. McCrudden. *Understanding Human Dignity*. Oxford: Oxford University Press, 2013. P. 393—402.

8. Council of Europe Framework Convention on Artificial Intelligence and Human Rights. *Democracy and the Rule of Law*. 2024. URL: https://rm.coe.int/1680afae3c (last accessed: 27.01.2025).
9. Dastin J. Amazon Scraps Secret AI Recruiting Tool That Showed Bias against Women. *Reuters.* 2018. URL: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-womenidUSKCN1MK08G (last accessed: 27.01.2025).
10. European Convention on Human Rights (ECHR). 1950. URL: https://www.echr.coe.int/documents/d/echr/convention_ENG (last accessed: 27.01.2025).
11. General Data Protection Regulation (GDPR). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (last accessed: 27.01.2025).
12. Becchi P., Mathis K. Human Dignity and the European Convention on Human Rights. *Handbook of Human Dignity in Europe*. Springer Nature Switzerland AG, 2019.
13. International Covenant on Civil and Political Rights (ICCPR). 1966. URL: https://treaties.un.org/doc/treaties/1976/03/19760323%2006-17%20am/ch_iv_04.pdf (last accessed: 27.01.2025).
14. Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data. 2018. URL: https://www.coe.int/en/web/data-protection/convention108/modernised (last accessed: 27.01.2025).
15. Schwichow von L. Die Menschenwürde in der EMRK [Human Dignity in the ECHR]; ed. W. Marauhn. *Jus Internationale et Europaeum*. Mohr Siebeck; Tübingen, 2016. Vol. 123.
16. UN Guiding Principles on Business and Human Rights. 2011. URL: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf (last accessed: 27.01.2025).
17. United Nations Charter. 1945. URL: https://www.un.org/en/about-us/un-charter (last accessed: 27.01.2025).
18. United Nations Recommendations on the Ethics of Artificial Intelligence. 2021. URL: https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence (last accessed: 27.01.2025).
19. Universal Declaration of Human Rights (UDHR). 1948. URL: https://www.un.org/en/about-us/universal-declaration-of-human-rights (last accessed: 27.01.2025).

https://doi.org/10.15407/akademperiodyka.545.040

IVANOVA ROKSOLANA
Associate Professor, Candidate of Legal Sciences,
Professor of the Department
of International and European Law,
Leonid Yuzkov Khmelnytskyi University
of Management and Law
Khmelnytskyi, Ukraine
https://orcid.org/ 0000-0001-8257-4486

THE CONTRIBUTION OF INTERNATIONAL ORGANIZATIONS IN THE FINANCIAL LEGAL FRAMEWORK OF UKRAINE AND THE DIGITAL FINANCIAL GOVERNANCE

The purpose of this research is to analyze the activity of Intl. organizations in Ukraine and the financial legal relations concerning its methodological foundations, doctrinal implications, and legal consequences. The paper deals with the classification of the legal entity and the impact of some intergovernmental and non-governmental financial organizations on the drafting of financial law in Ukraine. Also covered is the emergence of blockchain technology, DeFi, and AI regulation in digital finance law and their consequences on the law of finance.

The legal system of Ukraine should grant revenue-producing institutions within intergovernmental organizations special standing and importance as part

Cite: Ivanova Roksolana. The contribution of international organizations in the financial legal framework of Ukraine and the digital financial governance. https://doi.org/10.15407/akademperiodyka.545.040

of the Ukraine's financial legal system. The research studies the contribution of those intl. organizations in financial, budgetary, tax, customs, and banking structures and processes and their relations with citizens and legal entities of Ukraine. In addition, it studies other phenomena resulting from the broad use of financial technologies based on blockchain and AI.

Methodological Approaches To Financial Law Relations With International Institutions. International law of finance is studied from the perspective of international financial relations development and its taxonomy. The studied subjects include particularities of international financial legal relations, the international treaties, and the arbitration awards as sources of law. Moreover, the paper discusses the phenomenon of emergence of the so called hyperdecentralized finance, "smart" contracts, and the relations of these systems with international financial law.

The Contribution of International Organizations To Financial Law Relations And Digital Currencies. It provides an intergovernmental and nongovernmental international financial organization taxonomy, transnational corporations and international regional economic organizations. The research focuses on the international legal personality of these organizations and their impacts on global financial governance. The FATA and EBA's roles in forming rules for blockchain-based financial transactions and decentralized finance are under scrutiny.

Action by International Bodies in International Budgetary, Taxation and Digital Financial Relations. The budgetary legal relations of countries receives a noticeable attention from international organizations when it comes to the development of legal instruments such as policies and their budgets. The Europe's Council, UNESCO, WHO, and UNICEF are noteworthy programs and policies and policy instruments which aid in the financial management of countries. For instance, WTO, UNCTAD and other regional organizations also influence border economic activities by setting trade and customs policies which are Aids Ukraine's investment in

economic policies. The research also addresses the emerging issues of tax compliance and transparency through blockchain technology and associated challenges regulations as barriers.

Financial-Control, Regulation of the Blockchain and Banking Relations. The financial scrutiny of international organizations ensures that correct processes are followed in the allocation of reserves to various projects in the country. This chapter examines the repercussions of the alliances such as IMF, World Bank and European Central Bank on the monitoring and monetary politics in Ukraine. Besides, global financial clubs and creditor unions such as the London and Paris Clubs enhance economic stability to debt. The research also examines regulation concerning the application of blockchain technology, smart contracts, decentralized finance (DeFi) powers and AI in the financial services industry.

Conclusions and Prospects for Legal Reforms. The World Bank and International Monetary Fund are extremely important to Ukraine's economic legal order because they aid in the achievement of Ukraine's full regulatory development, economic integration and harmonization of laws to international standards. The study seeks to propose legislative reforms that will enable Ukraine to intensify relations with international financial institutions and adjust the institutional structure for financial legal relations. Also, introducing blockchain as an underlying technology for the financial governs serve the purpose of increasing the transparency and effectiveness of governance and control.

REFERENCES

1. Principles for Effective Banking Supervision. 2022. *Basel Committee on Banking Supervision*. URL: https://www.bis.org/bcbs/publ/d522.htm (last accessed: 30.01.2025).
2. Guidelines on Digital Finance and Blockchain Regulation. 2023. *European Banking Authority*. URL: https://www.eba.europa.eu/regulation-and-policy (last accessed: 30.01.2025).

3. Guidance on Crypto-Assets and AML Compliance. 2022. *Financial Action Task Force (FATF)*. URL: https://www.fatf-gafi.org/publications/virtualassets (last accessed: 30.01.2025).
4. Monetary and Financial Stability in a Digital World. 2021. *International Monetary Fund (IMF)*. URL: https://www.imf.org/en/Publications/WP (last accessed: 30.01.2025).
5. Global Financial Governance and Regulatory Reforms. 2023. *World Bank*. URL: https://www.worldbank.org/en/topic/financialsector (last accessed: 30.01.2025).
6. Trade and Financial Regulation in the Digital Economy. 2022. *WTO*. URL: https://www.wto.org/english/res_e/reser_e/trade_finance_e.htm (last accessed: 30.01.2025).
7. Digital Trade and Emerging Technologies in Global Finance. 2023. *UNCTAD*. URL: https://unctad.org/topic/e-commerce-and-digital-economy (last accessed: 30.01.2025).
8. The Role of Central Banks in Digital Finance. 2022. *European Central Bank*. URL: https://www.ecb.europa.eu/pub/pdf (last accessed: 30.01.2025).
9. Taxation and Blockchain: Policy Challenges and Opportunities. 2023. *OECD*. URL: https://www.oecd.org/tax/ (last accessed: 30.01.2025).
10. Smart Contracts and Legal Frameworks for Digital Finance. 2021. *International Chamber of Commerce*. URL: https://iccwbo.org/publication (last accessed: 30.01.2025).

https://doi.org/10.15407/akademperiodyka.545.044

KHANAS KHRYSTYNA
Doctor, Astraea Group,
London, UK

RUSSIAN USE OF CRYPTO ASSETS FOR SANCTIONS EVASION

Russia's recent shift on crypto assets Historically, Russia's stance on crypto was changing back and forth depending on various factors. Going back to 2021 and just the beginning of 2022 (before the war with Ukraine), the Central Bank of Russia (the "CBR") — Russia's main financial regulator — was a vocal critic of all things crypto.

On 20 January 2022, the CBR published a consultation paper [9] which proposed a blanket ban of cryptocurrencies on Russian territory, citing threats to financial stability, citizens' wellbeing and sovereign monetary policy. The CBR said that cryptoassets displayed aspects of a financial pyramid and warned it could be used to "service illegal activities".

The Russian Security Service (FSB) also advocated for the ban, saying that Russians were using crypto to donate to undesirable organizations and 'foreign agents'.

In its consultation paper, the CBR proposed:

- to prohibit the issue and/or circulation of cryptocurrency inside Russia (including through cryptocurrency exchanges);
- to prohibit Russian financial institutions, financial intermediaries and the country's financial infra-

Cite: Khanas Khrystyna. Russian use of crypto assets for sanctions evasion. https://doi.org/10.15407/akademperiodyka.545.044

structure from trading cryptocurrencies and creating related financial instruments;

- to prohibit cryptocurrency mining in Russia.

There was no proposed ban for Russian citizens to hold cryptocurrencies or trade cryptocurrencies abroad.

At the same time, the CBR reported that the volume of transactions of Russian citizens with cryptocurrencies reached USD 5 billion in 2021, and Russian citizens were active users of Internet platforms that trade cryptocurrencies.

In addition, the CBR noted that Russia was among the leaders in terms of crypto mining capacities globally.

A month later, in February 2022, Russia invaded Ukraine and unprecedented packages of sanctions were imposed on Russia, including:

- SWIFT ban imposed on major Russian banks and their subsidiaries;
- US, EU, and UK freeze around USD 300 billion in Russian sovereign reserves;
- major Russian Banks were designated;
- a ban on the provision of high value crypto assets to Russian persons (over €10 000 [12]);
- a ban on the provision of crypto wallets to Russian persons.

As of 2024, we can see a completely different picture in Russia:

- Crypto mining is legalised in Russia. Russia is second largest crypto miner in the world by its mining capacity.
- Cryptocurrencies are legalised for the use in cross-border settlements.
- Putin calls cryptocurrencies "a very dynamic and promising direction of the modern economy".
- CBR reported that as of September 2024, the amount of assets on the wallets of cryptocurrency exchanges belonging to Russian users is 651 billion Rubles [8] (USD 7,4 billion).

According to Chainalysis' reports and its Global Crypto Adoption Index, Russia rose from 13th place in 2023 to 7th place in 2024

in level of embracing crypto after the war with Ukraine had begun [11]. In 2024, cryptocurrencies worth USD 182,44 billion came to Russia [2].

Sanctions and the complications they cause with international settlements and transactions have been accelerating the use of cryptocurrency in Russia for the third year in a row. However, the rise in the ranking by 6 positions is most likely because the government began to actively regulate crypto payments in 2024, thereby opening up prospects for the expansion of legal crypto business.

New Russian legislation related to crypto assets. *Legalisation of using crypto assets in cross-border trade.* In July 2024, the State Duma passed the law allowing for crypto assets to be used in international payments [7]. The law came into force on 1 September 2024, and, according to the new legislation, businesses were allowed to use cryptocurrencies for cross-border trade within the experimental regime and crypto payments trials were set to begin in September 2024. Elvira Nabiullina, the governor of the CBR, said that the payments in crypto were set to be launched already by the end of 2024 [3].

The experimental regime is not public and the information about its participants and the number of transactions is not being published. However, Russian finance minister Anton Siluanov said in December 2024 that Russian companies are beginning to embrace cryptocurrencies for cross-border transactions and that "As part of the experimental regime, it is possible to use Bitcoin, which we had mined here in Russia". Siluanov expressed confidence that the use of crypto assets in international trade will expand and develop further in 2025 [15].

