НАЦІОНАЛЬНА АКАДЕМІЯ ПРАВОВИХ НАУК УКРАЇНИ
НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ
ІННОВАЦІЙНОГО РОЗВИТКУ НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК
УКРАЇНИ

# ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ РОЗВИТКУ ТЕХНОЛОГІЙ ЦИФРОВОЇ ЕКОНОМІКИ ТА СУСПІЛЬСТВА

Колективна монографія

Харків
2023

УДК 346.2:004
П 68
JEL K22, K24, O33, H54, O34, O38, O43

*Рекомендовано до друку вченою радою*
*Науково-дослідного інституту правового забезпечення інноваційного розвитку*
*Національної академії правових наук України*
*(протокол № 8 від 30 жовтня 2023 року)*

***Рецензенти:***

**І. А. Яковюк** – доктор юридичних наук, професор, професор кафедри права Європейського Союзу Національного юридичного університету імені Ярослава Мудрого

**А. В. Домбровська** – кандидатка юридичних наук, доцентка, доцентка кафедри патентознавства та основ правозастосовної діяльності Харківського національного університету міського господарства імені О. М. Бекетова

**Г. М. Шовкопляс** – кандидатка юридичних наук, доцентка, доцентка кафедри господарського права Національного юридичного університету імені Ярослава Мудрого

***Колектив авторів:***

*М. Г. Хаустова* – розд. 1, *Д. І. Шматков* – розд. 2, *І. О. Мамаєв* – підрозд. 3.1 розд 3, розд. 4, *П. М. Дуравкін* – підрозд. 3.2 розд. 3 (співавт. І. *І. Гафич*), *І. І. Гафич* – підрозд. 3.2 розд. 3 (співавт. *П. М. Дуравкін*), *К. В. Єфремова* – розд. 5, *Є. А. Новіков* – розд. 6, *О. В. Шаповалова* – розд. 7.

П 68 **Правове забезпечення розвитку технологій цифрової економіки та суспільства** : монографія / за ред. О. В. Шаповалової, К. В. Єфремової. – Харків: НДІ прав. забезп. інновац. розвитку НАПрН України, 2023. – 292 с.

**ISBN 978-617-7806-46-1**

Монографію присвячено дослідженню питань правового забезпечення цифрової трансформації суспільства та економіки на шляху до членства в ЄС в умовах відновлення економіки України. Розкриті питання застосування міжнародного досвіду реалізації програм та стратегій цифровізації в державній політиці України. Робота містить окремі дослідження з актуальних напрямків правового забезпечення права інтелектуальної власності на цифрових платформах, розкрито правові проблеми забезпечення ефективності регулювання персональних даних та впровадження цифрових технологій.

Видання призначене для на фахівців, науковців, викладачів, аспірантів, студентів закладів вищої освіти, а також, усіх тих, хто цікавиться проблемами правового регулювання цифрової економіки та суспільства, використанням цифрових технологій.

**Ключові слова:** цифровізація суспільства, цифрова економіка, управління цифровими інфраструктурами, право інтелектуальної власності, захист персональних даних, публічні реєстри, цифрові послуги, мережі трансферу технологій, цифровізація фінансів.

ISBN 978-617-7806-46-1

NATIONAL ACADEMY OF LEGAL SCIENCES OF UKRAINE
SCIENTIFIC AND RESEARCH INSTITUTE
OF PROVIDING LEGAL FRAMEWORK FOR THE INNOVATIVE
DEVELOPMENT

# LEGAL SUPPORT FOR THE DEVELOPMENT OF DIGITAL ECONOMY AND SOCIETY TECHNOLOGIES

Monograph

*Team of authors:*
Maryna Khaustova, Daniil Shmatkov, Illia Mamaiev, Pavlo Duravkin,
Ivan Hafych, Kateryna Yefremova, Yevhen Novikov, Olha Shapovalova

UDC [346.2:330.341.1]:004
JEL K22, K24, O33, H54, O34, O38, O43

The monograph is dedicated to researching issues of legal support for the digital transformation of society and the economy on the way to EU membership in the conditions of economic recovery of Ukraine. The issues of application of international experience in the implementation of digitalization programs and strategies in the state policy of Ukraine are revealed. The work contains separate studies on the current directions of legal enforcement of intellectual property rights on digital platforms, and addresses legal problems related to ensuring the effectiveness of personal data regulation and the implementation of digital technologies.

This publication is intended for professionals, researchers, educators, postgraduate students, university students, and anyone interested in the problems of legal regulation of the digital economy and the use of digital technologies.

**Keywords:** digitalization of society, digital economy, management of digital infrastructures, intellectual property rights, personal data protection, public registries, digital services, technology transfer networks, digitalization in financial services.

# ЗМІСТ

# ВСТУП

Монографія підготовлена колективом авторів Науково-дослідного інституту правового забезпечення інноваційного розвитку Національної академії правових наук України за результатами виконання фундаментальної наукової теми «Правове забезпечення розвитку технологій цифрової економіки і суспільства» (РК УкрІНТЕІ № 0119U103826) і об'єднує положення напрацювань науковців, підготовлених протягом всього періоду фундаментального дослідження 2020–2023 років.

Актуальність тематики дослідження підкреслюється викликами, що постали перед Україною через пришвидшену євроінтеграцію за визначеними пріоритетними напрямками, серед яких забезпечення цифрової трансформації економіки та суспільства.

Колективна монографія містить окремі дослідження з актуальних напрямків державної політики цифровізації економіки та суспільства в умовах відновлення України щодо ефектів цифрової трансформації, ризиків та пропозицій визначення стратегічних напрямів процесу післявоєнного відновлення України; дослідження ролі інтелектуальної власності на цифрових платформах щодо автоматизації саморегулювання в галузі авторського права, ліцензійних угод на використання інтелектуальної власності користувачів на цифровому ринку, правових аспектів демонстрування винаходів оборонного призначення на українських краудфандингових платформах; нормативно-правового забезпечення опрацювання даних від становлення і базових засад регулювання неперсональних даних до визначення переваг Єдиного цифрового ринку в контексті опрацювання та вільного руху даних та ступінь адаптації вітчизняного регулювання до вимог ЄС; правового забезпечення впровадження цифрових технологій у контексті цифрової трансформації фінансових послуг та впливу цих

процесів на економічну безпеку України. Окремо приділено увагу посиленню цифрової трансформації у напрямі зеленого курсу та запровадженню в України застосування індексу цифрової економіки та суспільства; досліджено мережи трансферу технологій в аспекті національної безпеки. А також оприлюднені напрацювання щодо реалізації інформаційно-комунікаційної та правоохоронної функцій публічних електронних реєстрів як юридичних гарантій реалізації цифрових прав.

У зв'язку з обраним Україною євроінтеграційним шляхом та стрімким розвитком нових цифрових технологій виникає нагальна необхідність у зміні правового регулювання цифрової економіки, вільного руху та захисту даних, що ставить актуальним питання щодо узагальнення розгалуженого регуляторного масиву, якому має відповідати Україна. Виявлення структурних розбіжностей має сприяти кращому розумінню процесу гармонізації українського та європейського законодавства, а приведення вітчизняної нормативно-правової бази до європейських стандартів сприятиме оперативній адаптації бізнесу до актуальних конкурентних вимог, що є важливим в контексті економічної відбудови.

Колективну монографію призначено для фахівців і наукових працівників, юристів, викладачів, аспірантів, студентів закладів вищої освіти та всіх, хто цікавиться правовими проблемами забезпечення розвитку технологій цифрової економіки та суспільства.

Колектив авторів висловлює щиру подяку рецензентам за позитивну оцінку монографії.

**Сергій ГЛІБКО**
**Катерина ЄФРЕМОВА**

# 1. ДЕРЖАВНА ПОЛІТИКА ЦИФРОВІЗАЦІЇ СУСПІЛЬСТВА В УМОВАХ ВІДНОВЛЕННЯ УКРАЇНИ

## 1.1. Поняття цифровізації (цифрової трансформації) – національні та міжнародні підходи

Цифровізація – у сучасній науці та практиці визначається як провідний напрям розвитку людської цивілізації, що формує більш інклюзивне суспільство та ефективні механізми управління, підвищує якість та охоплення державних та адміністративних послуг, розширює доступ до охорони здоров'я та освіти, банківських послуг, визначає найкращий спосіб співпраці людей, а також дає змогу скористатися більшим розмаїттям товарів за нижчими цінами. Сучасні геополітичні процеси, подальша інтеграція України у міжнародний світовий простір та у Європейську спільноту довели важливість та актуальність цифрових технологій для добробуту населення, ефективність реалізації стратегічних напрямів та розвитку економік. Використання цифровізації у країнах світу вже протягом тривалого часу є об'єктивною потребою сьогодення[1].

В Україні також проводиться активна законодавча робота у цьому напрямі. Так, 03 березня 2021 року Кабінет Міністрів України своєю Постановою № 179 затвердив Національну економічну стра-

[1] Хаустова М. Г. Поняття цифровізації: національні та міжнародні підходи. *Право та інновації.* 2022. № 2 (38). С. 7. URL: https://doi.org/10.37772/2518-1718-2022-2(38)-1.

тегію на період до 2030 року, у якій визначаються орієнтири, принципи та цінності в економічній політиці, серед яких вказується на необхідність подальшого розвитку ефективної цифрової сервісної держави та компактних державних інститутів (розвиток цифрової економіки як одного із драйверів економічного зростання України)[1].

Крім того, також 03 березня 2021 року Кабінет Міністрів України своїм розпорядженням № 167-р схвалив Концепцію розвитку цифрових компетентностей, а також затвердив план заходів з її реалізації. Ухвалення цієї Концепції стало стратегічним кроком вперед у побудові цифрової держави. Основною її метою є визначення пріоритетних напрямів і основних завдань з питань розвитку цифрових навичок та цифрових компетентностей, підвищення рівня цифрової грамотності населення, в умовах розвитку цифрової економіки та цифрового суспільства на період до 2025 року. В документі, зокрема вказується, що реалізація Концепції дасть змогу прискорити процеси цифрової трансформації в Україні; суттєво підвищити рівень цифрових навичок та цифрових компетентностей в суспільстві, а також рівень конкурентоспроможності держави та якість людського капіталу тощо[2].

Використання цифрової економіки для української держави набуває все більшої актуальності. Як слушно зазначають дослідники, у цифровій економіці базою для створення нових продуктів, цінностей, властивостей, унікальних систем і процесів визнаються цифрові технології[3]. Це підтверджується й Економічною стратегією України 2030, зокрема, відповідно до підпункту 6.2.2 «Цифрові тренди. Виклики та можливості для України» пункту 6.2, який має назву «Укра-

[1] Національна економічна стратегія на період до 2030 року : затв. постановою Кабінету Міністрів України від 03.03.2021 р. № 179. URL: https://zakon.rada.gov.ua/laws/show/179-2021-п#Text.

[2] Концепція розвитку цифрових компетентностей: схв. розпрядженням Кабінету Міністрів України від 03.03.2021 р. № 167-р. URL: https://zakon.rada.gov.ua/laws/show/167-2021-р#Text.

[3] Чудак О. М. Вплив цифровізації на адміністрування податків і зборів в Україні. *Право та інновації*. 2022. № 2 (38). С. 71. URL: https://doi.org/10.37772/2518-1718-2022-2(38)-9.

їна 2030Е – країна з розвинутою цифровою економікою» – дані стають активом, зокрема, збирання, опис, зберігання та опрацювання даних дають змогу отримувати цінну інформацію для використання в ділових процесах, суспільному житті, роботі держави, а вміння працювати з даними та їх аналізувати – це можливість першим отримувати цінні ринкові «інсайти», тобто бути конкурентоздатнішим[1].

Отже, сьогодні такі сфери життєдіяльності як економіка та бізнес, податкові відносини, медицина, політичні процеси, безпека, освіта, транспорт, екологія, адміністративні послуги, підприємницька діяльність неможливо уявити без використання інформаційно-комунікаційних технологій. У нових геополітичних умовах переваги в результаті технологічних і цифрових інновацій, отримує держава, в якій розвиваються, взаємодіють, удосконалюються і зростають усі складові економіки[2]. Саме тому сучасний етап розвитку багатьох країн, зокрема і України, пов'язаний з пошуком та переходом на нову модель економічного розвитку, в основу якої покладено використання інтелектуального і творчого потенціалу людської особистості.

Провідною метою цифровізації є досягнення цифрової трансформації існуючих та створення нових галузей економіки, а також трансформація існуючих сфер життєдіяльності у нові модернізовані та актуальні. Пріоритет можливий тоді, коли ідеї, дії, ініціативи та програми, які стосуються цифровізації, будуть інтегровані у національні, регіональні, галузеві стратегії і програми розвитку. Цифровізація є визнаним механізмом економічного зростання завдяки здатності технологій позитивно впливати на ефективність, результативність, вартість та якість економічної політики держави[3].

---

[1] Економічна стратегія України 2030. Український інститут майбутнього. URL: https://strategy.uifuture.org.

[2] Цифрова економіка: тренди, ризики та соціальні детермінанти. Центр Разумкова. Київ: Заповіт, 2020. С. 4. URL: https://razumkov.org.ua/uploads/article/2020_digitalization.pdf.

[3] Соснін О. Цифровізація як нова реальність України. Юридичний вісник України. 2020. № 1. С. 46. URL: https://lexinform.com.ua/dumka-eksperta/tsyfrovizatsiya-yak-nova-realnist-ukrayiny/.

Так, у резюме до пункту 6.2 «Україна 2030Е – країна з розвинутою цифровою економікою» Економічної стратегії України 2030 зазначається, що цифровізація (з англ. digitalization) – це впровадження цифрових технологій в усі сфери життя: від взаємодії між людьми до промислових виробництв, від предметів побуту до дитячих іграшок, одягу тощо. Це перехід біологічних та фізичних систем у кібербіологічні та кіберфізичні (об'єднання фізичних та обчислювальних компонентів). Перехід діяльності з реального світу у світ віртуальний (онлайн)[1]. Ще одне визначення наводиться у Енциклопедії інформаційних наук і технологій, в якій зазначається, що «цифровізація – це інтеграція цифрових технологій у повсякденне життя суспільства шляхом оцифровки всього, що можна оцифрувати»[2]. Крім того, цифровізація означає комп'ютеризацію систем і робочих місць для більшої легкості та доступності[3]. У свою чергу, один із засновників і виконавчих директорів Agile Elephant Девід Террар зазначав, що «цифрова трансформація» – це процес переходу до нових способів роботи і мислення з використанням цифрових, соціальних, мобільних і нових технологій, що передбачає зміну лідерства, інше мислення заохочення інновацій і нових бізнес-моделей, оцифрування активів і розширення використання технологій для покращення досвіду співробітників, клієнтів, постачальників, партнерів і зацікавлених сторін[4].

Виходячи з вищезазначеного, важливо підкреслити, що поняття «цифровізація» та «цифрова трансформація» не мають чіткого визначення. Однак, можливо зазначити, що вони між собою пов'язані. Так, цифровізація більш загальне поняття, яке охоплює багато мето-

[1] Економічна стратегія України 2030. Український інститут майбутнього. URL: https://strategy.uifuture.org.

[2] Encyclopedia of Information Science and Technology, Fourth Edition (10 Volumes). IGI Global, June. 2017. 8104 p. URL: https://www.igi-global.com/dictionary/it-strategy-follows-digitalization/7748.

[3] Osarenkhoe Aihie, Fjellström Daniella. The Oxymoron of Digitalization: A Resource-Based Perspective. *Journal of Information Technology Research (JITR).* 2021. No. 14 (4). URL: https://www.igi-global.com/article/the-oxymoron-of-digitalization/271802.

[4] What is Digital Transformation? Enterprise Digital Summit. London, 23-24 Nov. 2016. URL: https://www.theagileelephant.com/what-is-digital-transformation/.

дик, а цифрова трансформація – це процес, завдяки якому організації з використанням цифрових технологій переходять на новий рівень не тільки виробництва, а й відношення між партнерами, клієнтами та працівниками. Цифровізація виступає фундаментом цифрової економіки. Саме тому цифровізація розглядається як важливий елемент сталого розвитку економіки та суспільства, а такі технології як інтернет речей (IoT), хмарні технології, електронна ідентифікація (eID) та штучний інтелект (AI) можуть сприяти досягненню Глобальних Цілей Сталого Розвитку Організації Об'єднаних Націй до 2030 року[1].

При цьому слід враховувати, що термін «цифровізація» використовується у вузькому та широкому значеннях. Так, під цифровізацією у вузькому сенсі розуміється перетворення інформації в цифрову форму, що у більшості випадків призводить до зниження витрат, та появи нових можливостей тощо. Велика кількість конкретних перетворень інформації у цифрову форму призводить до суттєвих позитивних наслідків, які обумовлюють застосування терміну цифровізації у широкому сенсі. Як перехід до цифрової інформації всіх сторін економічного та соціального життя, цифровізація з простого методу покращення різних приватних сторін життя перетворюється у драйвер світового суспільного розвитку, який забезпечує підвищення ефективності економіки та покращення рівня життя. Цифровізацію у широкому сенсі можливо розглядати як тренд ефективного світового розвитку тільки у тому випадку, якщо цифрова трансформація відповідає наступним вимогам: вона охоплює виробництво, бізнес, науку, медицину, соціальну сферу та звичайне життя громадян; супроводжується тільки ефективним використанням її результатів; її результати доступні користувачам перетвореної інформації; її результатами користуються не тільки фахівці, але й пересічні громадяни, а користувачі цифрової інформації мають навички роботи з нею[2].

[1] Хаустова М. Г. Поняття цифровізації: національні та міжнародні підходи. *Право та інновації.* 2022. № 2 (38). С. 9. URL: https://doi.org/10.37772/2518-1718-2022-2(38)-1.

[2] Там само.

Урядом України приймаються широкомасштабні заходи з розвитку цифровізації суспільства, цифрового сектору економіки, впроваджуються електронні платежі та вдосконалюється нормативно-правова база у сфері електронної комерції. Задля реалізації цих та інших проєктів 18 вересня 2019 року Уряд затвердив Положення про Міністерство цифрової трансформації України. Прийняття акта створило правові передумови для функціонування нового органу, визначивши засади, цілі, завдання та принципи його діяльності. Так, відповідно до Положення Міністерство цифрової трансформації України (Мінцифри) є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України. Мінцифри є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики: у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій та технологій, робототехніки та роботизації, електронного урядування та електронної демократії, розвитку інформаційного суспільства, інформатизації; у сфері впровадження електронного документообігу; у сфері розвитку цифрових навичок та цифрових прав громадян; у сферах відкритих даних, публічних електронних реєстрів, розвитку національних електронних інформаційних ресурсів та інтероперабельності, електронних комунікацій та радіочастотного спектра, розвитку інфраструктури широкосмугового доступу до Інтернету, електронної комерції та бізнесу; у сфері надання електронних та адміністративних послуг; у сферах електронних довірчих послуг та електронної ідентифікації; у сфері розвитку ІТ-індустрії; у сфері розвитку та функціонування правового режиму Дія Сіті[1].

Отже, технологічні зміни відбуваються швидко, що вимагає якісного та своєчасного реагування, у тому числі і в питаннях адаптації законодавчої та регуляторної сфер[2]. Як зазначено у резюме до пункту

[1] Положення про Міністерство цифрової трансформації України: затв. постановою КабінетуМіністрів України від 18.09.2019 р. № 856. URL: https://zakon.rada.gov.ua/laws/show/856-2019-п#Text.

[2] Хаустова М. Г. Поняття цифровізації: національні та міжнародні підходи. *Право та інновації.* 2022. № 2 (38). С. 9. URL: https://doi.org/10.37772/2518-1718-2022-2(38)-1.

6.2 «Україна 2030Е – країна з розвинутою цифровою економікою» Економічної стратегії України 2030 цифровізація – це один із головних факторів зростання світової економіки в найближчі 5–10 років. Крім прямого підвищення продуктивності, яке отримують компанії від цифрових технологій, є ланцюг непрямих переваг цифровізації, як-то економія часу, створення нового попиту на нові товари й послуги, нова якість та цінність тощо[1].

Цифрова економіка – це вся економічна діяльність, яка забезпечується застосуванням інформаційно-комунікаційних та інших цифрових технологій. Це передусім електронна комерція, результати діяльності цифровізованих підприємств та різноманітні цифрові послуги. В найближче десятиліття близько 70 % створеної вартості буде спиратися на цифрові продукти. Якщо в 2018 році сума світового ВВП, яка припадала на цифровізовані підприємства, становила 13,5 трлн дол. США, то уже в 2023 році цей показник має сягнути рівня 53,3 трлн дол. США (тобто майже вчетверо вище), що становитиме більше половини номінального світового ВВП[2]. Безумовно, цифровізація стає головним інструментом для досягнення стратегічної цілі України – збільшення ВВП у 8 разів, до 1 трлн дол. США у 2030 році, та забезпечення добробуту, комфорту та якості життя українців на рівні, вищому за середній показник у Європі[3].

Як підкреслюється у світовій та вітчизняній науці, цифрова економіка може стати фактором стійкості економіки та надійним джерелом податкових надходжень, оскільки вона менше залежна від фізичних активів, ніж сільське господарство або промисловість. Стійкість цифрового сектору найбільш помітна в кризових умовах. Після початку повномасштабного вторгнення українська ІТ-галузь стала однією з найстабільніших сфер економіки; це єдина галузь, обсяг експорту

[1] Економічна стратегія України 2030. Український інститут майбутнього. URL: https://strategy.uifuture.org.

[2] Круп'яник А. Цифрова економіка України: основні фактори розвитку. Вокс Україна. 22 серпня 2023. URL: https://voxukraine.org/tsyfrova-ekonomika-ukrayiny-osnovni-faktory-rozvytku.

[3] Економічна стратегія України 2030. Український інститут майбутнього. URL: https://strategy.uifuture.org.

якої виріс у 2022 році. Саме інформаційні технології в змозі підвищити ефективність майбутнього процесу відбудови України після закінчення воєнних дій. Йдеться не лише про розвиток ІТ-сектору та застосування цифрових технологій в інших галузях для підвищення ефективності виробництва, але й про цифрові рішення для справедливого розподілу міжнародної фінансової допомоги та контролю за її використанням, що дозволить знизити корупційні дії в цій галузі[1].