Rosbank, one of the Russian Federation's most important financial institutions, was reported to become the first major bank to offer cross-border transactions in cryptocurrency. Under the process, Russian companies that opt to pay for imported goods or services in cryptocurrency may do so after arranging with the supplier and indicating the wallet from which it will pay. The supplying company then would issue an invoice that includes the amount due in cryptocurrency and its receiving wallet address. Once the contract is signed, the purchasing company deposits the owed

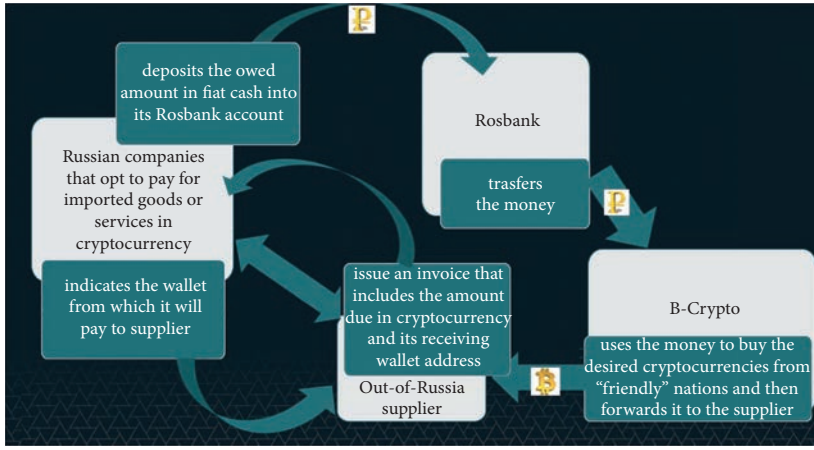

Fig. 1. Rosbank: pioneering cross-border crypto transactions

amount in fiat cash into its Rosbank account; Rosbank then transfers the money to third-party partner institution B-Crypto, which uses the money to buy the desired cryptocurrencies from so-called "friendly" nations and then forwards it to the supplier [6].

B-Crypto has since been sanctioned. *Crypto assets recognised as property and taxation of crypto assets.* In November 2024, Vladimir Putin also signed a law officially designating crypto assets as property, laying the groundwork for taxation and regulation within the sector [5].

Under the new law, mining and selling digital currencies are exempt from value-added tax (VAT), and no taxes apply to organisations facilitating transactions within the experimental regime. However, mining operators must report users of their infrastructure to tax authorities.

Instead, earnings from cryptocurrency transactions will be taxed similarly to securities income, with a 15 % personal income tax cap on crypto-related profits.

From the beginning of 2025, corporate profits from mining are subject to a 25 % tax.

Legalising crypto mining and its regulation. In summer 2024, a law was enacted to legalise cryptocurrency mining in Russia [1] which came into force on the 1 of November 2024.

The new law required commercial miners and data centre operators to register in a government database, report operations and comply with regional energy consumption limits. Individual miners can operate without registration if their energy consumption stays below government-set limits.

The government can restrict mining in energy-deficient regions and adjust power supply conditions for previously connected mining operations.

The legislation also set guidelines for foreign partnerships and cross-border operations, allowing for Russian-mined cryptocurrency to be used for international settlements.

Bitcoin mining in Russia. Crypto mining is a big part of the whole scheme of how Russia is trying to bypass Western sanctions. I am referring here to Bitcoin mining (as opposed to crypto) — this is because 90 % to 95 % of all the crypto mining activities in Russia are focused on bitcoin.

Russia has recently emerged as the second largest crypto miner globally, after the US. The growth of mining capacity in Russia was to be expected:

- Vast remote areas with **cheap electricity**. Crypto mining farms are often based within the sites of the strategic energy objects (like hydroelectric station or power plant).
- **Cold climate**, allowing miners to save considerable costs on cooling equipment for their mining farms.
- **China's blanket ban on crypto** in 2021 has pushed crypto miners from China into Russia.
- **Sanctions —** shortage of hard cash, but with a surplus of oil and natural gas.

Russia had to divert its energy flow from EU in 2022 and was left with large excess capacity. With bitcoin mining Russia could offset energy supply losses and convert energy into crypto.

Fig. 2. Some statistics regarding crypto mining in Russia

Sanctions put extreme pressure on banking support for Russians inside the country due to shutdown of corresponding bank relationships and limited ability to make payments outside of Russia.

This pushed more people inside Russia to look for ways to convert their Ruble-based capital into liquid alternatives such as BTC and stablecoins. Bitcoin mining became a tool for dealing with capital flow control (spend Rubles and get BTC).

- Flooded hardware market. In Q4 2024, demand for industrial mining equipment and services in Russia increased threefold compared to the same period last year. There is also high interest among foreign market participants, including those from the BRICS countries [4].

Herew is some more statistics regarding the market of mining: Since mid — 2022, Russian crypto mining market has been growing faster than any other region. Media also reported large volumes of mining hardware being purchased on spot market and destined for Russia.

The sector has gained strategic importance for the country's economy, allowing it to:

- Re-deploy excess energy, and
- Convert non-liquid capital (Rubles) into crypto.

Russian market is reportedly more diversified in terms of participants and very active on hardware market — compared to USA which is mainly driven by a couple of dozen large players with institutional funding and long-term contracts for supply of mining equipment.

The Russian mining market is formed by 4 groups:

- Hosting sites that were offering plug & play solution for Russian and non-Russian clients;
- Strategic players that went into mining for self-mining purposes;
- Retail miners that try to deploy 5—20 units with discounted residential tariff;
- Financial investors with the goal to convert Rubles — or energy — into more liquid capital — BTC (or stablecoins).

The volume of industrial mining in Russia, according to the Industrial Mining Association's website, currently amounts to about 1,5—1,7 GW [14] and occupies 65 % of the total mining market in the Russian Federation (35 % is private mining).

The largest crypto mining operator in Russia is BitRiver — it is also the 5th largest one in the world.

Opened in 2018, in Bratsk (Irkutsk Oblast) — ideally located considering 2 key factors:

- freezing temperatures, and
- low electricity prices.

The mean annual temperature in Bratsk is —1,5 degrees Celsius, which helps to cool all the GPU power needed for the process. There are reportedly more than 20 000 mining devices which are controlled by a team of engineers 24/7 and an armed guard making regular patrols around the farm.

BitRiver currently operates 21 data centres in Russia with 10 more under construction.

Fig. 3. BitRiver's cooperation with Russian government agencies [10]

BitRiver proudly advertises on its website it's close relationships with various Russian government agencies — the list is below (from its official website) [10].

The three most important, "strategic" and "critical" partners of BitRiver (according to its website) are:

- **Gazprom Neft** — a subsidiary of Russia's state-owned energy company, GazProm. In February 2022, both GazProm and GazProm Neft were sanctioned as agents of the government of Russia.
- **SberBank** — a Russian majority state-owned bank. BitRiver announced strategic cooperation with Sberbank in July 2024. The parties reportedly intend to develop long-term partnerships for digital transformation projects.

- **EN+ Group** — world leader in the production of low-carbon aluminium and renewable energy sources and the largest private energy holding in the world, with strong links to Oleg Deripaska. BitRiver and EN+ Group formed a separate company for collaboration called Bit+. Due to close partnership with EN+, BitRiver has built its facilities and is using resources of the various strategic objects of the energy infrastructure in Russia, like Bratsk Hydroelectric Station (owned by EuroSibEnergo), a hydroelectric dam in Ust-Ilimsk (owned by IrkutskEnergo, another subsidiary of En+) and others.

Gazprom Neft and Sberbank sanctioned. EN+ is not. It was sanctioned in 2018 together with its subsidiaries, Rusal, Eurosibenergo as well as Deripaska. But in 2019 — OFAC delisted EN+ and its subsidiaries from sanctions, because of reduction of Oleg Deripaska's ownership in the group from 70 % to 45 %. Deripaska personally is still sanctioned.

Russia Launches BRICS Mining Infrastructure Project. In 2024, the Russian state and BitRiver unveiled plans to build mining data centres across BRICS nations.

The partners will focus on "expanding the potential" of crypto mining data centres "with the possibility of further scaling of technologies".

The partnership aims to expand Russia's share in the global computing market through construction of high-performance data centres equipped for cryptocurrency mining and artificial intelligence workloads. The Russian Direct Investment Fund, RDIF, has invested over 2,2 trillion rubles (USD 22,7 billion) across more than 100 projects [13].

RDIF CEO Kirill Dmitriev added that the development of computing power for AI was "a priority for Russia and its BRICS partners".

Crypto sanctions and key takeaways:

- Crypto industry in Russia is booming — it is backed by the state regulators and most powerful players in both energy and banking sectors of Russia, including GazProm Neft, RosEnergoAtom, En+, Rusal, EuroSibEnergo and SberBank.

- Russian miners earn billions of dollars a year, the supply of specialised mining hardware to Russia is breaking all records.
- Russian energy companies affected by the Western sanctions increase their income through crypto mining — they sell their surplus energy to crypto mining companies and generate profits (despite sanctions).
- Crypto mining companies, in turn, get cheap electricity for their mining operations and create bitcoin — which in 2024 only rose in price by 134,08 %.
- The new legislation passed in 2024 allows Russia to generate large profits in crypto mining industry alone.
- This, coupled with enabling Russia to use crypto assets (both mined in Russia and elsewhere) in cross-border trade, is a golden route to evading Western financial sanctions.

Although BitRiver was sanctioned by the US in 2022, it is not sanctioned by the EU or the UK. And being sanctioned by the US, it did not create pressure enough to stifle its operation or profits.

None of the other Russian largest crypto miners or data centre operators are sanctioned. They need to be designated by the US, UK and EU, which will make it illegal for US, UK and EU citizens and companies to deal with them.

Financial institutions that facilitate crypto payments from/to Russia are mostly sanctioned and they are increasingly involved in trade with "friendly" to Russia countries, such as BRICS.

Secondary sanctions in these scenarios are especially important including against:

- Non-KYC crypto exchanges facilitating crypto transactions with Russia;
- Crypto mining equipment producers and suppliers collaborating with Russian miners and data centre operators like BitRiver;
- Crypto traders and exchanges accepting payments in fiat currencies from Russian banks, converting it to crypto and sending it on to non-Russian suppliers (like B-Crypto);

- Foreign companies using Russian crypto mining facilities etc.

Mining pools should adopt transaction filtering aligned with international sanctions and exclude Russian mined bitcoin from new blocks on blockchain.

Effective tracing techniques are needed to allow to detect crypto which was mined in Russia and restrict its further purchase or sale.

REFERENCES

1. Gosudarstvennaya Duma Rossiiskoi Federatsii. *Novosti*. URL: http://duma.gov.ru/news/59800/ (last accessed: 01.02.2025).
2. Kriptovalyuti: novie tendentsii i regulirovanie. *Habr.* URL: https://habr.com/ru/articles/870378/ (last accessed: 01.02.2025).
3. Nabiullina E. Pervie mezhdunarodnie platezhi v kriptovalyute sostoyatsya do kontsa goda. *Bits Media*. URL: https://www.bits.media (last accessed: 01.02.2025).
4. Novosti maininga. *CryptoNews.* URL: https://cryptonews.net/news/mining/30358019/ (last accessed: 01.02.2025).
5. Putin podpisal zakon, priznayushchii kriptovalyutu imushchestvom v Rossii. *Bitcoin.com.* URL: https://news.bitcoin.com/ru/putin-podpisal-zakon-priznayushchiy-kriptovalyutu-imushchestvom-v-rossii/ (last accessed: 01.02.2025).
6. Rosbank pervim zapustit transgranichnie platezhi v kriptovalyute. *Vedomosti*. 2023. URL: https://www.vedomosti.ru/finance/articles/2023/06/02/978259-rosbank-pervim-zapustit-transgranichnie-platezhi-v-kriptovalyute (last accessed: 01.02.2025).
7. *Federalnoe Sobranie Rossiiskoi Federatsii*. Zakonoproekt No. 341257-8. URL: https://sozd.duma.gov.ru/bill/341257-8 (last accessed: 01.02.2025).
8. Tsentrobank nazval razmeri rossiiskoi auditorii kriptobirzh. *Bits Media.* URL: https://www.bits.media/tsentrobank-nazval-razmery-rossiyskoy-auditorii-kriptobirzh/ (last accessed: 01.02.2025).
9. Bank of Russia. Cryptocurrencies: Trends, Risks, and Regulation. 2022. URL: https://cbr.ru/Content/Document/File/132242/Consultation_Paper_20012022_eng.pdf (last accessed: 01.02.2025).
10. BitRiver. About Us. URL: https://www.bitriver.vip/en/about.html (last accessed: 01.02.2025).