Головними факторами, що сприяють розвитку цифрової економіки, є – розвинена галузь інформаційно-комунікаційних технологій (далі – ІКТ), а також сильні освітні інституції та конкурентоспроможні інновації. Інформаційні технології – це основа цифрової трансформації підприємств. Розвиток таких технологій як штучний інтелект, великі дані, інтернет речей дедалі більше впливає на бізнес-процеси. У свою чергу наукові розробки та дослідження – основа створення інформаційних технологій та інших цифрових продуктів, які згодом використовують підприємства. Так, за результатами 2022 року галузь інформаційно-комунікаційних технологій забезпечила надходження до економіки України у розмірі 7,35 млрд дол. США або 4,5 % ВВП[2].

На відміну від галузі ІКТ, в українському секторі науки та інновацій ситуація менш оптимістична. Сьогодні Україна у «хвості» інноваційних рейтингів[3]. Наприклад, у Глобальному інноваційному індексі (2022) Україна посідає 57 місце серед 132 економік, утримуючи 4-ту позицію серед 36 країн із групою доходів нижче середнього (lower-middle- income) та 34-ту – серед 39 економік Європи[4], а у Рейтингу глобальної цифрової конкурентоспроможності (2021) – 54 місце з 64 країн[5]. Причини цього – незначне фінансування наукових

[1] Круп'яник А. Цифрова економіка України: основні фактори розвитку. Вокс Україна. 22 серпня 2023. URL: https://voxukraine.org/tsyfrova-ekonomika-ukrayiny-osnovni-faktory-rozvytku.

[2] Там само.

[3] Там само.

[4] Global Innovation Index 2022. URL: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_2000_2022/ua.pdf.

[5] IMD World. Digital Competitiveness Ranking 2021. URL: https://imd.cld.bz/Digital-Ranking-Report- 2021/168/.

досліджень, неефективна організація наукової сфери, а також проблеми із захистом інтелектуальної власності[1]. За даними Рейтингу електронної участі ООН за 2022 рік Україна вперше перейшла з групи високого EGDI до дуже високого[2]. Натомість низькою стала патентна активність в Україні. Так, за даними ВОІВ (Всесвітньої організації інтелектуальної власності), у 2022 році в Україні було зареєстровано лише 1080 патентних заявок, тоді як у 2021 їх було – 1706, а у 2020 – 1710[3]. При цьому середнє значення в країнах Європи становить 12680, а Східної Європи – 4010[4].

Також варто враховувати, що для подальшого розвитку та впровадження в усі сфери життя цифровізації існує необхідність у подальшому активному фінансуванні впровадження стартапів. Так, у більшості розвинених країн існує інфраструктура доведення інноваційної ідеї до ринкового продукту, яка включає венчурні фонди, державні та недержавні гранти, краудфандинг тощо. В Україні така інфраструктура розвинена дуже слабко – наприклад, краудфандингу навіть немає в законодавстві[5].

Крім того, завдання зі швидкої цифрової трансформації неможливо вирішити без тісної міжнародної співпраці[6]. Зокрема, передовий досвід цифровізації та розвитку цифрових інформаційних технологій в рамках Європейського Союзу та інших країн світу визначає їх як стратегічних партнерів у галузі цифрових технологій та інформати-

[1] Круп'яник А. Цифрова економіка України: основні фактори розвитку. Вокс Україна. 22 серпня 2023. URL: https://voxukraine.org/tsyfrova-ekonomika-ukrayiny-osnovni-faktory-rozvytku.

[2] E-Government Survey 2022. The Future of Digital Government. United Nations. Department of Economic and Social Affairs. URL: https://desapublications.un.org/sites/default/files/publications/2022- 09/Web%20version%20E-Government%202022.pdf.

[3] Intellectual property statistical country profile. 2022. Ukraine. URL: https://www.wipo.int/edocs/statistics-country-profile/en/ua.pdf.

[4] Круп'яник А. Цифрова економіка України: основні фактори розвитку. Вокс Україна. 22 серпня 2023. URL: https://voxukraine.org/tsyfrova-ekonomika-ukrayiny-osnovni-faktory-rozvytku.

[5] Там само.

[6] Павлов К. В., Асадуллина Н. Р. Формы, методы и направления цифровизации экономики. *Економічний вісник Донбасу*. 2020. № 3 (61). С. 232. URL: http://dspace.nbuv.gov.ua/handle/123456789/173862.

зації. Європейський Союз та інші розвинені країни декларують підтримку розвитку цифрового простору та роблять практичні кроки в цьому напрямі[1].

Задля перевірки та аналізу якості використання інструментів цифровізаціїї суспільства та їх позитивного впливу на всі сфери діяльності у країнах Європейського Союзу використовується оціночний показник рівня технологічного розвитку та ступеня запровадження інноваційних технологій у цифровому суспільстві – Індекс DESI. Цей індекс охоплює п'ять основних субіндексів: зв'язок, людський капітал, використання Інтернету, інтеграція цифрових технологій і цифрові державні послуги[2]. Вимір людського капіталу складається з п'яти показників, об'єднаних у два підвиміри, що вивчають навички, необхідні для використання можливостей цифрового суспільства. Для визначення індексу DESI важливою складовою є наявність цифрових навичок у населення та у випускників навчальних закладів. Відповідно до значення індексу DESI, у 2020 р. лідерами з розвитку цифрових технологій серед країн Європейського Союзу стали Бельгія, Нідерланди, Люксембург, Данія, Фінляндія, Швеція, Великобританія, Ірландія, Естонія, Австрія[3].

Так, за даними Звіту DESI (2020) у домогосподарствах Європейського Союзу збільшилося покриття цифровими мережами нового покоління (зростання відбулося на рівні з 83 % до 86 %). Також за останні 2 роки простежується зростання доступу домашніх господарств до фіксованих широкосмугових мереж: з 15 % до 26 %. Покриття 4G охоплює майже все населення ЄС (96 %), але рівень покриття 5G все ще порівняно низький (25 %). Найбільш розвинені країни Євросоюзу з точки зору цифрової готовності мають більші

[1] Хаустова М. Г. Поняття цифровізації: національні та міжнародні підходи. *Право та інновації.* 2022. № 2 (38). С. 9. URL: https://doi.org/10.37772/2518-1718-2022-2(38)-1.

[2] Індекс цифрової економіки та суспільства (DESI) 2020. URL: https://eufordigital.eu/uk/library/digital-economy-and-society-index-desi-2020/.

[3] International Digital Economy and Society Index 2020. Final Report. URL: https://op.europa.eu/en/publication-detail/-/publication/fb3f7212-433c-11eb-b27b- 01aa75ed71a1/language-en.

інформаційно-комунікаційні можливості, зокрема: Фінляндія, Німеччина, Угорщина та Італія. Найвищий рівень доступності зв'язку у межах цифрового доступу в країнах ЄС належить Данії, Швеції, Люксембургу (68-65-бальна позиція за індексом DESI). Середній рівень серед країн ЄС становить 50 балів рейтингової позиції. Найнижчий показник у Болгарії, Кіпру, Греції[1].

Найвищий рівень цифрового розвитку людського капіталу уФінляндії, Швеції, Естонії; найнижчий серед країн ЄС – у Болгарії, Румунії та Італії. В країнах Євросоюзу відбувається активна інтеграція цифрових технологій на підприємствах залежно від розміру компанії, сектора і держави-члена. У 2019 р. 38,5 % великих компаній покладалися на передові сервіси хмарних обчислень, а 32,7 % використовували рішення для великих даних. Переважна більшість малих і середніх підприємств заявили, що вони не використовували ці рішення, при цьому 17 % малих і середніх підприємств використовують хмарні сервіси, а 12 % використовують великі дані. Згідно зі звітом DESI 2020 тільки 17,5 % малих і середніх підприємств продавали свою продукцію через Інтернет (це на 1,4 % більше, ніж у 2016 р.). Ірландія, Фінляндія та Бельгія лідирують за показником інтеграції цифрових технологій[2].

У зв'язку з цим варто зазначити, що 05 вересня 2023 р. розпорядженням Кабінету Міністрів України № 774-р було затверджено Перелік показників Індексу цифрової економіки та суспільства (DESI)[3]. Крім того, досліджуючи порядок використання інструментів щодо перевірки показників цифровізації в рамках Європейського Союзу, у березні 2021 року Кабінет Міністрів України схвалив Концепцію розвитку цифрових компетентностей та затвердження плану заходів з її реалізації, одним із яких є розроблення та затвердження опису

[1] Самойленко А. Особливості цифровізації країн Європейського Союзу в умовах глобалізації. *Вісник економіки.* 2021. № 1. С. 51. URL: http://visnykj.wunu.edu.ua/index.php/visnykj/article/view/1214.

[2] Там само. С. 52.

[3] Перелік показників Індексу цифрової економіки та суспільства (DESI) : затв. розпорядженням Кабінету Міністрів України від 05.09.2023 р. № 774-р. URL: https://zakon.rada.gov.ua/laws/show/774-2023-p#Text.

цифрової компетентності (рамки цифрової компетентності) та відповідних рамок цифрових компетентностей для основних професійних груп за сферами економічної діяльності[1]. При цьому слід наголосити, що за основу Рамки цифрових компетентностей для громадян України (DigCompUA for Citizens 2.1) взято європейську концептуально-еталонну модель цифрових компетентностей для громадян DigComp 2.1: The Digital Competence Framework for Citizens та рекомендації у сфері цифрових компетентностей від європейських та міжнародних інституцій[2]. При цьому більшу частину змісту документа, цілком логічно, складають напрацювання європейських учених[3].

Підхід ЄС до цифрової трансформації означає розширення можливостей та залучення до неї кожного громадянина, посилення потенціалу кожного бізнесу та вирішення глобальних викликів, і передбачений рамковими та стратегічними документами, такими як: Стратегія Єдиного цифрового ринку (Digital Single Market Strategy for Europe), Підключення до Європейського Гігабітного суспільства (Connectivity for a European Gigabit Society), нещодавно розробленої стратегії Цифрова Європа 2025 (Digital Europe 2025) та Програми розвитку загальноєвропейських стандартів у сфері телекомунікацій та цифрових технологій тощо. Стратегія Єдиного цифрового ринку ЄС була запропонована Європейською Комісією у 2015 році з метою досягнення синергії між країнами ЄС у царині новітніх технологій, транскордонної торгівлі та надання послуг в межах Єдиного цифрового ринку (далі – ЄЦР)[4]. Стратегія спрямована на те, щоб економіка,

---

[1] Концепція розвитку цифрових компетентностей: схв. розпорядженням Кабінету Міністрів України від 03.03.2021 р. № 167-р. URL: https://zakon.rada.gov.ua/laws/show/167-2021-р#Text.

[2] Опис рамки цифрової компетентності для громадян України. DigCompUA for Citizens 2.1. Міністерство цифрової трансформації України. 2021. URL: https://thedigital.gov.ua/storage/uploads/files/news_post/2021/3/mintsifra-oprilyudnyue-ramku-tsifrovoi-kompetentnosti-dlya-gromadyan/OP%20ЦК.pdf.

[3] Хаустова М. Г. Поняття цифровізації: національні та міжнародні підходи. *Право та інновації.* 2022. № 2 (38). С. 10. URL: https://doi.org/10.37772/2518-1718-2022-2(38)-1.