11. Chainalysis. *Global Crypto Adoption Index*. 2023. URL: https://www.chainalysis.com/blog/2023-global-crypto-adoption-index/ (last accessed: 01.02.2025).
12. European Union. *Regulation (EU) 2022/111*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2022:111:FULL&from=EN ((last accessed: 01.02.2025).
13. Forbes Digital Assets. Russia launches BRICS mining infrastructure project. *Forbes*. 2024. URL: https://www.forbes.com/sites/digital-assets/2024/10/23/russia-launches-brics-mining-infrastructure-project/ (last accessed: 01.02.2025).
14. Mining.ru. *Ofitsialnii sait*. URL: https://mining.ru/#informaciya (last accessed: 01.02.2025).
15. TradingView. *Novosti kriptovalyut*. URL: https://ru.tradingview.com/news/getblock:7721a2c4267b8:0/ (last accessed 01.02.2025).

https://doi.org/10.15407/akademperiodyka.545.056

НАМОНЮК ВАСИЛЬ
доцент кафедри міжнародних фінансів,
Київський національний університет
імені Тараса Шевченка
м. Київ, Україна

БЛОКЧЕЙН ТЕХНОЛОГІЇ ТА ТРАНСФОРМАЦІЯ ПРАКТИКИ ESG-ЗВІТНОСТІ

Верифікація даних за критеріями ESG є ключовим викликом сучасного сталого фінансування, оскільки традиційні системи звітності часто страждають від недостатньої прозорості, ризиків маніпуляцій та значних витрат на аудит і підтвердження достовірності інформації. Блокчейн технології, що базуються на принципах децентралізації, криптографічної верифікації та незмінності даних, потенційно можуть трансформувати парадигму ESG-звітності, створюючи інфраструктуру для достовірної верифікації екологічного, соціального й управлінського впливу компаній та інвестиційних продуктів.

Фундаментальною технологічною перевагою блокчейну в контексті ESG-верифікації є імутабельність даних, що забезпечується криптографічними хеш-функціями та консенсусними алгоритмами. Кожен запис про екологічні, соціальні чи управлінські показники фіксується в хронологічній послідовності блоків, що унеможливлює ретроактивні

Cite: Namonyuk Vasyl. Blockchain technologies and the transformation of ESG reporting practices. https://doi.org/10.15407/akademperiodyka.545.056

корективи без відповідного сліду. Ця архітектурна особливість блокчейну створює безпрецедентний рівень довіри до ESG-даних, усуваючи можливість маніпуляцій зі звітністю після проведення аудиту [4]. Наприклад, компанія Societe Generale 2023 р. випустила «зелені» облігації у формі токенів на блокчейні Ethereum, де кожна транзакція містить деталізовані ESG-метрики [6]. Розподілена мережна архітектура блокчейну також забезпечує можливість багатосторонньої валідації даних, залучаючи до процесу верифікації всіх учасників ланцюжка поставок — від постачальників сировини до аудиторських фірм. Зокрема, у секторі сільського господарства платформа Regen Network використовує IoT-датчики для фіксації стану ґрунтів, а отримані дані автоматично синхронізуються з блокчейном через оракулів [5]. Такий підхід забезпечує кросплатформову перевірку інформації без централізованого контролю, суттєво підвищуючи надійність ESG-даних.

Одним із найбільш перспективних інструментів для автоматизації ESG-верифікації є смартконтракти — самовиконувані програмні алгоритми, що функціонують на блокчейні. Програмовані умови виконання ESG-зобов'язань дають можливість створювати механізми автоматичного нарахування штрафів або винагород, мінімізуючи суб'єктивність експертних оцінок та людський фактор у процесах верифікації [7]. Наприклад, у проєкті KlimaDAO токенізовані вуглецеві кредити зв'язуються зі смартконтрактами, які блокують кошти до підтвердження досягнення цілей зі скорочення викидів [1]. Така модель зменшує залежність від суб'єктивних рішень аудиторів і скорочує операційні витрати на 40—60 %, порівняно з традиційними методами [2]. Смартконтракти можуть бути запрограмовані на автоматичне виконання різноманітних ESG-умов, таких як блокування фінансування за умови перевищення лімітів викидів, нарахування бонусів за досягнення соціальних цілей або модифікація процентних ставок відповідно до ESG-результативності. Інтеграція смартконтрактів з технологіями інтернету

речей (IoT) та розподіленими сенсорними мережами дає змогу автоматизувати збір первинних ESG-даних у режимі реального часу, що усуває можливість маніпуляцій з даними на етапі їх збору та забезпечує оперативність ESG-моніторингу.

Важливою компонентою верифікації ESG-даних є можливість чіткої ідентифікації суб'єктів відповідальності за екологічний, соціальний та управлінський вплив. Системи на основі децентралізованих ідентифікаторів (DIDs) присвоюють унікальні цифрові ідентифікатори кожному учаснику ESG-ланцюжка, забезпечуючи прозоре відстеження відповідальності під час виникнення порушень або недотримання зобов'язань. У випадку скандалів із порушенням трудових прав на фабриках у Південно-Східній Азії, блокчейн-платформи дають можливість точно ідентифікувати відповідальні підрозділи та керівництво, надаючи інвесторам інструменти для цілеспрямованого тиску [9]. Використання DIDs у поєднанні з незмінністю блокчейн-реєстрів створює ефективний механізм підзвітності, що стимулює компанії до дотримання задекларованих ESG-принципів і підвищує довіру стейкхолдерів до корпоративної звітності. Цей підхід особливо актуальний для транснаціональних корпорацій зі складними ланцюгами постачання, де традиційні методи верифікації часто не дають можливості точно встановити суб'єктів відповідальності за ESG-порушення.

Відомі кейси впроваджень згаданих вище механізмів демонструють суттєві переваги блокчейн-систем, порівняно з традиційними методами ESG-верифікації за ключовими параметрами ефективності. Зокрема, час верифікації скорочується з 2—6 місяців до режиму реального часу, що дає змогу оперативно реагувати на зміни ESG-показників і корегувати інвестиційні стратегії. Вартість аудиту знижується з 50—200 тис. дол. до 10—50 тис. дол. за проєкт, що робить ESG-верифікацію доступною для середніх та малих підприємств. Рівень автоматизації процесів верифікації підвищується з 15—30 до 70—90 %, що мінімізує вплив людського фактора та суб'єктивнос-

ті у процесах оцінки ESG-результативності [2; 12]. Значущою перевагою є практично повне виключення можливості маніпуляцій з даними, що критично важливо для боротьби з практиками «зеленого камуфляжу» (greenwashing) і забезпечення достовірності ESG-декларацій. Ці переваги трансформують ESG-верифікацію з формальної процедури у дієвий інструмент забезпечення прозорості та відповідальності бізнесу перед суспільством і довкіллям.

Синергія блокчейну з технологіями штучного інтелекту (ШІ) й аналізу великих даних відкриває нові можливості для поглибленої верифікації та прогнозування ESG-ризиків. Алгоритми машинного навчання можуть аналізувати історичні дані, зафіксовані в блокчейні, для виявлення прихованих кореляцій між ESG-показниками та фінансовими метриками, що дає можливість розробляти більш ефективні стратегії сталого інвестування. Платформи типу DeFi ESG використовують ШІ для моделювання впливу змін клімату на фінансові показники компаній, пропонуючи інвесторам динамічні стратегії хеджування ESG-ризиків [3; 11]. Аналіз великих обсягів неструктурованих ESG-даних, таких як супутникові знімки лісових масивів, дані соціальних мереж про порушення трудових прав або публічні документи про корпоративне управління, забезпечує комплексну оцінку ESG-результативності, що виходить за межі формальної звітності. Така інтеграція створює технологічну основу для переходу від статичної ESG-верифікації до динамічного моніторингу в режимі реального часу, що суттєво підвищує релевантність ESG-даних для прийняття інвестиційних рішень.

Незважаючи на значний потенціал, впровадження блокчейн-технологій для ESG-верифікації супроводжується рядом суттєвих викликів, що потребують комплексного вирішення. Проблема стандартизації ESG-метрик є однією з найбільш актуальних, оскільки відсутність єдиних протоколів для оцінки ESG-показників ускладнює масштабування блокчейн-рішень. Наприклад, вимірювання «соціального впливу»

може охоплюваьт відмінні набори індикаторів у різних юрисдикціях, що вимагає розробки адаптивних смартконтрактів, здатних працювати з різними методологіями оцінки [4]. Іншим значним викликом є конфлікт між прозорістю блокчейну та вимогами конфіденційності даних. Імутабельність блокчейну може суперечити нормам захисту особистих даних, зокрема вимогам GDPR щодо права на забуття. Компанії хімічної промисловості, що використовують приватні блокчейни Hyperledger, змушені балансувати між публічним доступом до ESG-даних і захистом комерційних таємниць [4]. Крім того, технічна складність та енергоємність публічних блокчейнів, особливо тих, що використовують механізм консенсусу Proof-of-Work, створює додаткові екологічні витрати, що потенційно суперечить ESG-цілям. Ці виклики актуалізують необхідність розробки спеціалізованих протоколів й архітектурних рішень, оптимізованих для завдань ESG-верифікації.

Подальший розвиток блокчейн-систем для ESG-верифікації вимагає формування адаптивного регуляторного середовища та розробки міжнародних стандартів. Ініціативи типу Green Digital Finance Taxonomy пропонують комбінувати публічні блокчейни для аудиту з приватними сайдчейнами для обробки конфіденційних даних, забезпечуючи сумісність із вимогами SFDR (Sustainable Finance Disclosure Regulation) без втрати переваг децентралізації [8]. Регуляторні «пісочниці» у юрисдикціях типу Швейцарії чи Сінгапуру тестують моделі часткової анонімізації даних через технології zero-knowledge proof, що дає можливість підтверджувати виконання ESG-критеріїв без розкриття чутливих бізнес-показників [11]. Розвиток міжнародної співпраці між технологічними компаніями, фінансовими регуляторами й неурядовими організаціями є необхідною умовою для створення глобальних стандартів ESG-верифікації на блокчейні, що забезпечить сумісність різних систем та методологій. Перспективним напрямком також є розробка енергоефективних протоколів і механізмів консенсусу, спеціально опти-

мізованих для завдань ESG-верифікації, що дасть можливість мінімізувати екологічний слід самих блокчейн-систем та забезпечити їхню відповідність ESG-критеріям.

Блокчейн технології трансформують парадигму ESG-верифікації, створюючи децентралізовану інфраструктуру для прозорого, автоматизованого й достовірного моніторингу екологічного, соціального та управлінського впливу. Імутабельність блокчейн-реєстрів, програмованість смартконтрактів і можливість багатосторонньої валідації даних забезпечують безпрецедентний рівень довіри до ESG-звітності, що є критично важливим для подолання проблеми «зеленого камуфляжу» та підвищення ефективності сталого інвестування. Інтеграція блокчейну з технологіями штучного інтелекту, інтернету речей та аналізу великих даних відкриває перспективи створення комплексних систем ESG-моніторингу, здатних забезпечувати верифікацію в режимі реального часу та прогнозувати потенційні ESG-ризики. Водночас подальший прогрес у цій сфері залежить від подолання викликів стандартизації, конфіденційності й енергоефективності, а також від формування адаптивного регуляторного середовища, що сприятиме масштабуванню блокчейн-рішень для ESG-верифікації на глобальному рівні.

ЛІТЕРАТУРА

1. Ballesteros-Rodríguez A., De-Lucio J., Sicilia M.-Á. Tokenized carbon credits in voluntary carbon markets: the case of KlimaDAO. *Frontiers in Blockchain*. 2024. Vol. 7. https://doi.org/10.3389/fbloc.2024.1474540
2. Huang W., Han Y., Gu Q., Han X., et al. Smart blockchain-powered natural resource asset management and ecological governance countermeasures. *Heliyon*. 2025. Vol. 11, No. 2. https://doi.org/10.1016/J.HELIYON.2024.E41475
3. Lee S., Perera H., Liu Y., Xia B., et al. Integrating ESG and AI: A Comprehensive Responsible AI Assessment Framework. *arXiv.org*. 2024. https://doi.org/10.48550/arxiv.2408.00965

4. Pizzi S., Caputo A., Venturelli A., Caputo F. Embedding and managing blockchain in sustainability reporting: a practical framework. *Sustainability Accounting, Management and Policy Journal*. 2022. Vol. 13, No. 3, P. 545—567. https://doi.org/10.1108/SAMPJ-07-2021-0288
5. Regen Network Review. *Blockchain Platform for Soil Regeneration*. URL: https://unblock.net/regen-network-review/#:~:text=Regen%20Network%20is%20a%20startup,to%20being%20simple%20food%20producers (дата звернення: 01.03.2025).
6. Societe Generale issues a first digital green bond on a public blockchain. *Societe Generale*. 2023. URL: https://www.societegenerale.com/en/news/press-release/first-inaugural-digital-green-bond-public-blockchain (дата звернення: 01.03.2025).
7. Stuit A., Brockington D., Corbera E. Smart, Commodified and Encoded: Blockchain Technology for Environmental Sustainability and Nature Conservation. *Conservation and Society*. 2022, Vol. 20, No. 1. P. 12—23. https://doi.org/10.4103/CS.CS_41_21
8. Sustainability-related disclosure in the financial services sector. *Finance.* URL: https://finance.ec.europa.eu/sustainable-finance/disclosures/sustainability-related-disclosure-financial-services-sector_en (дата звернення: 01.03.2025).
9. Tan S. Blockchain in Southeast Asia: Striking a Balance Between Innovation and Protection. *The Diplomat — Asia-Pacific Current Affairs Magazine*. URL: https://thediplomat.com/2022/06/blockchain-in-southeast-asia-striking-a-balance-between-innovation-and-protection/ (дата звернення: 01.03.2025).
10. Yadav A., Shivani S., Manda V., Sangwan V., Demkiv A. Blockchain technology for ecological and environmental applications. *Ecological Questions*. 2024. Vol. 35. P. 1—20. https://doi.org/10.12775/EQ.2024.050
11. Zhao Y. Empowering Sustainable Finance: The Convergence of AI, Blockchain, and Big Data Analytics. *Advances in Economics, Management and Political Sciences*. 2024. https://doi.org/10.54254/2754-1169/85/20240925
12. Zhou G. Research on Application of Blockchain Technology in Departure Audit of Natural Resources Assets. *IOP Conference Series: Earth and Environmental Science*. 2021. Vol. 687, No. 1. https://doi.org/10.1088/1755-1315/687/1/012172

https://doi.org/10.15407/akademperiodyka.545.063

НОСОВА НАТАЛІЯ
провідний інженер,
Державна установа «Інститут ринку і економіко-екологічних досліджень НАН України»,
м. Одеса, Україна
https://orcid.org/0009-0008-4830-0009

ТЕНДЕНЦІЇ ВПРОВАДЖЕННЯ СУЧАСНИХ ЦИФРОВИХ ТЕХНОЛОГІЙ У РОЗВИТОК АГРОПРОДОВОЛЬЧОГО СЕКТОРА УКРАЇНИ ТА ЇХ ЗАКОНОДАВЧЕ ВРЕГУЛЮВАННЯ

Сучасний світ, який активно розвивається і запроваджує нові цифрові рішення у різні технологічні процеси, зокрема у агропродовольчий сектор, потребує вирішення гострих загальнолюдських проблем, однією з яких є «…подолання голоду, досягнення продовольчої безпеки, покращення харчування і сприяння сталому розвитку сільського господарства» [11]. Ця проблема є об'єктом досліджень науковців і практиків, які бачать її вирішення у впровадженні цифрових технологій, яке може суттєво вплинути на ефективність і швидке зростання цього сектора.

Цифрові технології проникли в усі сфери життя, змінили економічні та організаційні процеси,

Cite: Nosova Natalia. Trends in the implementation of modern digital technologies in the development of the agricultural and food sector of Ukraine and their legislative regulation. https://doi.org/10.15407/akademperiodyka.545.063

способи комунікацій між постачальниками й споживачами товарів і послуг [1]. Цифровізація агробізнесу передбачає використання сучасних інструментів, моніторингу та аналітики даних, а також прийняття рішень з використанням цифрових технологій у сільському господарстві для покращення та оптимізації систем землеробства, підвищення якості врожаю і врожайності, зменшення відходів та боротьби зі шкідниками й хворобами [10]. Україна активно проводить політику щодо цифровізації усіх сфер життя, визначивши її однією з пріоритетних і створюючи цифрові платформи на кшталт «Дії». Проводиться активна законодавча робота у цьому напрямку.

Передумовами для продовження розвитку сфери цифровізації є законодавство щодо цифрової економіки та телекомунікацій, наявність цифрової інфраструктури, а також досягнення у сфері безготівкової економіки, зокрема розвиток електронної торгівлі (e-Trade), електронного захисту (e-Trust) і кібербезпеки (Cybersecurity) [2]. Сфера цифровізації функціонує на основі таких законів: «Про національну програму інформатизації» [8], «Про державну підтримку розвитку індустрії програмної продукції» [5], «Про електронні документи та електронний документообіг» [6], «Про інформацію» [7] та багатьох інших. Формування і реалізацію політики держави у сфері цифрового розвитку економіки і цифрових технологій забезпечує Міністерство цифрової трансформації України.

Досвід передових країн світу свідчить про «…можливість переходу України на наступний етап розвитку законодавства в цій області, зокрема, його системну кодифікацію. Підхід ЄС до цифрової трансформації означає розширення можливостей та залучення кожного громадянина до неї, посилення потенціалу кожного бізнесу та вирішення глобальних викликів, що визначено у рамкових та стратегічних документах» [2].

Також надходять пропозиції щодо прийняття Цифрового кодексу України, що надасть можливість упорядкувати законо-

давство з цифровізації та зосередити в одному правовому документі всі законодавчі норми.

З огляду на законодавство в агропромисловій сфері виникає необхідність його адаптації щодо використання у різних сільськогосподарських екосистемах і на різних етапах виробництва сільгосппродукції, починаючи з обробки земель і закінчуючи отриманням готового продукту, а також на різних ланцюжках створення вартості.

Цифрові технології сприяють підвищенню ефективності багатьох бізнес-процесів, включаючи фінансування, підготовку звітності, моніторинг виконання різних етапів робіт, виробництво та використання сільськогосподарської техніки, складських й елеваторних приміщень, а також приміщень для утримання тварин, включаючи контроль за своєчасним їх годування та виконанням санітарних процедур.

Відстеження якості виконуваних робіт — завдання вкрай важливе в аграрному бізнесі. Згідно з дослідженнями в більшості випадків проблемні ділянки на полях виникають через людський фактор. Тому виникає необхідність застосовувати у сільському господарстві смарттехнології, які ще називають розумними технологіями, і використовуються для збору й аналізу інформації; моніторингу різних процесів; для управління і прийняття рішень; для виконання прийнятих рішень. Смарттехнології працюють насамперед з інформаційним середовищем. За допомогою смарттехнологій відстежують роботу великогабаритної техніки, контролюють обробку ґрунту, висаджування і збір врожаю, внесення добрив та постачання товарів до сховищ й до торгової мережі [4].

Одним із пріоритетних напрямів використання сучасних технологій є геоінформаційні технології (ГІС-технології) для відстеження стану ґрунтів, водойм, відходів, регулювання вегетації рослин, їх зрошення тощо [3]. ГІС-технології надають можливість оперативно визначати сільгоспугіддя, які потребують першочергової меліорації. Це дає змогу скорочувати

Рис. 1. Ієрархічна модель формування продовольчої безпеки

витрати на оперативне отримання необхідної інформації та обробку даних, що сприяє підвищенню врожайності сільгоспкультур та упереджає можливий негативний вплив на довкілля.

Важливою умовою розвитку агропромислового комплексу країни є стійке функціонування аграрних підприємств, що забезпечують продовольчу безпеку. Поняття «продовольча безпека» в широкому розумінні характеризує стан продовольчого ринку як окремої людини, так і громади, регіону, держави і світу загалом (рис. 1).

У забезпеченні продовольством населення і вирішення цим питань продовольчої безпеки великого значення набуває використання сучасних технологій, які останнім часом все ширше використовуються у всіх сферах життєдіяльності людей [9].

Таким чином, цифровізація агропромислового комплексу полегшить роботу у цій сфері та вирішить питання нестач кадрів, а також сприятиме автоматизації багатьох технологічних процесів і виробництву високоякісної сільгосппродукції, що відповідає світовим стандартам якості.

ЛІТЕРАТУРА

1. Брюховецька Н.Ю., Черних О.В. Індустрія 4.0 та цифровізація економіки: можливості використання зарубіжного досвіду на промислових підприємствах України. *Економіка промисловості*. 2020. № 2. С. 116—132. http:/doi.org/10.15407/econindustry2020.02.116
2. Гедіков В. Загальний аналіз нормативно-правових актів у сфері цифровізації в Україні. *Юридичний вісник*. 2024. № 3. https://doi.org/10.32782/yuv.v3.2024.7
3. ГІС технології в сільському господарстві. URL: https://eos.com/uk/blog/suchasni-tekhnolohii-v-silskomu-hospodarstvi/ (дата звернення: 04.02.2025).
4. Носова Н.І. Впровадження цифрових технологій у агропродовольчий сектор як складова забезпечення продовольчої безпеки України. *Моделювання соціально-економічного розвитку в системі забезпечення продовольчої безпеки*: матеріали ІІ Всеукр. наук.-практ. конф. (8—9 трав. 2024 р.). Миколаїв: МНАУ. 2024. С. 146—148.
5. Про державну підтримку розвитку індустрії програмної продукції. Закон України від 16.10.2012. № 5450-VI. URL: https://zakon.rada.gov.ua/laws/ show/5450-17#Text (дата звернення: 04.02.2025).
6. Про електронні документи та електронний документообіг. Закон України від 22.05.2003. № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 04.02.2025).
7. Про інформацію. Закон України від 02.10.2022. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/ show/2657-12#Text (дата звернення: 04.02.2025).
8. Про національну програму інформатизації. Закон України від 01.12.2022. № 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text (дата звернення: 04.02.2025).

9. Тараканов М.Л., Носова Н.І. Роль сучасних технологій у забезпеченні продовольчої безпеки України. *Глобалізація та розвиток інноваційних систем: тенденції, виклики, перспективи*: матеріали ІІ Міжнар. наук.-практ. конф. (14—15 берез. 2024 р.). Харків: Держ. біотехнологічний ун-т, 2024. С. 253—256. URL: https://biotechuniv.edu.ua/wp-content/uploads/2024/04/conf-14-15-03-24-mater.pdf (дата звернення: 04.02.2025).
10. Abiri R., Rizan N., Balasundram S., Shahbazi A., Abdul-Hamid H. Application of digital technologies for ensuring agricultural productivity. *Heliyon*. 2023. Vol. 9, No. 12. P. 22601. https://doi.org/10.1016/j.heliyon.2023.e22601
11. End hunger, achieve food security and improved nutrition and promote sustainable agriculture. Department of Economic and Social Affairs. *Sustainable Development. United Nations.* URL: https://sdgs.un.org/goals/goal2 (дата звернення: 04.02.2025).

https://doi.org/10.15407/akademperiodyka.545.069

П'ЯТНИЧУК ІРИНА
доцент, кандидат економічних наук,
декан факультету управління,
Прикарпатський національний університет
імені Василя Стефаника
м. Івано-Франківськ, Україна
https://orcid.org/ 0000-0003-2876-6422

ЦИФРОВА ТРАНСФОРМАЦІЯ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ВИЩОЇ ОСВІТИ

У сучасних умовах цифрова трансформація публічного управління у сфері вищої освіти зазнає суттєвих змін, орієнтуючись на впровадження інноваційних технологій для підвищення ефективності, прозорості та доступності освітніх послуг. Однією з ключових тенденцій є застосування штучного інтелекту (далі — ШІ) та аналітики даних, що дає можливість автоматизувати адміністративні процеси, персоналізувати взаємодію з громадянами й оптимізувати обробку запитів.