[4] На шляху до Єдиного цифрового ринку ЄС: електронна комерція, телекомунікації, довірчі послуги. Український Центр Європейської Політики. 14 червня 2021.

промисловість та суспільство Європи в повній мірі скористалися перевагами нової цифрової ери. ЄС активно створює вільний та безпечний ЄЦР, де люди можуть безпечно спілкуватись, здійснювати покупки в інтернеті без кордонів, а підприємства можуть продавати свої товари/послуги через інструменти електронної комерції по всьому ЄС. Тобто, ЄЦР пропонує розширені можливості для: користувачів, малого та середнього бізнесу, інноваційних стартапів, креативного сектору, наукового та безпекозміцнюючого співробітництва у додаток до модернізації вже існуючих індустрій. Головна мета Єдиного цифрового ринку ЄС – усунення зайвих регуляторних бар'єрів і перехід від окремих національних ринків до єдиного, із загальноєвропейськими уніфікованими правилами у трьох секторах – телекомунікації, довірчі послуги та електронна комерція[1].

Таким чином, розгортання широких цифрових можливостей країн ЄС вимагає від урядів провадження стратегії розвитку цифрової економіки в контексті «цифровізації» країни, формування внутрішнього ринку ІТ та розвитку мотивації у споживачів цифрових технологій. Необхідно забезпечити розвинену цифрову інфраструктуру як основу розвитку цифрової економіки, яка охопить комплекс технологій, продуктів та процесів, що зможуть забезпечити обчислювальні, телекомунікаційні та мережеві можливості на цифровій основі. Виявлені потенційні можливості цифрової економіки в країнах ЄС дають змогу дійти висновку, що більшість країн Євросоюзу мають провадити активну й ефективну державну політику щодо подолання «цифрового розриву». Важливу роль відіграє цифровізація багатьох сфер діяльності, активне впровадження мережі Інтернет у домогосподарствах, формування необхідних професійних цифрових навичок. Будь-які цифрові перетворення є складним завданням для

URL: https://ucep.org.ua/doslidzhennya/na-shlyahu-do-yedynogo-czyfrovogo-rynku-yes-elektronna- komercziya-telekomunikacziyi-dovirchi-poslugy.html.

[1] На шляху до Єдиного цифрового ринку ЄС: електронна комерція, телекомунікації, довірчі послуги. Український Центр Європейської Політики. 14 червня 2021. URL: https://ucep.org.ua/doslidzhennya/na-shlyahu-do-yedynogo-czyfrovogo-rynku-yes-elektronna- komercziya-telekomunikacziyi-dovirchi-poslugy.html.

урядів країн Євросоюзу. Водночас перед країнами, що досягли найвищого рівня цифрової зрілості, відкривається багато цифрових перспектив та можливостей подальшої активізації розвитку національної ІТ-сфери[1].

В межах Європейського Союзу, для подальшого ефективного впровадження цифровізації в усі сфери життя були затверджені такі документи, як «Індустрія 4.0.» (Industry 4.0.) «Розумне виробництво» (Smart manufacturing), «Інтернет у промисловості» (Internet of manufacturing), «Цифрове виробництво» (Digital manufacturing) та «Відкрите виробництво» (Open Manufacturing), прийнята в 2011 р. в Німеччині[2]. Враховуючи досвід ЄС та сучасні глобалізаційні процеси, в українській науці та у законодавстві визначається, що Індустрія 4.0 – це сукупність відносин, що складаються в процесі виробництва товарів (робіт, послуг) структурами усіх галузей економіки на основі цифрових технологій з метою підвищення конкурентоспроможності бізнесу і країни в цілому. Ключовими технологіями стають: Великі дані; Інтернет речей; віртуальна і доповнена реальність; хмарні обчислення; 3D-друк; друкована електроніка; блокчейн тощо. Практично у всіх галузях вітчизняної економіки як у державній, так і в приватній сферах впроваджуються передові інформаційні технології, в тому числі хмарні технології як пул використовуваних ресурсів, включаючи комп'ютерну апаратуру і програмне забезпечення[3].

З огляду на те, що застосування інноваційних технологій зменшує транзакційні витрати, підвищує продуктивність праці, скорочує час на здійснення онлайн комунікацій з партнерами, клієнтами тощо, їх впровадження на тих чи інших господарюючих суб'єктах стає на-

[1] Самойленко А. Особливості цифровізації країн Європейського Союзу в умовах глобалізації. *Вісник економіки.* 2021. № 1. С. 53. URL: http://visnykj.wunu.edu.ua/index.php/visnykj/article/view/1214.

[2] Хаустова М. Г. Поняття цифровізації: національні та міжнародні підходи. *Право та інновації.* 2022. № 2 (38). С. 11. URL: https://doi.org/10.37772/2518-1718-2022-2(38)-1.

[3] Концепція «Індустрія 4.0»: проблеми впровадження і окремі правові аспекти її реалізації в Україні : монографія / [Є. М. Білоусов, І. В. Борисов та ін.]; за ред. С. В. Глібка. Харків: НДІ прав. забезп. інновац. розвитку НАПрН України, 2021. С. 7. URL: https://ndipzir.org.ua/wp-content/uploads/2022/02/monografiya-industriya_2021.pdf.

гальною проблемою, яку без належного правового забезпечення господарської діяльності таких суб'єктів вирішити неможливо і законодавець прагне вирішити цю проблему, приймаючи відповідні Закони України[1]. Слід зазначити, що з 14.08.2021 р. набув чинності Закон України «Про стимулювання розвитку цифрової економіки в Україні», який визначає організаційні, правові та фінансові засади функціонування правового режиму Дія Сіті, що запроваджується з метою стимулювання розвитку цифрової економіки в Україні шляхом створення сприятливих умов для ведення інноваційного бізнесу, розбудови цифрової інфраструктури, залучення інвестицій, а також талановитих спеціалістів[2]. На сьогодні інформатизація та проведена на її основі інтелектуа- лізація промислових технологій, методів управління економікою повинні стати основною умовою прогресивного розвинення сучасної економіки. Крім природно-ресурсного потенціалу країни, його фінансів, основним капіталом стає інтелектуальний (в тому числі, науково-освітній, інформаційний та комунікаційний) потенціал[3].

Ефективний електронний уряд ЄС також позитивно впливає на більшість галузей економіки та може спростити і прискорити різні процедури. Саме тому динамічний розвиток цифрових технологій в Євросоюзі ставить перед державним сектором нові завдання. Згідно зі звітом DESI 2020 р. кількість осіб, які використовували послуги електронного уряду в 2019 р., збільшилася з 58 % до 67 %[4]. Естонія,

[1] Концепція «Індустрія 4.0»: проблеми впровадження і окремі правові аспекти її реалізації в Україні : монографія / [Є. М. Білоусов, І. В. Борисов та ін.]; за ред. С. В. Глібка. Харків: НДІ прав. забезп. інновац. розвитку НАПрН України, 2021. С. 7. URL: https://ndipzir.org.ua/wp-content/uploads/2022/02/monografiya- industriya_2021.pdf.

[2] Про стимулювання розвитку цифрової економіки в Україні : Закон України від 15.07.2021 р. № 1667-IX. URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text.

[3] Концепція «Індустрія 4.0»: проблеми впровадження і окремі правові аспекти її реалізації в Україні : монографія / [Є. М. Білоусов, І. В. Борисов та ін.]; за ред. С. В. Глібка. Харків: НДІ прав. забезп. інновац. розвитку НАПрН України, 2021. С. 15. URL: https://ndipzir.org.ua/wp-content/uploads/2022/02/monografiya-industriya_2021.pdf.

[4] Індекс цифрової економіки та суспільства (DESI) 2020. EU4Digital. Червень 2020. URL: https://eufordigital.eu/uk/library/digital-economy-and-society-index-desi-2020/.

Іспанія та Данія мають першість за цим показником[1]. У сфері послуг цифрові технології дозволяють здійснювати діяльність з будь-якого куточка світу, проводити відеоконференції, купувати продукти та різні побутові товари через мережу Інтернет. Цифровізація може сприяти вирішенню соціальних проблем, полегшивши доступ до основних послуг у сфері охорони здоров'я (електронна система охорони здоров'я) та освіти (дистанційне навчання), наданню фінансових послуг, прозорості та ефективності діяльності уряду (електронний уряд: система електронних регламентів та реєстрацій)[2].

Отже, подальше впровадження цифровізації та розвиток сектору цифрової економіки в Україні може забезпечити стабільність та зростання фінансових надходжень необхідних, зокрема, для післявоєнної відбудови. Цифрові рішення становлять не лише фінансовий, а й стратегічний інтерес, оскільки здатні посилювати ефективність тих галузей, в які вони інтегруються, зокрема в урядовий та військовий сектори. Підґрунтям цифрової економіки є інформаційні технології, освіта, наука та інновації, для яких є необхідним: створення законодавчої бази для врегулювання питань альтернативних джерел фінансування та спрощення процедур залучення недержавного фінансування для університетів та наукових установ; реформування вищої освіти, зокрема підвищення автономії університетів та актуалізація навчальних програм у відповідності до вимог ринку праці; підвищення базових цифрових навичок населення за допомогою субсидованих державою курсів (наприклад, такі курси можуть адмініструвати Державні центри зайнятості); впровадження місцевою владою проектів з цифровізації (цифрові громади), зокрема розвитку цифрової інфраструктури з урахуванням потреб кожної громади; продовження реформ у галузі захисту інтелекту-

[1] Самойленко А. Особливості цифровізації країн Європейського Союзу в умовах глобалізації. *Вісник економіки*. 2021. № 1. С. 52. URL: http://visnykj.wunu.edu.ua/index.php/visnykj/article/view/1214.

[2] Маркевич К. Цифровізація: переваги та шляхи подолання викликів. Український центр економічних та політичних досліджень ім. О. Разумкова. Статті та інтерв'ю. 06 вересня 2021 р. URL: https://razumkov.org.ua/statti/tsyfrovizatsiia-perevagy-ta-shliakhy-podolannia-vyklykiv.

альної власності, зокрема гармонізація українського законодавства із нормами ЄС[1].

## 1.2. Розвиток цифрової політики в умовах цифровізації суспільства. Міжнародний досвід реалізації програм та стратегій цифровізації

Поширення процесів цифровізації відбувається й в політичному вимірі, яке проявляється у застосуванні інформаційно-комунікаційних технології в політичному процесі, державному управлінні та політичній комунікації.

Цифровізація політики є наслідком глобалізації та полягає в тому, що вона кардинально змінює сучасні тренди політичних процесів, функціональне призначення політичних інститутів, суспільні інтеракції та сценарії майбутнього. Цифрові технології обумовлюють результати виборів, формують і модерують громадянську активність, впливають на зовнішній імідж держави, виступають каталізатором гібридності політичних режимів, роблять впізнаваними і легітимними публічних персон, політичні кампанії, доленосні рішення[2].

Виокремлюються різні підходи щодо визначення сутності цифрової політики. Так, Н. О. Стеблина цифрову політику визначила як процес упорядкування політичного дискурсу у межах цифрової інфраструктури, що під впливом цифрового поля безперервно модифікується (самовдосконалюється та самооновлюється) за рахунок мережевої природи політики й суспільства. Відповідно, внаслідок глобальної цифровізації, сьогодні політичні актори функціонують в умовах

[1] Круп'яник А. Цифрова економіка України: основні фактори розвитку. Вокс Україна. 22 серпня 2023. URL: https://voxukraine.org/tsyfrova-ekonomika-ukrayiny-osnovni-faktory-rozvytku.

[2] Стеблина Н. О. Цифровізація державної політики як дискурс сучасності: автореф. дис д-ра політ. наук. Вінниця, 2021. С. 1. URL: https://abstracts.donnu.edu.ua/issue/view/353.

перманентної зміни цифрової інфраструктури, де є можливою поява нових цифрових політичних суб'єктів, які внаслідок миттєвої інтеграції мережевих спільнот ставатимуть центрами ухвалення рішень[1].

Цифрова політика у вузькому значенні розуміється як інтенсифікація використання цифрових технологій у політичних процесах. Таке розуміння не дає змоги пояснити процеси, що викликані цифровізацією політики, оскільки базові цифрові можливості наявні у більшості держав світу. Цифровізація політики у широкому значенні – формування цифрової політичної інфраструктури під впливом дискурсу глобальної цифровізації, що детермінує способи взаємодії цифрових політичних суб'єктів із цією інфраструктурою та зумовлює специфіку утворення мереж для здійснення політики. Цифровізація у цьому широкому значенні призводить до формування політики нового типу – цифрової політики[2].

Цифрову політику визначають як процес упорядкування політичного дискурсу під впливом цифрового поля, що визначає способи використання цифрової інфраструктури. Цю політику здійснюють цифрові політичні суб'єкти, використовуючи потенціал фрагментованих мереж, інтегруючи їх (утворюючи спільноти із слабкими горизонтальними зв'язками) для впливу на процеси визначення та ухвалення політичних рішень. Особливості трансформації політики під впливом цифровізації необхідно визначати через цифрові політичні практики – процес перетворення/перекодування смислів на текст, що у свою чергу породжує нові тексти і нові смисли[3].

Отже, цифровізацію політики можливо виокремити як новий феномен політичного процесу в сучасному світі, що виникає під впливом глобальної цифровізації. Процес цифровізації політики є валентним, нестійким, незавершеним процесом, що можна пояснити самою природою глобальної цифровізації, що постійно самовдоско-

[1] Стеблина Н. О. Цифровізація державної політики як дискурс сучасності: автореф. дис д-ра політ. наук. Вінниця, 2021. С. 22. URL: https://abstracts.donnu.edu.ua/issue/view/353.

[2] Там само. С. 11.

[3] Там само. С. 11.

налюється та самооновлюється. Це позначається і на принципах формування цифрових політичних суб'єктів, які постійно удосконалюють свій інструментарій через утворення усе більш масштабних спільнот. Тож баланс сил у цифровому світі залежить від миттєвої інтеграції цих спільнот тими або іншими цифровими політичними суб'єктами. Цифровізація державної політики виступає як постійна модифікація цифрової інфраструктури політичного процесу[1].

Слід зазначити, що якщо цифровізація політики в теоретичному аспекті представляє собою новий напрямок дослідження, то в практичному плані вона не є раптовим явищем[2]. Так, ще Е. Тоффлер у роботі «Третя хвиля» зазначає, що прискорена зміна суспільства призводить до ускладнення системи уряду. В умовах третьої хвилі інформатизації «формується нова система розподілу влади, в якій нація як така втратить своє значення, проте більш важливу роль набудуть інші інститути – від транснаціональних корпорацій до місцевих органів влади»[3]. Фактично процес інформатизації в політиці можна спостерігати з формуванням ідей про електронну демократію. Основою електронної демократії є участь громадян у здійсненні влади таким чином, щоб широка громадськість могла ефективно впливати на прийняття політичних рішень[4]. Електронна демократія «включає розширення участі, оновлення комунікаційної взаємодії, оптимізацію управлінських механізмів, оперативність реагування, гнучкість регулювання тощо»[5].

---

[1] Стеблина Н. О. Цифровізація державної політики як дискурс сучасності: автореф. дис д-ра політ. наук. Вінниця, 2021. С. 1, 2, 31. URL: https://abstracts.donnu.edu.ua/issue/view/353.

[2] Милосердна І. М., Краснопольська Т. М. Процес цифровізації в політиці: межі пізнання та особливості трансформації. *Актуальні проблеми політики.* 2022. Вип. 70. URL: https://doi.org/10.32782/app.v70.2022.17.

[3] Toffler A. The Third Wave. New York : WILLIAM MORROW AND COMPANY, INC., 1980. URL: https://ia801200.us.archive.org/9/items/TheThirdWave-Toffler/The-Third-Wave_-_Toffler.pdf.

[4] Freeman J. Local E-Government and Citizen Participation: Case Studies from Australia and Italy. *E- Government Success Around the World: Cases, Empirical Studies, and Practical Recommendations.* Hershey, Pennsylvania: IGI Global. 2013. URL: https://www.irma-international.org/chapter/local-government-citizen- participation/76642/.

[5] Кормич Л. І., Кормич А. І. Вдосконалення публічного управління в Україні в контексті діджиталізації: теоретичний аспект. *Актуальні проблеми політики.* 2022. № 69. С. 5. URL: https://doi.org/10.32837/app.v0i69.1295.

20 вересня 2017 р. розпорядженням Кабінету Міністрів України було схвалено Концепцію розвитку електронного урядування в Україні, згідно із якою електронне урядування визначається, як форма організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян. Для досягнення мети Концепції передбачено забезпечення виконання комплексних заходів за такими напрямами: модернізація публічних послуг та розвиток взаємодії влади, громадян і бізнесу за допомогою інформаційно-комунікаційних технологій; модернізація державного управління за допомогою інформаційно-комунікаційних технологій; управління розвитком електронного урядування. Реалізація Концепції передбачена на період до 2020 року[1].

Згодом, 08 листопада 2017 р. Кабінет Міністрів України схвалив Концепцію розвитку електронної демократії в Україні[2] та План заходів щодо її реалізації[3]. Відповідно до Концепції електронна демократія визначена як форма суспільних відносин, за якої громадяни та організації залучаються до державотворення та державного управління, а також до місцевого самоврядування шляхом широкого застосування інформаційно- комунікаційних технологій у демократичних процесах. Для досягнення мети Концепції передбачено забезпечення виконання комплексних заходів за такими напрямами: нормативно-правове забезпечення розвитку електронної демократії; ресурсне забезпечення впровадження та використання інструментів електронної

[1] Концепція розвитку електронного урядування в Україні : схвал. розпорядженням Кабінету Міністрів України від 20.09.2017 р. № 649-р. URL: https://zakon.rada.gov.ua/laws/show/649-2017-р#Text.

[2] Концепція розвитку електронної демократії в Україні : схвал. розпорядженням Кабінету Міністрів України від 08.11.2017 р. № 797-р. URL: https://zakon.rada.gov.ua/laws/show/797-2017-р#Text.

[3] План заходів щодо реалізації Концепції розвитку електронної демократії в Україні : схвал. розпорядженням Кабінету Міністрів України від 08.11.2017 р. № 797 р. URL: https://zakon.rada.gov.ua/laws/show/797-2017-р#Text.

демократії суб'єктами владних повноважень; підвищення готовності органів державної влади та органів місцевого самоврядування до використання можливостей електронної демократії; забезпечення доступності інструментів електронної демократії. Забезпечення координації та здійснення контролю за реалізацією Концепції, виконання плану заходів, моніторингу стану їх виконання покладено на Мінцифри. Реалізація Концепції передбачена на період до 2020 року[1].

Ще одним проявом трансформації політики під впливом процесу цифровізації можна вважати створення електронного уряду (e-government)[2], який представляє собою «більше, ніж просто впровадження ІКТ систем, які б трансформували уряд до надання послуг в режимі онлайн, а це повна реорганізація державного сектору за допомогою використання ІКТ[3]. У свою чергу, У. Лофстедт зазначає, що електронний уряд концептуалізується через різні поняття: управління та організація, електронна демократія (e- democracy), взаємодія, електронна безпека (e-security), електронні послуги (e-services)[4]. Сьогодні громадяни не тільки надають перевагу цифровим послугам і взаємодії з органами влади, але мають можливість через цифрові послуги більше залучатися у роботу уряду[5].

Але як зазначають Б. Коридон, В. Ганесан та М. Лундквіст переведення уряду на цифрові технології потребує уваги до двох основних

[1] Концепція розвитку електронної демократії в Україні : схвал. розпорядженням Кабінету Міністрів України від 08.11.2017 р. № 797-р. URL: https://zakon.rada.gov.ua/laws/show/797-2017-p#Text.

[2] Милосердна І. М., Краснопольська Т. М. Процес цифровізації в політиці: межі пізнання та особливості трансформації. *Актуальні проблеми політики*. 2022. Вип. 70. С. 107. URL: https://doi.org/10.32782/app.v70.2022.17.

[3] Hunnius S., Schuppan T. Competency Requirements for Transformational E-Government. *46th Hawaii International Conference on System Sciences.* 2013. Pp. 1664–1673. URL: https://www.researchgate.net/publication/235345539_Competency_Requirements_for_Transformational_E-Government.

[4] Löfstedt U. E-Government-Assessment of Current Research and Some Proposals for Future Directions. *International Journal of Public Information Systems.* 2005. No. 1. Vol. 1. Pp. 39–52. URL: http://www.ijpis.net/ojs/index.php/IJPIS/article/view/22.

[5] Милосердна І. М., Краснопольська Т. М. Процес цифровізації в політиці: межі пізнання та особливості трансформації. *Актуальні проблеми політики*. 2022. Вип. 70. С. 108. URL: https://doi.org/10.32782/app.v70.2022.17.

аспектів. Перше – це основні можливості які уряди використовують для взаємодії з громадянами та бізнесу та виконання своєї роботи: методи та інструменти, які вони використовують для надання послуг, процеси, які вони впроваджують, їхній підхід до прийняття рішень, а також обмін і публікація корисних даних. По-друге, організаційні чинники, які підтримують уряди в забезпеченні цих можливостей: стратегія, управління та організація, лідерство, таланти і культура, технології (експонат)[1].

Можна також погодитися з М. Бакус, що в умовах поширення процесу цифровізації в політиці застосування e-government є вузьким, а більше можливостей надається у функціонуванні електронного урядування (e- governance), яке є ширшим за обсягом і охоплює регулювання, прозорість операцій та контроль як з боку громадян, так і з боку урядів. Крім цього, електронне урядування спрямоване на постійне вдосконалення послуг, участь зацікавлених сторін у формуванні політики та прийнятті рішень з використанням ІКТ та пов'язаних з ними каналів для кращого управління[2].

Варто зазначити, що електронне урядування складається з трьох компонентів, які є дуже важливими для громадян: електронне адміністрування, яке спрямоване на покращення урядових процесів; електронні громадяни та електронні послуги; електронне суспільство, яке покликано для налагодження взаємодії з громадянським суспільством та всередині нього. Фактором, який сприяв поширенню ідей щодо впровадження як електронного уряду, так й електронного урядування був розвиток Web 2.0, який забезпечує двосторонню комунікацію, а також створює широкі перспективи. Так громадяни отримують можливість прийняття участі в онлайнових урядових

[1] Corydon B., Ganesan V., Lundqvist M. Digital by default: A guide to transforming government. McKinsey & Company. McKinsey Center for Government. November 2016. URL: https://www.mckinsey.com/~/media/mckinsey/industries/public%20and%20social%20sector/our%20insig hts/transforming%20government%20through%20digitization/digital-by-default-a-guide-to-transforming- government-final.pdf.