Паралельно з цим активно розвиваються мобільні додатки та онлайн-платформи, які надають громадянам можливість швидко й зручно отримувати державні послуги у сфері вищої освіти без необхідності особистого відвідування установ. Крім того, дедалі більше уваги приділяється використанню блокчейн-технологій для забезпечення безпеки й

Cite: Piatnychuk Iryna. Digital transformation of public administration in higher education. https://doi.org/10.15407/akademperiodyka.545.069

надійності збереження даних, що сприяє підвищенню рівня довіри до освітніх установ.

Важливим аспектом сучасного управління є принцип «одноразової ідентифікації», який спрощує доступ громадян до різних послуг без необхідності повторного надання особистих даних. Також значна увага приділяється електронному документообігу та використанню електронного підпису, що пришвидшує адміністративні процеси й мінімізує бюрократичні перешкоди.

Таким чином, сучасні технологічні тенденції та цифрові рішення спрямовані на створення більш ефективної, прозорої і доступної системи публічного управління у сфері вищої освіти. У подальшому дослідженні буде розглянуто рекомендації та стратегії впровадження цих інновацій з урахуванням актуальних потреб стейкхолдерів освітнього процесу.

Найбільш популярна тенденція полягає в застосуванні ШІ й аналітики даних для автоматизації та оптимізації роботи державних органів у сфері вищої освіти. ШІ допомагає виявляти патерни в обробці запитів громадян та розробляти персоналізовані рішення, що забезпечує ефективніше й швидше здійснювати освітню діяльність [1, с. 157; 2].

Крім того, велика увага приділяється розвитку мобільних додатків та онлайн-платформ, які дають можливість громадянам зручно й швидко звертатися за допомогою до державних органів, зокрема і у сфері вищої освіти. Це забезпечує легкий доступ до інформації та послуг з будь-якого місця та в будь-який час [5].

Ще однією інноваційною практикою є використання блокчейн- технологій для забезпечення безпеки й надійності даних у системах публічного управління. Блокчейн дає змогу створювати недоступні для змін записи, що робить процес обробки даних більш прозорим і безпечним.

Деякі країни вже впроваджують інноваційні практики, такі як «одноразова ідентифікація» або «одного разу для всіх», де громадяни мають можливість один раз надати свої особисті

дані й отримати доступ до різних послуг без необхідності повторно вводити ці дані для кожної послуги [3, с. 121].

Зокрема, важливою тенденцією є зростання уваги до прозорості та відкритості діяльності державних органів. Це означає публікацію відкритих даних, відкритість процесів прийняття рішень і залучення громадськості до управління.

Іншою важливою інноваційною практикою є впровадження «електронного документообігу» та «електронного підпису», що спрощує та прискорює процеси обміну документами між державними органами й громадянами чи підприємствами.

Загалом сучасні тенденції та інноваційні підходи у сфері публічного управління вищою освітою спрямовані на забезпечення більш ефективного, зручного та прозорого надання освітніх послуг зацікавленим сторонам.

За підсумками проведеного дослідження, можна сформулювати рекомендації та стратегії для покращення ефективності публічного управління вищою освітою з урахуванням сучасних потреб стейкхолдерів і тенденцій у цій сфері [1, с. 158]:

1. Підвищення доступності й освіченості: розробка освітніх програм та тренінгів, зокрема і з цифрової грамотності для громадян усіх вікових категорій, щоб забезпечити більший доступ до освітніх послуг і підвищити рівень їхньої ефективності.

2. Розвиток мобільних додатків, тобто створення мобільних додатків для доступу до освітніх послуг на смартфонах та планшетах, що забезпечить більшу зручність і доступність для користувачів.

3. Впровадження персоналізованих сервісів, що передбачає розробку інтерактивних платформ, які можуть адаптуватися до потреб кожного конкретного користувача, надаючи персоналізовану інформацію та послуги.

4. Забезпечення безпеки даних, тобто посилення заходів захисту даних в інформаційних системах ЗВО, використання сучасних технологій шифрування та ідентифікації для забезпечення конфіденційності й безпеки інформації.

5. Розвиток інтерактивного зворотного зв’язку, що включає створення механізмів збору відгуків від користувачів щодо якості та ефективності наданих освітніх послуг для постійного їх вдосконалення.

6. Стандартизація та спрощення процедур, тобто впровадження єдиної системи стандартів і процедур надання освітніх послуг та системи управління ЗВО задля спрощення процесів взаємодії стейкхолдерів освітнього процесу державними органами й органами місцевого самоврядування.

7. Стимулювання інновацій, що означає підтримку та стимулювання інноваційних рішень у сфері вищої освіти, залучення приватного сектора й стартапів для розробки нових технологічних рішень та платформ для надання освітніх послуг.

Застосування поданих рекомендацій має багато переваг, які сприяють покращенню ефективності публічного управління вищою освітою. По-перше, підвищення доступності освіти. Розвиток мобільних додатків для доступу до освітніх послуг на смартфонах і планшетах дасть можливість здобувачам освіти отримувати доступ до необхідних сервісів у будь-який час та будь-де, що підвищить їхню зручність й ефективність взаємодії із суб’єктами публічного управління вищою освітою. Це особливо важливо для молоді, яка віддає перевагу мобільним технологіям. Забезпечення безпеки даних в інформаційних системах публічного управління вищою освітою є критично важливим складником для збереження довіри здобувачів до органів публічного управління вищою освітою. Застосування сучасних технологій шифрування і захисту даних допомагатиме уникнути витоку конфіденційної інформації та збереже довіру здобувачів вищої освіти до освітніх послуг [4, с. 218].

Таким чином, можемо підсумувати, що цифрова трансформація публічного управління у сфері вищої освіти є важливим напрямом розвитку сучасної освітньої системи. Використання штучного інтелекту, аналітики даних, мобільних додатків та блокчейн-технологій сприяє підвищенню ефективності

адміністративних процесів, покращенню доступності освітніх послуг і забезпеченню їхньої прозорості.

Розвиток онлайн-платформ та впровадження принципу «одноразової ідентифікації» дає можливість громадянам швидко й зручно отримувати необхідні послуги, мінімізуючи бюрократичні процедури. Своєю чергою, електронний документообіг та цифровий підпис спрощують взаємодію між державними органами, закладами вищої освіти і користувачами освітніх послуг.

Запровадження цих інноваційних підходів сприяє не лише оптимізації управлінських процесів, а й формуванню більш відкритої, прозорої та зручної системи взаємодії між усіма учасниками освітнього процесу. Подальші дослідження і практичні впровадження цифрових технологій у сфері вищої освіти нададуть можливість забезпечити ще вищий рівень ефективності та якості освітніх послуг.

ЛІТЕРАТУРА

1. П'ятничук І. Інформаційний механізм публічного управління вищою освітою. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2024. Вип. 9. С. 151—160.
2. П'ятничук І.Д. Публічне управління наданням електронних послуг: аналіз ефективності та напрямки подальших покращень. *Успіхи і досягнення у науці (Серія «Право», Серія «Освіта», Серія «Управління та адміністрування», Серія «Соціальні та поведінкові науки»)*. 2024. Т. 4, № 4. С. 522—533.
3. Alsarraf H., Aljazzaf S., Ashkanani A. Do you see my effort? An investigation of the relationship between e-government service quality and trust in government. *Transforming Government: People, Process and Policy*. 2023. Vol. 17, No. 1. P. 116—133.
4. Nawafleh S., Khasawneh A. Drivers of citizens E-loyalty in E-government services: E-service quality mediated by E-trust based on moderation role by system anxiety. *Transforming Government: People, Process and Policy*. 2024. Vol. 18, No. 2. P. 217—240.
5. Putrevu J., Mertzanis C. The adoption of digital payments in emerging economies: challenges and policy responses. *Digital Policy, Regulation and Governance*. 2023. Vol. 26, No. 5. P. 476—500.

https://doi.org/10.15407/akademperiodyka.545.074

RAMSDEN JAMES
King's Councel, Astraea Group,
London, UK

TRENDS IN ARTIFICAL INTELLIGENCE AND DIGITAL ECONOMY

Trends in Digital Economy. *DeFi protocols are gaining momentum.* Against the backdrop of the self-destructive tendencies of the centralized financial system based on the dollar, decentralized finance is growing in popularity. The leaders are Indonesia and, ironically, the United States. DeFi systems allow you to trade, invest, buy, exchange and withdraw crypto and receive p2p loans without banks.

Stablecoins are the choice of the majority. Stablecoins like USDT or USDC give users confidence that their assets will not depreciate overnight. This is especially true for countries with unstable economies.

Central Bank Digital Currencies (CBDCs) — specifically by Russia. Russia has been building alternative financial structures that bypass the US dollar and potentially undermine the US-centric international monetary system. Russia has been actively developing its own digital currency — digital ruble in hopes of trading directly with the countries that would accept the funds without first converting them to US dollars. Three major Russian banks have successfully piloted digital ruble transactions on their mobile banking apps.

Cite: Ramsden James. Trends in artifical intelligence and digital economy. https://doi.org/10.15407/akademperiodyka.545.074

VTB and PSB conducted the first successful testing of transactions with digital rubles issued on a test version of the CBR's digital ruble platform back in February 2022 [7]. In August 2023, VTB became the first Russian bank to conduct transactions using digital ruble. Currently, 30 companies in 11 cities are reported to accept the digital ruble through VTB [4]. For instance, Lukoil gas stations accept the CBDC for purchases, users can pay for phone or internet services at Rostelecom, and it is usable on the Moscow Metro (underground services). The plan is for the cross-border payments to be made in digital ruble — without using the banking system of other countries, only through the digital ruble platform, which is operated by the Bank of Russia. This will promote business operations internationally with "friendly" to Russia businesses — who are not susceptible to the opinion of the West and ready to continue transacting with Russia.

Digital Financial Assets in Russia. In February 2024, the Russian Duma (parliament) passed a law to allow international payments to be made with DFAs [5] on a Russian block chain that is controlled by Russia's Central Bank — it will be the only entity able to scrutinise international payments made with DFAs between residents and non-residents of the Russian Federation. It is now possible to conduct traditional financial market processes (asset trading, clearing and rights accounting) using blockchain and smart contracts.

DFAs can "wrap" a wide variety of assets in digital packaging, which simplifies their trading. Over the past years, precious metals, real estate, corporate debt obligations and many other financial instruments have been tokenised in Russia on various digital platforms that permit different repayment mechanics, and as a result, investors have a wider choice of exit than they typically have using a conventional exchange.

DFAs are useful where bank settlements are impossible due to sanctions or counterparties are not interested in receiving Russian rubles as means of payment but would like to acquire some asset expressed in digital form.

BRICS PAY system. BRICS Pay system was created in 2023, which was set to challenge the Western SWIFT payment system

and promote BRICS-based alternatives — all in line with the bloc's long-embraced efforts of de-dollarization. BRICS PAY is a digital payments platform that is being jointly developed by the member countries of the BRICS bloc. BRICS PAY aims to enable digital payments between the different countries in BRICS PLUS format, allowing businesses to make and receive payments in their local currency.

BRICS's single currency. Further, the creation of a single currency within BRICS which would be backed by gold, which could be used in mutual trade, is being currently actively discussed. Whilst there are critics saying that it would be a long and difficult way for BRICS to issue its own currency, some experts claim that the prospect of it is quite realistic. [The total gold reserve of the BRICS members is 6,3 thousand tons [6], and this figure is growing steadily. BRICS countries are the world's largest buyers of gold since 2022. For comparison, the leader in terms of gold reserves — the United States — has a little more than 8 thousand tons, and they have been at this level since the early 1970s. In addition, members of BRICS are currently actively buying gold. The Reserve Bank of India alone added more than nine tonnes to its reserves in June, the highest in two years. India's reserves have increased by 37 tonnes to 841 tonnes this year, according to the World Gold Council.

BRICS BRIDGE. The BRICS nations — Brazil, Russia, India, China, and South Africa are driving a new vision for economic independence with the launch of the BRICS Bridge.

- Reducing Remittance Costs and Boosting Efficiency.
- Fostering Financial Inclusion and Independence.
- Challenging Western Financial Dominance.
- Setting a Global Precedent for Remittance Reform.

The BRICS Bridge could inspire global remittance reforms by offering a model for economic collaboration. Its success may encourage non-Western nations to create independent, cost-effective systems, reshaping international finance and promoting financial inclusion. BRICS Bridge has the potential to make remittance flows more efficient and equitable, boosting economic resilience within BRICS and beyond.