[2] Backus M. E-Governance and Developing Countries: Introduction and examples. Research report. April 2001. No. 3. URL: https://bibalex.org/baifa/Attachment/Documents/119334.pdf.

пропозиціях через Really Simple Syndication (RSS) подкасти, блоги, чати та інші додатки, які покращують послуги електронного уряду[1].

В умовах трансформації політики під впливом ІКТ разом з формуванням електронної демократії, електронного уряду та електронного урядування відбувається формування цифрової бюрократії, яка передбачає створення та впровадження нових алгоритмів взаємодії суб'єкта та об'єкта політико-управлінської діяльності. В таких умовах цифрова бюрократія певною мірою може сприяти зниженню впливу неефективних реформ в різних сферах життєдіяльності. Так, в Україні для посилення взаємодії та розвитку відносин держава-громадянин, в умовах діджиталізації та онлайн можливостей, відбувається формування онлайн-простору через законодавчу ініціативу «Держава в смартфоні» та «Держава і Я» (ДіЯ)[2].

Отже, у процесі цифровізації політики відбувається трансформація політичних інститутів, з'являються та стрімко розширюються нові можливості політичної участі громадян та їх взаємодії з владою[3]. Для ідеальної моделі цифрової політики важливою є циклічна структура цифрових можливостей, в якій ключовою ланкою є спроможність політичних акторів досягати успіху внаслідок використання цифрових технологій, що своєю чергою призводить до постійної модернізації наявного цифрового інструментарію, який використовується в політичній боротьбі[4]. Трансформація політики в умовах цифровізації представляє собою інтеграцію цифрових технологій, які змінюють методи роботи та надання нових можливостей громадянам та зацікавленим групам: швидкі темпи інформованості щодо діяльності органів влади, участь у відкритих обговореннях актуальних питань, електронні консультації та електронна участь, які підтриму-

[1] Милосердна І. М., Краснопольська Т. М. Процес цифровізації в політиці: межі пізнання та особливості трансформації. *Актуальні проблеми політики*. 2022. Вип. 70. С. 108. URL: https://doi.org/10.32782/app.v70.2022.17.

[2] Там само. С. 108.

[3] Там само. С. 110.

[4] Стеблина Н. О. Складові цифровізації політики: цифровий форум, цифровий капітал та структура цифрових можливостей. *Політикус: наук. журнал*. 2020. Вип. 5. С. 126, 130. URL: http://dspace.pdpu.edu.ua/handle/123456789/10373.

ються державою через створення співробітництва в межах інформаційного простору[1].

## 1.3. Ефекти цифрової трансформації для відновлення України

Головною метою цифровізації виступає досягнення цифрової трансформації існуючих та створенні нових галузей економіки, трансформації усіх сфер життєдіяльності у нові більш сучасні, модернізовані та ефективні. Такий приріст є можливим лише тоді, коли все, що стосується цифровізації, буде інтегровано, зокрема, в національні, регіональні, галузеві стратегії і програми розвитку. В сучасному світі одним із пріоритетних стратегічних завдань та загальнонаціональних пріоритетів розглядається впровадження інформаційно-комунікаційних технологій (ІКТ) та розвиток елементів цифрового суспільства. Цифрові технології, а також пов'язана з ними громадська та людська діяльність утворюють цифрову сферу сучасного соціуму, яка в нинішніх умовах визначає економічний та інноваційний потенціал держави, рівень освіти та людського розвитку, обумовлює соціальний прогрес, ефективність державного управління та здійснення демократичних процедур[2].

Сучасні цифрові технології, проникаючи у різні сфери діяльності, здійснюють значний вплив на життєдіяльність суспільства, створюючи можливості для політичного та соціально-економічного розвитку будь-якої країни світу. Вони здатні сприяти «подоланню соціальної

[1] Милосердна І. М., Краснопольська Т. М. Процес цифровізації в політиці: межі пізнання та особливості трансформації. *Актуальні проблеми політики.* 2022. Вип. 70. С. 110. URL: https://doi.org/10.32782/app.v70.2022.17.

[2] Хаустова М. Г. Державна політика в сфері цифрового розвитку: значення та перспективи. *Економічна безпека: міжнародний і національний рівень*: за матеріалами І-ї науково-практичної конференції (м. Харків, 27 травня 2022 року). Харків: НДІ ПЗІР НАПрН України, 2022. С. 179. URL: https://ndipzir.org.ua/wp-content/uploads/2022/11/conf_27.05.2022.pdf.

ізоляції, підвищенню продуктивності праці, впровадженню інновацій», «докорінно перетворити наше життя, забезпечуючи процвітання націй», а завдяки використанню економії від масштабу та мережевих ефектів формують додаткові резерви для економічного росту країн, які розвиваються. Однак слід констатувати, що трансформаційні процеси одночасно пов'язані зі значною кількістю викликів і проблем, які потребують своєчасного вирішення у рамках відповідної державної політики, особливо в нинішній час військової агресіїї росії проти України. Серед основних із них варто відзначити такі: рівень розвитку інфраструктури та доступ до необхідних даних; забезпечення кібербезпеки; формування необхідної нормативно- правової бази; стимулювання інвестиційних процесів тощо[1].

Провідна роль держави у процесах цифровізації та необхідність формування державної політики, яка повинна мати системний характер, доведена досвідом розвинутих країн світу, котрі пройшли значний шлях у цьому напрямі та мають напрацювання стосовно запровадження інструментів державного регулювання[2]. До початку повномасштабних воєнних дій у нашій країні вже було реалізовано значну кількість цифрових ініціатив, серед яких: створення додатка Дія та програми єПідтримка, проєктів Дія. Цифрова освіта, Дія. Бізнес,Дія. Центр, Е-резиденство, розробка цифрових документів, легалізація віртуальних активів, реформування ІТ-освіти в Україні, створення спеціального податкового та правового режиму для ІТ-компанії Дія.City[3].

---

[1] Островий О. В. Формування державної політики цифрового розвитку: сучасні тенденції та перспективи. *Таврійський науковий вісник.* 2021. № 3. С. 86. URL: https://journals.ksauniv.ks.ua/index.php/public/article/view/122/110.

[2] Хаустова М. Г. Державна політика в сфері цифрового розвитку: значення та перспективи. *Економічна безпека: міжнародний і національний рівень*: за матеріалами І-ї науково-практичної конференції (м. Харків, 27 травня 2022 року). Харків: НДІ ПЗІР НАПрН України, 2022. С. 178. URL: https://ndipzir.org.ua/wp-content/uploads/2022/11/conf_27.05.2022.pdf.

[3] Іванова Н. Цифровий розвиток регіонів України: тренди довоєнного періоду та перспективи післявоєнного відновлення. *Проблеми та перспективи економіки та управління*. 2022. № 4 (32). С. 209. URL: http://ppeu.stu.cn.ua/article/view/277072/271847.

Сьогодні здійснюється активне формування вітчизняної системи державного управління цифровим розвитком, особливо при розробці напрямів відновлення України, що актуалізує питання дослідження її сучасного стану та визначення перспективних напрямів із урахуванням актуальних викликів і загроз[1]. Ті, хто підтримують Україну в її боротьбі проти неспровокованого російського вторгнення, вважають, що повоєнна Україна має стати зразковою демократією, економіка якої наздожене успішніші в економічному плані країни з перехідною економікою. Після війни Україна матиме шанс модернізувати свою інфраструктуру, економіку, системи освіти та охорони здоров'я подібно до того, як це було в Західній Європі після Другої світової війни. Але також вона матиме унікальну історичну можливість перезавантажити свої політичну та судову системи і стати повноправною частиною Європи двадцять першого століття. Кандидатство України в ЄС виборювалося важко і завойовано кров'ю тисяч невинних українців. ЄС має прагнути розширення, щоб прийняти Україну як повноправну державу-члена після повоєнного процесу інтеграції[2].

Коли настане час повоєнної відбудови України, важливо пам'ятати про декілька принципів. По-перше, Україна має стати повноцінною ліберальною демократією з усіма інституційними запобіжниками демократії. Цю орієнтацію потрібно захищати всередині Україні, а також це мають робити прихильники України серед розвинених демократій. По-друге, щоб зберегти цю орієнтацію та враховуючи те, що Україна стала центром тяжіння нової холодної війни між демократією та автократією, а отже, форпостом демократичного світу, Україна має стати повноправним членом ЄС після зрозумілого процесу приєднання[3].

[1] Островий О. В. Формування державної політики цифрового розвитку: сучасні тенденції та перспективи. *Таврійський науковий вісник.* 2021. № 3. С. 86. URL: https://journals.ksauniv.ks.ua/index.php/public/article/view/122/110.

[2] Милованов Т., Ролан Ж. Повоєнна відбудова та реформи державного управління України. Відбудова України: принципи та політика: монографія. CEPR PRESS. Паризький звіт 1. С. 44, 45, 46. URL: https://cepr.org/system/files/2022-12/reconstruction%20book_Ukrainian_0.pdf.

[3] Там само. С. 47, 48.

Сучасний геополітичний контекст із вторгненням росії в Україну робить впровадження інноваційних цифрових рішень, технологій та розвиток цифрових інфраструктур, заснованих на цінностях і принципах ЄС, а також зміцнення кібербезпеки ще більш актуальним. Отже, наближення України до Єдиного цифрового ринку ЄС є складовою частиною цифрового безвізу з ЄС.

ЄС проводить комплексну політику у сфері цифрової економіки та цифрової трансформації, створюючи цілу екосистему. Тому для України важливо формувати координовані з ЄС політики, беручи до уваги стратегічні документи ЄС в комплексі[1]. Так, у вересні 2022 року Україна долучилася до Програми «Цифрова Європа» до 2027 року. Пришвидшенню цифрової трансформації та відновленню економіки України сприятиме подання заявки на фінансування проєктів цифрових глобальних шлюзів Програми ЄС *Connecting Europe Facility* на суму близько 6 млрд євро за наступними напрямами: високопродуктивний комп'ютинг – 2,2 млрд євро (проєкти щодо обчислення великих масивів даних для рішень у сфері економіки, оборонної промисловості та охорони здоров'я); штучний інтелект, дані та хмарні послуги – 2,1 млрд євро (проєкти, які створюють продукти на базі штучного інтелекту для полегшення роботи підприємств, держадміністрацій, дослідницьких установ); використання цифрових технологій в економіці та суспільстві – 1,1 млрд євро (проєкти, які впроваджують цифровізацію у бізнесі, сфері електронного урядування, охорони здоров'я, навколишнього середовища, освіти та культури, технологій Smart City); цифрові навички – 580 млн євро (проєкти для набуття нових навичок у сфері ІТ); кібербезпека (напрям закритий для держав не членів ЄС)[2].

[1] На шляху до Єдиного цифрового ринку ЄС: електронна комерція, телекомунікації, довірчі послуги. Український Центр Європейської Політики. 14 червня 2021. URL: https://ucep.org.ua/doslidzhennya/na-shlyahu-do-yedynogo-czyfrovogo-rynku-yes-elektronna-komercziya-telekomunikacziyi-dovirchi-poslugy.html.

[2] Україна долучилася до Програми «Цифрова Європа»: що це означає. Міністерство цифрової трансформації України. Новини. 05 вересня 2022. URL: https://thedigital.gov.ua/news/ukraina-doluchilasya-do-programi-tsifrova-evropa-shcho-tse-oznachae.

В напрямі подальшої цифровізаціїї та відновлення країни необхідними є розробка та впровадження незалежних інструментів моніторингу реалізації програм цифрової трансформації та конкурентоспроможності економіки. Наприклад Індекс Цифрової Економіки та Суспільства (DESI), що дозволяє інвесторам та міжнародним партнерам відстежувати прогрес кожної держави-члена ЄС у розбудові цифрової економіки та суспільства[1]. Індекс цифрової економіки та суспільства (DESI) – це зведений індекс, який узагальнює відповідні показники з ефективності цифрових технологій в Європі і відстежує еволюцію держав-членів ЄС в області цифрової конкурентоспроможності[2]. Індекс DESI охоплює п'ять основних областей: зв'язок, людський капітал, використання Інтернету, інтеграція цифрових технологій і цифрові державні послуги[3]. DESI вимірює показники цифрової економіки 27 держав- членів ЄС та ЄС загалом у порівнянні з 19 іншими країнами світу (Австралія,  Албанія, Боснія та Герцеговина, Бразилія, Канада, Чилі, Ісландія, Ізраїль, Японія, Мексика, Чорногорія, Північна Македонія, Норвегія, Сербія, Південна Корея, Швейцарія, Туреччина, Великобританія та Сполучені Штати). I-DESI має на меті відобразити та розширити результати Індексу цифрової економіки та суспільства (DESI) Європейської комісії шляхом пошуку показників, які вимірюють подібні змінні для країн, що не входять до ЄС[4].

Отже, необхідно замислитися щодо побудови екосистеми DESI в Україні. Цифровізація державних сервісів, бізнесу та доступ до

[1] Огляд заходів щодо цифрової трансформації та відновлення економічного розвитку України в умовах війни. Цифрова трансформація та відновлення економічного розвитку України в умовах війни. (12 жовтня 2022). Національний інститут стратегічних досліджень. URL: https://niss.gov.ua/news/komentari-ekspertiv/ohlyad-zakhodiv-shchodo-tsyfrovoyi-transformatsiyi-ta-vidnovlennya.

[2] Індекс цифрової економіки та суспільства (DESI) 2020. EU4Digital. Червень 2020. URL: https://eufordigital.eu/uk/library/digital-economy-and-society-index-desi-2020/.

[3] Там само.

[4] Єфремова К. В. Індекс цифрової економіки та суспільства в Україні як необхідна передумова інтеграції до ЄС. *Актуальні питання розбудови науково-дослідницької інфраструктури у воєнний та повоєнний періоди*: Інтернет-конференція (м. Харків, 28 лютого 2023 року). Харків, 2023. С. 51. URL: https://ndipzir.org.ua/wp-content/uploads/2023/04/conf_28.02.23.pdf.

технологій відкривають безліч можливостей. Важливо зрозуміти прогрес держави у цій сфері та покращувати цифровий досвід громадян шляхом запровадження DESI в Україні. 16 листопада 2022 р. проєкт EU4DigitalUA разом із місією технічної допомоги та обміну інформацією (TAIEX) Європейської Комісії провів воркшоп щодо створення передумов впровадження DESI в Україні. Проєкт EU4DigitalUA підтримує впровадження DESI в Україні, а запрошені експерти аналізують нормативно-правову та політичну базу збору цифрових даних та допомагають створити передумови для застосування DESI в Україні[1].

Окремої уваги заслуговує аналіз світового досвіду країн у процесі відновлення їх у післявоєнний період або після катастроф, і тому можливо окреслити основні принципи їх успішного відновлення: 1. Відновленням повинні керувати органи країни, яка потребує відновлення. Ні міжнародні організації, ні громадські не повинні замінювати собою функції державних інституцій; 2. Відновлення країни повинно базуватися на економічному відновленні. Фінансова допомога має сприяти економічному зростанню, а не заміщувати його; 3. Відновлення повинно відбуватися швидко та починатися якомога раніше; 4. Використання цифрових інструментів та відповідної інфраструктури дозволяє боротися з корупцією та підвищувати ефективність використання ресурсів; 5. Залучення місцевої влади та громадянського суспільства мають велике значення для успішного та ефективного відновлення[2]. Необхідно будувати нові об'єкти кращої якості, використовуючи передові та екологічні технології, ніж зруйновані. Можливість впровадити ключо-

[1] Єфремова К. В. Індекс цифрової економіки та суспільства в Україні як необхідна передумова інтеграції до ЄС. *Актуальні питання розбудови науково-дослідницької інфраструктури у воєнний та повоєнний періоди*: Інтернет-конференція (м. Харків, 28 лютого 2023 року). Харків, 2023. С. 51, 52. URL: https://ndipzir.org.ua/wp-content/uploads/2023/04/conf_28.02.23.pdf.

[2] Шаповал Н., Федосеєнко М., Грибановський О., Терещенко О. Повоєнне відновлення України. Нові ринки та цифрові рішення: монографія. Kyiv School of Economics. 2022. С. 6. URL: https://kse.ua/wp-content/uploads/2022/09/Digital-instruments-in-Ukrainian-recovery.pdf.

ві принципи ЄС переходу до «Зеленої» економіки та Цифрової трансформації[1].

Отже, відбудовою мають займатися державні органи тієї країни, де вона відбувається, це допомагає створювати досконалі інституції всередині держави. Відновлення держави має базуватися на відбудові економіки, щоб створювати робочі місця та наповнювати бюджети коштами, закладаючи фундамент для подальшого зростання. Проєкти відновлення мають відбуватися швидко та починатися якомога раніше. Залучення місцевої влади та громадськості мають вирішальну роль в ефективності відбудови. Використання цифрових інструментів дозволяє боротися з корупцією та ефективніше використовувати ресурси[2].

Аналізуючи міжнародні процеси відновлення після воєн, що відбулися за останнє півстоліття (дослідження на прикладі понад 36 країн – в більшості це громадянські війни), враховуючи досвід Боснії, Афганістану, Камбоджі та Іраку, можливо сформувати основні тези/висновки світової практики: Існує два види міжнародних допомог (International Aid and UN Peacekeeping Missions), всі вони або невдалі або малопродуктивні – свідчать дослідження World Bank; Органи влади країни повинні самостійно керувати процесом реконструкції, встановлювати найбільш нагальні пріоритети та координувати відповідну політику; Громадянське суспільство і місцева влада має бути залученою (через дорадчі органи) до процесів відбудови[3].

Так, Міжнародна організація SocialBoost в партнерстві з Міністерством цифрової трансформації України та за підтримки Програми

[1] План відновлення України. Національна Рада з відновлення. Липень 2022. URL: http://kyiv- heritage.com/sites/default/files/План%20Відновлення%20України%202022-07- 04%2C%20з%20дод%20№%201-22%203077c.pdf.

[2] Федосеєнко М. Цифрові інструменти для відновлення України. Результати конференції. Київська школа економіки. 28 жовтня 2022 р. URL: https://www.rise.org.ua/blog-ua/cifrovi-instrumenti-dlya-vidnovlennya-ukrayini-yak-zabezpechiti-prozore-i-rozumne-upravlinnya-vidbudovoyu.

[3] Шаповал Н., Федосеєнко М., Грибановський О., Терещенко О. Повоєнне відновлення України. Нові ринки та цифрові рішення: монографія. Kyiv School of Economics. 2022. С. 9, 10. URL: https://kse.ua/wp-content/uploads/2022/09/Digital-instruments-in-Ukrainian-recovery.pdf.

«U-LEAD з Європою» запускає акселераційну програму «Громада 4.0» для громад, яка допоможе створити та реалізувати проєкти цифрової трансформації. Буде сприяти теперішнім і майбутнім лідерам цифрової трансформації сформувати концепції і запустити диджитал-проєкти, засновані на поточних потребах мешканців та органів влади громад. Програма «Громада 4.0» передбачає використання вже наявних технологій та розробку нових рішень задля посилення стійкості, оптимізації цифрових процесів і впровадження інновацій, які сприятимуть відновленню і відбудові країни[1].

Отже, важливо, щоб місцева влада відігравала провідну роль в реконструкції (досвід Боснії), не можна її підміняти (досвід Афганістану, Боснії, Камбоджі, Східного Тимору та Іраку); грошова допомога сприяє, а не замінює економічне відновлення; належне врядування та безпекові питання здійснюють найбільший вплив на економічне відновлення; Уряд має концентрувати зусилля на відновленні підприємств і економічних зв'язків, а не на відновленні зруйнованого житла; необхідно впроваджувати системи «Моніторингу і оцінки»; важлива ефективна боротьба із корупцією за рахунок створення відповідної інфраструктури і електронних сервісів; треба залучати місцевий персонал та експертизу (НГО та донори не мають конкурувати за таланти і кадри із владою); важлива сталість, відсутність короткого планування і створення місцевої експертизи[2].

Під час відновлення України важливо ефективно використовувати всі наявні ресурси, незалежно від джерел їх надходження – як внутрішні державні, так і від зовнішніх партнерів. Тому важливо впроваджувати цифрові інструменти у процесах від надходження до розподілу та використання всіх видів ресурсів, у тому числі зовнішньої допомоги партнерів, управлінні державною власністю Укра-

[1] Час диджитальних змін: нова можливість для цифровізації українських громад. Децентралізація. Новини. 31 January 2023. URL: https://decentralization.gov.ua/en/news/16062.

[2] Шаповал Н., Федосеєнко М., Грибановський О., Терещенко О. Повоєнне відновлення України. Нові ринки та цифрові рішення: монографія. Kyiv School of Economics. 2022. С. 10. URL: https://kse.ua/wp-content/uploads/2022/09/Digital-instruments-in-Ukrainian-recovery.pdf.

їни, розподілі ресурсів державної та приватної власності (продаж, аукціони, оренда тощо)[1].

Цифрові інструменти дозволяють боротися з корупцією та зловживаннями, запобігають ризикам неефективного використання ресурсів[2]. Для боротьби з основними викликами відновлення, цифрові рішення мають бути спрямовані на: побудову інтегрованої цифрової платформи державного масштабу, яка дозволить бачити грошові потоки «від донору до будівництва», від державного до місцевого бюджету, у будь якому розрізі – за принципом «всі бачать все»; поєднання на платформі інформації з різних цифрових реєстрів та платформ – новостворених та наявних (наприклад, ЄДЕССМ, Prozorro, Prozorro.Sale, ДІЯ, spending.gov.ua тощо). Має бути взаємозв'язок цільових програм відновлення та коштів за ними між бюджетами усіх рівнів; впровадження модульного принципу розгортання цифрових систем, який дозволятиме інтегрувати різні ініціативи з відновлення та прозорого державного управління на єдиній цифровій платформі. Наприклад, модулі пріоритезації заявок на відновлення бізнесу, модуль заявок та обліку нефінансової допомоги, гуманітарної допомоги тощо[3].