DFAs first appeared on the Russian market as long ago as July 2022 (some 4 months after the Russian full-scale invasion of Ukraine) when three operators — Lighthouse, Sberbank, and Atomyze — carried out pilot issues for 60 million rubles [1] (USD 660 000).

As of now, there are 14 such operators entered on the register. Whilst both Atomyze and Lighthouse were designated under the Russia sanctions regime back in March 2024, at least three of the issuers of DFAs in Russia have not yet been sanctioned.

Russia's digital financial asset market has experienced explosive growth in 2024, reaching a total volume of 684 billion rubles — more than seven times its 2023 size [3]. Russia's DFA market grew more than 4 times in 2024, according to the Russian ACRA credit rating agency. Further, according to ACRA, the market volume of DFA issues will reach 1 trillion rubles by 2027. The total volume in 2025 is expected to be 600—700 billion rubles (USD 6,7 billion — 7,8 billion).

Trends in Artificial Intelligence. Artificial Intelligence (AI) Statistics:

- AI market size is expected to reach $1339 billion by 2030.
- AI will have an estimated 21 % net increase on the United States GDP by 2030.
- Over 75 % of consumers are concerned about misinformation from AI.

A major concern for consumers is the potential for AI to perpetuate the spread of misinformation. More than 75 % of consumers are worried about the impact that AI has on the ability to trust information found on the internet.

- ChatGPT had 1 million users within the first five days of being available.
- One in 10 cars will be self-driving by 2030.
- It is expected that 10 % of vehicles will be driverless by 2030 [8], as the global market of self-driving cars is forecasted to increase from 20,3 million in 2021 to 62,4 million.
- 64% of businesses expect AI to increase productivity.

AI Adoption Statistics.

- Half of U.S. mobile users use voice search every day.

Voice search is on the rise, with 50 % of U.S. mobile users using it daily. This trend showcases the growing prevalence of AI-powered voice assistants in everyday life.

- AI is expected to see an annual growth rate of 36,6% from 2023 to 2030.

AI continues to revolutionize various industries, with an expected annual growth rate of 36,6 % between 2023 and 2030, as reported by Grand View Research. This rapid growth emphasizes the increasing impact of AI technologies in the coming years.

- 72 % of businesses have adopted AI for at least one business function.

Nearly three out of four businesses have started using AI for at least one business function. In addition, half of survey respondents use AI for two or more of their business functions. This is a sharp uptick from 2023 when less than a third of respondents had reported using AI for at least two business functions.

- India is the country with the highest AI adoption rate at 59 % [2].

AI adoption rates are the highest for organizations in India (59 %), followed closely by the United Arab Emirates (58 %). Businesses in Singapore (53 %) and China (50 %) are also leaders in AI use. In contrast, businesses in Australia (29 %), Spain (28 %) and France (26 %) have been slower to try out AI.

How AI Will Impact the Future:

1. Improved Business Automation.

2. Job Disruption.

3. Data Privacy Issues. Companies require large volumes of data to train the models that power generative AI tools, and this process has come under intense scrutiny. Concerns over companies collecting consumers' personal data have led the FTC to open an investigation into whether OpenAI has negatively impacted consumers through its data collection methods after the company potentially violated European data protection laws.

In response, the Biden-Harris administration developed an AI Bill of Rights that lists data privacy as one of its core principles.

4. Increased Regulation. AI could shift the perspective on certain legal questions, depending on how generative AI lawsuits unfold in 2024. For example, the issue of intellectual property has come to the forefront in light of copyright lawsuits filed against OpenAI by writers, musicians and companies like The New York Times. These lawsuits affect how the U.S. legal system interprets what is private and public property, and a loss could spell major setbacks for OpenAI and its competitors.

Ethical issues that have surfaced in connection to generative AI have placed more pressure on the U.S. government to take a stronger stance.

5. Climate Change Concerns. The energy and resources required to create and maintain AI models could raise carbon emissions by as much as 80 percent, dealing a devastating blow to any sustainability efforts within tech. Even if AI is applied to climate-conscious technology, the costs of building and training models could leave society in a worse environmental situation than before.

6. Accelerated Speed of Innovation. In an essay about the future potential of AI, Anthropic CEO Dario Amodei hypothesizes that powerful AI technology could speed up research in the biological sciences as much as tenfold, bringing about a phenomenon he coins "the compressed 21st century", in which 50 to 100 years of innovation might happen in the span of five to 10 years. This theory builds on the idea that truly revolutionary discoveries are made at a rate of maybe once per year, with the core limitation being a shortage of talented researchers. By increasing the cognitive power devoted to developing hypotheses and testing them out, Amodei suggests, we might close the time gap between important discoveries like the 25-year delay between CRISPR's discovery in the '80s and its application to gene editing.

Risks and Dangers of AI. ***Job Losses.*** Between 2023 and 2028, 44 percent of workers' skills will be disrupted. Not all workers will be affected equally — women are more likely than men to be exposed to AI in their jobs. Combine this with the fact that there is a gaping AI

skills gap between men and women, and women seem much more susceptible to losing their jobs. If companies don't have steps in place to upskill their workforces, the proliferation of AI could result in higher unemployment and decreased opportunities for those of marginalized backgrounds to break into tech.

Human Biases. The reputation of AI has been tainted with a habit of reflecting the biases of the people who train the algorithmic models. For example, facial recognition technology has been known to favour lighter-skinned individuals, discriminating against people of colour with darker complexions. If researchers aren't careful in rooting out these biases early on, AI tools could reinforce these biases in the minds of users and perpetuate social inequalities.

Deepfakes and Misinformation. The spread of deepfakes threatens to blur the lines between fiction and reality, leading the general public to question what's real and what isn't. And if people are unable to identify deepfakes, the impact of misinformation could be dangerous to individuals and entire countries alike. Deepfakes have been used to promote political propaganda, commit financial fraud and place students in compromising positions, among other use cases.

Data Privacy. Training AI models on public data increases the chances of data security breaches that could expose consumers' personal information. Companies contribute to these risks by adding their own data as well. A 2024 Cisco survey found that 48 percent of businesses have entered non-public company information into generative AI tools and 69 percent are worried these tools could damage their intellectual property and legal rights. A single breach could expose the information of millions of consumers and leave organizations vulnerable as a result.

Automated Weapons. The use of AI in automated weapons poses a major threat to countries and their general populations. While automated weapons systems are already deadly, they also fail to discriminate between soldiers and civilians. Letting artificial intelligence fall into the wrong hands could lead to irresponsible use and the deployment of weapons that put larger groups of people at risk.

Superior Intelligence. Nightmare scenarios depict what's known as the technological singularity, where superintelligent machines take over and permanently alter human existence through enslavement or eradication. Even if AI systems never reach this level, they can become more complex to the point where it's difficult to determine how AI makes decisions at times. This can lead to a lack of transparency around how to fix algorithms when mistakes or unintended behaviours occur.

REFERENCES

1. Digital financial assets in Russia. *TAdviser*. URL: https://tadviser.com/index.php/Article:Digital_financial_assets_in_Russia (last accessed: 01.02.2025).
2. India leads in AI deployment with 59 % adoption, according to IBM report. *IndiaAI*. URL: https://indiaai.gov.in/article/india-leads-in-ai-deployment-with-59-adoption-according-to-ibm-report (last accessed: 01.02.2025).
3. Russia's digital asset market growing at record pace, says Sberbank. *CCN*. URL: https://www.ccn.com/news/crypto/russias-digital-asset-market-record-pace-sberbank/ (last accessed: 01.02.2025).
4. Russia's digital ruble progress update: Soon to be used for transactions. *CoinLive*. URL: https://www.coinlive.com/news/russia-s-digital-ruble-progress-update-soon-to-be-used-for (last accessed: 01.02.2025).
5. Russian lawmakers approve use of digital assets in international transactions. *Reuters*. 2024. URL: https://www.reuters.com/business/finance/russian-lawmakers-approve-use-digital-assets-international-transactions-2024-02-27/ (last accessed: 01.02.2025).
6. The BRICS will use a gold standard. *VBL Gold Fix*. *Substack*. URL: https://vblgoldfix.substack.com/p/the-brics-will-use-a-gold-standard (last accessed: 01.02.2025).
7. VTB Bank and PSB conduct first test transfers of digital ruble. *Finextra*. URL: https://www.finextra.com/newsarticle/39691/vtb-bank-and-psb-conduct-first-test-transfers-of-digital-ruble (last accessed: 01.02.2025).
8. 1 in 10 vehicles will be autonomous by 2030. *TechRepublic*. URL: https://www.techrepublic.com/article/1-in-10-vehicles-will-be-autonomous-by-2030/ (last accessed: 01.02.2025).

https://doi.org/10.15407/akademperiodyka.545.082

RASPOPOV VIKTOR
Associate Professor,
PhD in Computer Science, Senior Researcher,
V.M. Glushkov Institute of Cybernetics of NAS of Ukraine
Kyiv, Ukraine

SOCIAL JUSTICE AND DIGITAL ECONOMY: UNLEASHING THE POTENTIAL OF EVERY INDIVIDUAL AS A KEY TO SUSTAINABLE SOCIETAL DEVELOPMENT

Introduction. Planet Earth is our common home. According to the concept of sustainable development formulated by world leaders at the historic international forum "Rio-92" in 1992 in Rio de Janeiro, Brazil, modern society, oriented towards sustainable growth, faces a crucial challenge: unlocking the potential of every child, regardless of their social background. History has shown that talent can emerge in any family — whether wealthy or impoverished — but without proper conditions, such talent may remain undiscovered. Therefore, creating an environment where every child can realize their abilities is of enormous significance

Cite: Raspopov Viktor. Social justice and digital economy: unleashing the potential of every individual as a key to sustainable societal development. https://doi.org/10.15407/akademperiodyka.545.082

not only for individuals but for society as a whole. One of the most successful examples of such support is the activity of the Junior Academy of Sciences of Ukraine (JAS), which fosters the scientific and creative potential of school students [1]. It is important to note that this initiative is directly related to the concepts of social justice and the digital economy, which open new opportunities for talent development.

Social Justice and Unlocking Children's Potential. Social justice implies equal rights and opportunities for all members of society, regardless of their background, wealth, or other factors. In the context of unlocking children's potential, this means that every child should have access to developmental opportunities, regardless of their socio-economic status. A society that upholds social justice seeks to eliminate barriers to quality education, science, and innovation [2].

JAS serves as one of the key instruments of social justice implementation in Ukraine, providing school students with equal access to advanced educational programs with the goal of future involvement in scientific research. This initiative allows talented children from various social backgrounds to gain access to cutting-edge knowledge and collaborate with leading scientists, significantly expanding their prospects. Additionally, participation in JAS programs fosters critical thinking, research skills, and problem-solving abilities in students, which are crucial elements of social mobility and sustainable development.

The Digital Economy as a Tool for Talent Development. The digital economy plays an increasingly vital role in educational processes and talent development. Thanks to modern digital technologies, school students can participate in scientific projects remotely, access global knowledge bases, and communicate with mentors and scientists from around the world. The Junior Academy of Sciences actively integrates digital tools that help children and adolescents master programming, artificial intelligence, robotics, and other promising fields [3].

Digital technologies help remove geographical and financial barriers, providing children from remote regions of Ukraine with access to quality education. A significant aspect of the digital economy is the creation of platforms for distance learning and interaction with the scientific community, enabling a larger number of students to engage in educational initiatives. For instance, JAS programs utilize virtual laboratories and online conferences, allowing students from rural areas and small towns to participate in high-level research on par with their peers from major scientific centers.

Blockchain Technology and Its Connection to Cryptocurrencies. Blockchain is a data storage technology that differs from traditional databases in its decentralized structure. In a conventional database, such as in banking systems, information is stored in a central location and managed by a single entity. In contrast, blockchain stores data simultaneously across multiple nodes (computers) in a network, making it nearly impervious to tampering or hacking.

How Does Blockchain Work?

1. Chain of Blocks Data in blockchain is stored in blocks linked sequentially. Each block contains a set of transactions and a reference to the previous block. This ensures that data cannot be altered without modifying the entire chain, which is virtually impossible due to the distributed nature of the system.

2. Decentralization Unlike centralized databases, blockchain is not controlled by a single server but by a network of computers (nodes). Each node stores a copy of the entire blockchain and participates in verifying new data. If an attempt is made to alter data in one node, the rest of the network will reject the modification.

3. Consensus Algorithms To add new transactions to the blockchain, network nodes must agree that the data is valid. This is achieved using consensus mechanisms such as **Proof-of-Work (PoW)**, which requires solving complex mathematical problems, or **Proof-of-Stake (PoS)**, where validators are chosen based on the number of tokens they hold.

How Is Blockchain Related to Cryptocurrencies?

Cryptocurrencies such as Bitcoin and Ethereum utilize blockchain as a decentralized database to store all transactions. Blockchain enables cryptocurrencies to function without banks or central governing authorities.

1. Transparency and Fraud Protection All blockchain transactions are public and verifiable. No one can alter or delete a transaction record, making cryptocurrency networks resistant to fraud.

2. Mining and Transaction Processing In Proof-of-Work networks, new blocks are created by miners who solve cryptographic puzzles. As a reward, they receive new cryptocurrency (e. g., Bitcoin). In Proof-of-Stake systems, validators are selected based on the amount of cryptocurrency they own, allowing them to confirm transactions.

3. Smart Contracts and Decentralized Applications Ethereum and other platforms support **smart contracts —** self-executing programs that automatically enforce agreements without intermediaries. This enables the creation of decentralized applications (DApps) that run on blockchain.

Conclusions. By integrating social justice principles with the opportunities of the digital economy and blockchain technology, we can create an inclusive, equitable, and forward-thinking society that unlocks the full potential of every individual. Governments, academic institutions, and private enterprises must continue investing in education, digital infrastructure, and blockchain innovations. This commitment will drive sustainable development, equipping future generations with the skills needed to thrive in an evolving technological landscape.

REFERENCES

1. Raspopov V.B. Learn to be a scientist. *Visnyk of the National Academy of Sciences of Ukraine*. 2012. No. 12. P. 44—54. URL: https://nasu-periodicals.org.ua/index.php/visnyk/article/view/5069 (last accessed: 01.02.2025).

2. Terpilovsky Y.O., Manzhula A.M., Raspopov V.B. Achievements of the Scientific and Educational Center of Applied Informatics of the NAS of Ukraine: *proceedings of the 10th All Ukrainian Scientific and Practical Conference «Scientific Youth-2022»*, Kyiv: KOMPRINT, 2022. P. 94—107.
3. Terpilovsky Y.O., Manzhula A.M., Raspopov V.B. Scientific and Educational Project Involving Academically Gifted Youth from the Junior Academy of Sciences of Ukraine in the Study of Natural Language and Informational Aspects of the Development Program for Living Organisms: proceedings of the International Scientific Conference «Information. Language. Intelligence». Kyiv; Warsaw: Ukrainian Language and Information Fund of the National Academy of Sciences of Ukraine, Institute of Slavic Studies of the Polish Academy of Sciences, 2023. P. 136—145.

https://doi.org/10.15407/akademperiodyka.545.087

SOVA OLENA
Associate Professor, Candidate of Economic Sciences,
Senior Research Fellow of the Department for problems
of social capital formation,
Institute for Demography and Life Quality Problems
of the National Academy of Sciences of Ukraine,
Kyiv, Ukraine
https://orcid.org/0000-0001-6386-6432

SOCIAL JUSTICE IN VIRTUAL SPACE

In the 21st century, digital technologies have become not only a tool for communication but also an environment in which social relations are formed, and the rights and responsibilities of citizens are realized. The virtual space is more than just a place for exchanging information; it is a new sphere of work, education, economic activity, as well as a space for civic engagement and human rights protection. However, just like in the real world, the digital sphere faces inequality, discrimination, and human rights violations, raising questions about the principles of social justice.

Today, the virtual space generates a number of socio-legal challenges: unequal access to digital services, algorithmic discrimination, issues of digital identity protection, freedom of speech, and cybersecurity. In Ukraine, these issues are particularly relevant, as the digital transformation of the economy and society continues amid wartime challenges and the need to adapt to European legal standards. Among the global issues of social justice in the virtual space, the following can be highlighted:

Cite: Sova Olena. Social justice in virtual space. https://doi.org/10.15407/akademperiodyka.545.087

1. Digital inequality — unequal access to the internet, technology, and digital literacy.

2. Algorithmic discrimination — hidden biases in artificial intelligence that affect different social groups.

3 The right to digital identity — protection of personal data and the problem of digital control.

4. Freedom of speech on the internet — balancing the fight against disinformation and censorship.

5. Cybersecurity and legal protection — preventing cyberbullying, online fraud, and privacy violations.

6. Social protection in the digital economy — the rights of freelancers, gig economy workers, and remote employees.

7. Activation of volunteering and social entrepreneurship — leveraging digital platforms to enhance civic initiatives, humanitarian aid, and socially responsible business.

8. State regulation of digital platforms — ensuring social equality in the era of digitalization.

The modern world is characterized by the rapid development of remote forms of interaction in all spheres of public life, a transformation that serves different interests of social relationship participants and introduces new governance methods [4, p. 62].

One of the defining challenges is digital marginalization. In the past, access to education, employment, or public services depended primarily on physical resources, but today, a person's digital status can become a barrier. Those who lack permanent internet access, smartphones, or digital skills find themselves on the margins of modern society. This affects not only the elderly but also vulnerable social groups that struggle to compete in the digital economy. Today, the principle of fair distribution must be complemented by a high level of social, spiritual, cultural, environmental, and other human rights protection [3, p. 74].

The transformation of the ideology of social justice in wartime conditions involves the following [5, p. 47—48]:

- increasing social support for the most vulnerable segments of the population while simultaneously encouraging an active position in the labor market among the able-bodied population;

- enhancing the social responsibility of businesses in accordance with the Sustainable Development Goals;
- developing social entrepreneurship, including volunteering, humanitarian aid, and supporting the state in fulfilling part of its social functions.

Social justice is one of the fundamental principles of humanizing socio-economic policy, which ensures an equitable distribution of resources and benefits among all members of society [6].

It is also important to mention the psychological dimension of social injustice in the virtual space. Social media algorithms, designed to create personalized content, can actually reinforce information bubbles and contribute to social polarization. The main causes of internet addiction include an inability to establish and maintain healthy social and psychological relationships in real life, as well as difficulty distinguishing between normal and abnormal behavior [1, p. 63—64].

Virtual communication often deepens social isolation, distorts perceptions of reality, and can exert psychological pressure on specific groups. For example, young people influenced by unrealistic standards of success and beauty in social networks experience high levels of stress and declining self-esteem. Account blocking without explanation, content deletion based on vague criteria, and censorship on social media create a situation where the right to exist in the virtual space is controlled not by state laws but by commercial corporations.

In the physical world, a person can change their image, move to another city, or start a new life stage. However, in the virtual space, their past can catch up with them at any moment. Old posts, comments, or even careless statements made years ago can affect a person's future. The development of virtual reality is one of the most striking examples of how modern technological advancements correlate with socio-cultural processes in society [2, p. 63].

A distinctive feature of social structure is increased social mobility, particularly among the middle class, which is constantly shifting in social, geographical, and professional aspects. In the

context of social stratification, a person within a social group loses significance as a stratum-forming factor, while social boundaries become increasingly blurred [7, p. 28].

Thus, social justice in the virtual space is not only a matter of access to technology but also a struggle for equal rights in the digital economy, the protection of personal data, humanism, and ethical virtual communications. These challenges require not only public attention but also a clear state policy that will ensure fair rules for all participants in the digital society.

REFERENCES

1. Hrechanovska O., Mehem O., Potapiuk L. The impact of social networks on the psychological state and self-esteem of Ukrainian youth. *Scientific Notes of Taurida National V.I. Vernadsky University.* Series: Psychology. 2023. Vol. 34, No. 73/4. P. 60—66. https://doi.org/10.32782/2709-3093/2023.4/11
2. Matyash S., Kuznetsova L. Virtual and its sociocultural factors. *Current Problems of Philosophy and Sociology*. 2023. N 10. P. 59—64. https://doi.org/10.32782/apfs.v043.2023.10
3. Kosovych V. Socio-economic justice: opportunities of expanding its understanding through law enforcement analysis. *Věda a perspektivy.* 2023. Vol. 3, No. 22. P. 69—80. https://doi.org/10.52058/2695-1592-2023-3(22)-69-80
4. Lutsenko V., Pikylia T. Legal security of digital transformation in Ukraine. *Uzhhorod National University Herald.* Series: Law. Uzhhorod, 2024. Vol. 5, No. 86. P. 61—67. https://doi.org/10.24144/2307-3322.2024.81.1.9
5. Petrunenko Ia. Transformation of the ideology of social justice in the conditions of regulating the economy of the war period. *Subcarpathian Law Herald*. 2023. Vol. 2, No. 49. P. 44—49. https://doi.org/10.32782/pyuv.v2.2023.8
6. Rym R., Tsisaryk V., Hnatyshyn Yu. Humanism as the foundation of sustainable socio-economic policy. *Academic Visions*. 2023. No. 19. https://doi.org/10.5281/zenodo.13351591
7. Vornikov V. The peculiarities of understanding the concept of the self-organizing information society: imaginary (figuratively)-semiotic dimension. *Visnyk of the Lviv University.* Series Philos.-Political Studies. 2023. No. 50. P. 22—29. https://doi.org/10.30970/PPS.2023.50.3

https://doi.org/10.15407/akademperiodyka.545.091

ФІЛЬКОВСЬКИЙ СЕРГІЙ
аспірант,
Інститут економіки промисловості НАН України
м. Київ, Україна
https://orcid.org/0009-0000-5835-2947

ПРОБЛЕМАТИКА DeFi-КРАУДФАНДИНГУ У ФІНАНСУВАННІ ВІДНОВЛЕННЯ ДЕОКУПОВАНИХ ТЕРИТОРІЙ

Три роки широкомасштабної війни вартували Україні не тільки значних людських і матеріальних втрат і збитків, а накопичили сотні квадратних кілометрів зруйнованих територій. Особливо це стосується деокупованих територій та територій активних бойових дій. Для забезпечення хоча б мінімального рівня життя, не кажучи про відновлення повноцінної життєдіяльності територіальних громад, необхідне першочергове відновлення критичної та соціально-економічної інфраструктури. На жаль, під час війни у держави для цього не вистачає коштів, що обумовлює пошук громадами донорів та інвесторів для реалізації нагальних проєктів відбудови.

«Коли йдеться про втілення суспільно важливих проєктів, головним викликом завжди залишається

Cite: Filkovskyi Serhii. The problems of DeFi-crowdfunding in financing the reconstruction of decommissioned territories. https://doi.org/10.15407/akademperiodyka.545.091

фінансування. Знайти підтримку у великих донорів — складно, державні програми часто мають обмежений бюджет, а власних ресурсів ініціативам зазвичай бракує. Саме тому краудфандинг стає тим інструментом, який дозволяє об'єднати людей навколо спільної ідеї й залучити кошти на її реалізацію» [3]. І хоча в Україні краудфандинг набуває все більшої популярності, однак органам місцевого самоврядування все ж складно залучити у такий спосіб мільйонні інвестиції чи гранти, оскільки це потребує впевненої фінансової грамотності. Саме тут виникає потреба у новому підході до грошових операцій, що усуває необхідність у посередниках — банках, урядах чи фінансових установах, тобто за допомогою децентралізованих краудфандингових кампаній.

Сучасні технології докорінно змінили фінансову систему, і одним із найпомітніших феноменів останніх років стало децентралізоване фінансування — DeFi (Decentralized Finance). Замість традиційної банківської системи всі процеси, включно з кредитами, страхуванням та переказом коштів, виконуються автоматизовано через смартконтракти — спеціальні програми на блокчейні, які гарантують виконання фінансових операцій без можливості їх підробки або зміни.

У цьому контексті DeFi-краудфандинг як інструмент залучення коштів через децентралізовані платформи може стати новим знаряддям до економічного відродження насамперед деокупованих територій. Він дає можливість отримувати фінансування від людей та організацій з усього світу напряму, без контролю традиційних фінансових посередників. Прикладом успішного застосування таких технологій є фонд «Повернись живим», який приймає пожертви у криптовалюті. Така практика забезпечує оперативне фінансування оборонних, гуманітарних і відновлювальних ініціатив. Головною перевагою криптоплатежів є їхня швидкість, незалежність від фінансових установ і прозорість використання коштів.

Метою цього дослідження є визначення переваг та викликів DeFi-краудфандингу, а також окреслення його перспектив у фінансуванні відновлення деокупованих територій України.

Сучасна наукова думка демонструє існування трьох підходів до визначення краудфандингу: як бізнес-моделі, як відкритого заклику для залучення фінансових ресурсів та як ініціативи збору коштів на певний проєкт [1, с. 15]. Так само розрізняють і такі його види: благодійний краудфандинг (Crowddonating), краудфандинг на основі винагороди (Reward-based crowdfunding), краудінвестинг (Crowdinvesting), краудлендинг (Crowdlending), торгівля рахунками-фактурами, децентралізований краудфандинг (Decentralized crowdfunding) [2, с. 7].

DeFi-краудфандинг вирізняється своїм підходом до фінансування проєктів, що зменшує витрати, підвищує прозорість і створює умови для тіснішої взаємодії між ініціаторами та спільнотами. Якщо провести аналогію, то традиційна фінансова система — це великий банк, де ви зберігаєте гроші, а будь-яка транзакція проходить через його перевірку. DeFi натомість схожий на цифровий кооператив, де кожен учасник самостійно контролює свої активи, а операції відбуваються напряму між користувачами за прозорими правилами.

Даний підхід передбачає використання блокчейн-технологій для здійснення фінансових операцій без залучення традиційних посередників, таких як банки чи урядові установи. Автоматизовані алгоритми у вигляді смартконтрактів забезпечують автономність, прозорість і незмінність транзакцій, що є важливим фактором у контексті сучасного цифрового середовища.

Однією з ключових переваг DeFi є можливість швидкого й відкритого фінансування різних ініціатив без бюрократії та територіальних обмежень. Це особливо актуально для України, яка після масштабних воєнних руйнувань потребує ефективних механізмів збору коштів на відновлення деокупованих територій.

З огляду на виклики, з якими стикається Україна, особливо у сфері відновлення деокупованих територій, DeFi-краудфандинг відкриває нові можливості для залучення коштів з усього світу. Його ефективність базується на швидкості транзакцій, прозорості руху фінансових ресурсів і відсутності бюрократичних бар'єрів. Зважаючи на це, актуальним є дослідження потенціалу DeFi-краудфандингу для фінансування суспільно значущих проєктів.

Застосування смартконтрактів дає можливість автоматизувати процеси збору і розподілу коштів безпосередньо між користувачами, мінімізуючи ризики корупції та неефективного використання фінансів. Вони забезпечують чітке виконання умов пожертвування та гарантують, що кошти будуть використані згідно з попередньо визначеними сценаріями.

Додатковим інструментом для залучення донорів є токенізація активів і NFT. Випуск благодійних NFT може стимулювати фінансування проєктів шляхом залучення міжнародної аудиторії та створення унікальних цифрових активів, що символізують підтримку відповідної ініціативи.

Незважаючи на очевидні переваги DeFi-краудфандингу, його широке впровадження стикається з низкою викликів, які необхідно враховувати під час оцінки його ефективності та можливостей інтеграції в економічну систему України. До основних перешкод належать: регуляторна невизначеність, питання безпеки й довіри, а також перспективи розвитку та інтеграції цих технологій у державні ініціативи.

Регуляторна невизначеність. Попри значний потенціал DeFi-краудфандингу, його використання стикається з проблемою відсутності чітких регуляторних норм в Україні. Правовий статус криптовалют та смартконтрактів у сфері фінансування благодійних ініціатив залишається невизначеним, що створює додаткові виклики для їх широкого впровадження.

Безпека та довіра. Одним із ключових аспектів використання DeFi-платформ є питання безпеки. Відсутність центра-

лізованого контролю збільшує ризик шахрайства, зломів та втрати коштів. Тому розробка ефективних механізмів захисту користувачів та підвищення довіри до таких фінансових рішень є важливим напрямом подальших досліджень.

Перспективи розвитку та інтеграції DeFi-краудфандингу в Україні залежать від регуляторних змін і готовності держави інтегрувати ці технології у фінансову систему. Співпраця між урядом, благодійними організаціями та DeFi-платформами може сприяти створенню ефективних механізмів збору коштів для відновлення деокупованих територій. Враховуючи світові тенденції, інтеграція блокчейн-технологій у державні ініціативи є питанням часу.

Отже, DeFi-краудфандинг є перспективним інструментом фінансування суспільно важливих проєктів, зокрема відновлення деокупованих територій України. Його переваги включають високу швидкість транзакцій, прозорість та усунення фінансових посередників. Водночас існують виклики, пов'язані з регуляторною невизначеністю та питаннями безпеки. Подальший розвиток DeFi-краудфандингу потребує адаптації законодавства й впровадження механізмів захисту користувачів, що сприятиме ефективному використанню цієї технології для економічного відродження країни.

Завдяки впровадженню певних правових і безпекових механізмів та розробці стратегії співпраці з державою DeFi-краудфандинг може стати ефективним інструментом фінансування відновлення, забезпечуючи глобальний доступ до пожертв. Основою для створення більш системних DeFi-рішень може стати досвід благодійних фондів, що працюють з криптовалютами.

ЛІТЕРАТУРА

1. Волосович С.В., Василенко А.В. Краудфандінг як інноваційний метод фінансування проєктів. *Modern Economics*. 2017. № 4. URL: https://modecon.mnau.edu.ua/issue/5-2017/UKR/volosovych.pdf
2. Мазаракі А., Волосович С. Краудфандинг благодійності в умовах протидії збройній агресії. *Scientia fructuosa*. 2023. № 1. С. 4—16. https://doi.org/10.31617/1.2023(147)01
3. Подольська В. Краудфандинг став поширенішим з початку повномасштабного вторгнення, просто більшість не називає це так. *Громадський простір*. 24.02.2025. URL: https://www.prostir.ua/?library=kraudfandynh-stav-poshyrenishym-z-pochatku-povnomasshtabnoho-vtorhnennya-prosto-bilshist-ne-nazyvaje-tse-tak-viktoriya-zatsnova-pro-kraudfandynh-sposoby-zaluchennya-donatoriv-ta-vyklyky-h (дата звернення: 01.02.2025).

ДОПОВІДАЧІ ТА УЧАСНИКИ

Володимир Устименко, директор Державної установи «Інститут економіко-правових досліджень імені В.К. Мамутова Національної академії наук України», член-кореспондент НАН України, член-кореспондент НАПрН України

Джеймс Рамсден, баристер, королівський радник, партнер-засновник Astraea-group (Лондон), міжнародний експерт із крипторегулювання та AML

Христина Ханас, PhD, соліситор, міжнародний експерт Astraea-group (Лондон)

Чарльз Мак, Школа права та соціальних наук Університету Роберта Гордона, науковий співробітник Оксфордського університету, стипендіат Форуму трансатлантичного технологічного права Стенфордської школи права, науковий співробітник Центру китайського та порівняльного права Міського університету Гонконгу, почесний співробітник Азійського інституту міжнародного фінансового права Університету Гонконгу

Тетяна Дмитренко, доктор економічних наук, голова ГО «Сучасна українська цифрова наука», експерт міжнародних проєктів ООН з протидії відмивання коштів (AML)

Тетяна Гудіма, доктор юридичних наук, міжнародний експерт з питань регулювання віртуальних активів, голова координаційного наукового центру з питань штучного інтелекту Донецького наукового центру НАН України та МОН України

Олег Шаулько, соліситор, партнер ЮФ «Кеннедіз» (Лондон), міжнародний експерт з транскордонних спорів та спорів у сфері криптовалют

Артемій Володін, віцепрезидент AIEI (Міжнародна асоціація етики та доброчесності AI)

Олександр Черних, адвокат, офіційний представник НААУ в Сполученому Королівстві, міжнародний експерт врегулювання криптоактивів, молодший науковий співробітник Державної установи «Інститут економіко-правових досліджень імені В.К. Мамутова Національної академії наук України»

Владислав Цвіркун, кібердетектив, експерт з розшуку і відслідковування активів, член команди міжнародних експертів Global Ledger

SPEAKERS AND PARTICIPANTS

Volodymyr Ustymenko, Director of the State Institution "V.K. Mamutov Institute of Economic and Legal Research of the National Academy of Sciences of Ukraine", Corresponding Member of the NAS of Ukraine, Corresponding Member of the NALS of Ukraine

James Ramsden, Barrister, King's Counsel, Founding Partner of Astraea-group (London), International Expert in Cryptoregulation and AML

Khrystyna Khanas, PhD, Solicitor, International Expert of Astraea-group (London)

Charles Mak, School of Law and Social Sciences, Robert Gordon University, Research Fellow, University of Oxford, Fellow of the Transatlantic Technology Law Forum, Stanford Law School, Research Fellow, Center for Chinese and Comparative Law, City University of Hong Kong, Honorary Fellow of the Asian Institute of International Financial Law, University of Hong Kong

Tetyana Dmytrenko, Doctor of Economics, Head of the NGO "Modern Ukrainian Digital Science", expert in international UN projects on combating money laundering (AML)

Tetiana Hudima, Doctor of Laws, International Expert in the Regulation of Virtual Assets, Head of the Coordination Scientific Center for Artificial Intelligence of the Donetsk Scientific Center of the NAS of Ukraine and MES of Ukraine, Senior researcher State Institution "V.K. Mamutov Institute of Economic and Legal Research of the National Academy of Sciences of Ukraine"

Oleg Shaulko, Solicitor, Partner Kennedys Law Firm (London), international expert on cross-border disputes and disputes in the field of cryptocurrencies

Artemiy Volodin, Vice-President of AIEI (International Association for AI Ethics and Integrity)

Oleksandr Chernykh, Attorney, Official Representative of the Ukrainian National Bar Association in the United Kingdom, International Expert in the Regulation of Crypto-Assets, junior researcher State Institution "V.K. Mamutov Institute of Economic and Legal Research of the National Academy of Sciences of Ukraine"

Vladyslav Tsvirkun, cyber detective, expert in asset tracing and tracking, team of international experts Global Ledger

ЗМІСТ

The collection contains materials presented at the international conference "Social Justice and the Digital Economy. 2025", dedicated to discussing the challenges of the digital economy. The conference brought together experts in the fields of digital finance, cryptocurrencies, sanctions policy, and artificial intelligence, as Ukraine currently needs modern legal mechanisms to regulate the digital economy (crypto assets and artificial intelligence in particular), which will contribute not only to economic stability but also to increasing confidence in the national financial market in the context of global economic changes.

For specialists in the digital economy and international law who are interested in the processes of digital transformation of society and the application of modern technologies for this purpose.

Наукове видання

Державна установа «Інститут економіко-правових досліджень
імені В.К. Мамутова Національної академії наук України»

СОЦІАЛЬНА СПРАВЕДЛИВІСТЬ ТА ЦИФРОВА ЕКОНОМІКА. 2025

**ЗБІРНИК МАТЕРІАЛІВ
МІЖНАРОДНОЇ
НАУКОВО-ПРАКТИЧНОЇ
КОНФЕРЕНЦІЇ
28.05.2025, Київ**

SOCIAL JUSTICE AND DIGITAL ECONOMY. 2025

**PUBLICATION OF MATERIALS
OF THE INTERNATIONAL
SCIENTIFIC AND PRACTICAL
CONFERENCE
28.05.2025, Kyiv**

Електронне видання

Редагування *Ірини Яловничої*

Художнє оформлення *Ольги Бурдік*

Виготовлення ілюстрацій
і комп'ютерна верстка *Олександра Кисельова*

Підп. до друку 18.08.2025. Формат 60 × 84/16.
Гарн. Candara. Об'єм даних 14,42 МБ.
Зам. № 7752е.

Видавець і виготовлювач
Видавничий дім «Академперіодика» НАН України
01024, Київ, вул. Терещенківська, 4

Свідоцтво про внесення до Державного реєстру суб'єктів
видавничої справи серії ДК № 544 від 27.07.2001


ВИДАВНИЧИЙ ДІМ
АКАДЕМПЕРІОДИКА