Отже, для України варто не тільки шукати рецепти вдалих відновлень після воєн і кращих практик, але й уникнути помилок, які були в інших країнах, які проходили схожий чи подібний шлях. Незважаючи на те, що Україна досягла чудових результатів у збереженні більшої частини цих основ, військовий конфлікт підкреслив необхідність фізичного захисту цифрової інфраструктури управління, досягнення більшої інтеграції між державними організаціями та

[1] Федосеєнко М. Цифрові інструменти для відновлення України. Результати конференції. Київська школа економіки. 28 жовтня 2022 р. URL: https://www.rise.org.ua/blog-ua/cifrovi-instrumenti-dlya- vidnovlennya-ukrayini-yak-zabezpechiti-prozore-i-rozumne-upravlinnya-vidbudovoyu.

[2] Там само.

[3] Шаповал Н., Федосеєнко М., Грибановський О., Терещенко О. Повоєнне відновлення України. Нові ринки та цифрові рішення: монографія. Kyiv School of Economics. 2022. С. 4. URL: https://kse.ua/wp-content/uploads/2022/09/Digital-instruments-in-Ukrainian-recovery.pdf.

вдосконалення управління даними. Ці кроки вимагатимуть мобілізації підтримки з боку партнерства зі спільнотою GovTech, а також навчання працівників державного сектору навичкам користувача цифрового управління та стимулювання керівників державного сектору знаходити способи заохочувати інновації та підтримувати гнучкість роботи. У середньостроковій перспективі (2023–2025 рр.) можна запровадити численні фіскальні, регуляторні та фінансові механізми для підтримки розвитку післявоєнної цифрової економіки. Для компаній, і зокрема для малих і середніх підприємств (МСП), фінанси та працівники будуть двома основними ресурсами, необхідними для підтримки цифрового переходу. Що стосується фінансів, уряд України вже запровадив індивідуальний спеціальний режим оподаткування ІТ-сектору, який набув чинності 1 січня 2022 року та відомий як податковий режим «Дія Сіті». Оскільки це новий пільговий режим оподаткування, його ще потрібно перевірити на відповідність міжнародним стандартам, зокрема критеріям, встановленим у 1998 році Форумом з шкідливих податкових практик (FHTP) щодо нездорової податкової конкуренції та оновленим у 2015 році в рамках Проєкту «Розмивання оподатковуваної бази й виведення прибутку з-під оподаткування» (BEPS), асоційованим учасником якого є Україна. За умови, що цей режим оподаткування відповідає узгодженим міжнародним стандартам, він забезпечить висококонкурентний і привабливий режим оподаткування для цифрових та інноваційних ІТ-компаній і співробітників, які працюють у таких компаніях. Будь-які фіскальні заходи, які запроваджені чи будуть запроваджені Україною та входять до сфери діяльності FHTP, повинні бути проаналізовані на предмет відповідності критеріям FHTP та повинні відповідати їм[1].

Окремий значний вклад у подальше вдосконалення цифровізації в усіх сферах життя в Україні вносить проєкт «Цифрова трансформація для України» (DT4UA), що підтримується ЄС, триває з листопада

[1] Цифровізація для відновлення України. OECD. 1 липня 2022. С. 5. URL: https:// uploads- ssl.webflow.com/625d81ec8313622a52e2f031/631986262b4bd804ce8d34b6_UA%20Digitalisation%20Recover y_UKR.pdf.

2022 року до квітня 2025 року. Мета проєкту – підвищити ефективність та безпеку надання державних послуг та покращити доступ до них громадян і бізнесу в Україні відповідно до вимог ЄС, а також забезпечити швидке реагування на потреби, спричинені війною. Загальний бюджет проекту становить 17 400 000 євро. Виконавцем проєкту є Академія електронного урядування з Естонії (EGA). Проєкт DT4UA базується на досягненнях проєктів EGOV4UKRAINE та EU4DigitalUA. З 2016 року ЄС підтримує цифрову трансформацію України із загальним бюджетом понад 51 млн євро[1].

Отже, Україна повинна розробити власну модель відновлення з використанням кращих підходів, розроблених в межах інших країн після військових конфліктів, стихійних лих та з використанням сучасних цифрових інструментів. Формулювання відповідної моделі відновлення необхідно визначити с урахуванням позитивних та негативних сторін в міжнародній світовій практиці. Це є необхідним задля того, щоб не допустити в майбутньому настання небажаних для суспільства результатів та наслідків. Саме активне впровадження цифровізації, цифрових інструментів з урахуванням європейського досвіду та напрацювань надасть можливості швидко відновити Україну, та модернізувати не тільки всі її сфери, інфраструктуру але й згуртувати суспільство навколо цих досягнень.

## 1.4. Ризики та пропозиції стратегічних напрямів процесу післявоєнного відновлення України

Оскільки в Україні цифровізація розглядається як один із державних пріоритетів, необхідно виокремити її позитивні рисі, обмеження

[1] ЄС розпочинає найбільший проєкт підтримки цифрової трансформації України із загальним бюджетом 17,4 млн євро. European External Action Service (EEAS). Press and information team of the Delegation to UKRAINE. Київ. 20.02.2023. URL: https://www.eeas.europa.eu/delegations/ukraine/єс- розпочинає-найбільший-проєкт-підтримки-цифрової-трансформації-україни-із-загальним-бюджетом- 174_uk?s=232.

та ризики. Характерними рисами сучасної епохи – епохи цифровізації – є експоненційне зростання використання інтелектуальних пристроїв, швидкості інтернету та масштабів його проникнення в економічне та соціальне життя суспільства. У доповіді Світового банку про стан цифрової економіки «Цифрові дивіденди», зробленій у 2016 році, наголошується на наступних вигодах цифровізації: зростання продуктивності праці; підвищення конкурентоспроможності підприємств; зниження витрат виробництва; створення нових робочих місць; збільшення ступеня задоволеності людських потреб; подолання бідності та соціальної нерівності[1].

Враховуючи міжнародний досвід та актуальні питання вітчизняних процесів цифровізації , можливо виокремити її наступні можливості:

1) Здешевлення та спрощення вирішення типових завдань, що реалізуються шляхом проведення великих обсягів операцій, а також створення нових робочих місць і підвищення продуктивності праці.

Група експертів Світового банку зазначає, що безпосередньо у сфері цифрових технологій створюється обмежена кількість нових робочих місць, проте їх розвиток може супроводжуватися збільшенням кількості робочих місць у супутніх сферах діяльності (наприклад, у Китаї зростання електронної торгівлі призвело до створення 10 млн робочих місць в онлайн- магазинах та суміжних службах)[2].

2) Збільшення додаткових вигод для споживача (поява нових товарів електронних книг, цифрової музики; доступу до соціальних мереж, інтернет-магазинів і т.д.).

3) Розширення участі в політичному та суспільному житті, онлайн-доступ до державних послуг.

4) Підвищення якості життя, в першу чергу за рахунок поліпшення задоволення конкретних вже відомих і нових потреб людей.

[1] Маркевич К. Цифровізація: переваги та шляхи подолання викликів. Український центр економічних та політичних досліджень ім. О. Разумкова. Статті та інтерв'ю. 06 вересня 2021 р. URL: https://razumkov.org.ua/statti/tsyfrovizatsiia-perevagy-ta-shliakhy-podolannia-vyklykiv.

[2] Там само.

5) Цифровізація стає важливим джерелом технологічного домінування, та, як наслідок, глобального впливу ряду провідних країн на світовій арені.

6) Відкривається широкий спектр нових можливостей впливу на формування політичних настроїв, ведення політичної боротьби.

7) Інтернет та інші мережеві механізми дозволяють не тільки реалізувати певні комунікаційні інтереси в політиці, а й постійно вдосконалювати їх, в тому числі через використання новітніх механізмів аналізу даних.

У сфері послуг цифрові технології дозволяють здійснювати діяльність з будь-якого куточка світу, проводити відеоконференції, купувати продукти та різні побутові товари через мережу Інтернет. Цифровізація може сприяти вирішенню соціальних проблем, полегшивши доступ до основних послуг у сфері охорони здоров'я (електронна система охорони здоров'я) та освіти (дистанційне навчання), наданню фінансових послуг, прозорості та ефективності діяльності уряду (електронний уряд: система електронних регламентів та реєстрацій)[1].

Безумовно, цифровізація не обмежується виключним використанням технологій; вона характеризується зміною культури, інтегрованої в усі сфери роботи, та трансформацією в управлінні різними командами. Мінімізації витрат (цифровізація документів, що призводить до загальної оптимізації процесу), децентралізація виробництва, підвищення ефективності та продуктивності, швидке, ефективніше прийняття рішень у реальному часі, підвищення рівня екологічності, виробництво сталих продуктів, скорочення часу та витрат на розробку продукції, підвищення якості продукції та швидка реакція на зміну кон'юнктури ринку, диверсифікація виробництва зростаючої кількості виробів на численних виробничих майданчиках – не єдині переваги цифровізації.

[1] Маркевич К. Цифровізація: переваги та шляхи подолання викликів. Український центр економічних та політичних досліджень ім. О. Разумкова. Статті та інтерв'ю. 06 вересня 2021 р. URL: https://razumkov.org.ua/statti/tsyfrovizatsiia-perevagy-ta-shliakhy-podolannia-vyklykiv.

Однак цифровизація несе і потенційні ризики, серед них: несанкціонований доступ до інформації та інші загрози кібербезпеці; масове безробіття; цифрова нерівність – розриви в рівні освіти та умовах доступу до цифрових послуг та продуктів між громадянами та бізнесами всередині країн, а також між державами.

Боротьба з цифровими ризиками вимагає колективних дій організацій, які мають спільні інтереси у боротьбі з загрозами, такими як ризик цифрового регулювання або ризик кібербезпеки. Базові підходи управління ризиками викладені Міжнародною організацією зі стандартизації (ISO) у стандартах, присвячених менеджменту ризику, а також інформаційній та кібер-безпеці[1]. Проте поліпшення фізичної та інституційної цифрової інфраструктури перебуває у компетенції як уряду, і приватного сектора, так і інших учасників відносин, наприклад, міжнародних економічних організацій чи промислових асоціацій. Методичні засади мінімізації цифрових загроз зазначені у доповіді ООН «Про цифрову економіку за 2021 рік» та спрямовані на створення умов для моніторингу та стандартизації процесів використання даних, у тому числі: формування ставлення до даних як (глобального) суспільного блага; вивчення нових форм керування даними; узгодження прав та принципів, пов'язаних з цифровими технологіями та даними; розроблення норм, пов'язаних з даними; розширення міжнародного співробітництва у питаннях управління платформами, у тому числі щодо політики конкуренції та оподаткування у цифровій економіці[2].

У доповіді наголошується на необхідності міжнародної технічної координації на глобальному рівні, щоб уникнути подальшої фрагментації інфраструктури Інтернету та цифрового простору[3].

[1] Стандарти ISO/IEC захистять від кіберзагроз. ДП «УКРМЕТРТЕСТСТАНДАРТ». 31 серпня 2016. URL: http://csm.kiev.ua/index.php?option=com_content&view=article&id=3631%3.

[2] Звіт про результати за 2021 рік. Представництво Організації Об'єднаних Націй в Україні. URL: https://ukraine.un.org/sites/default/files/2022-06/UNCountryResultsReport2021UA_v02.pdf.

[3] Резнікова О. О. Національна стійкість в умовах мінливого безпекового середовища: монографія. Київ: НІСД, 2022. С. 146. URL: https://niss.gov.ua/sites/default/files/2022-03/reznikova- ukraineresilience2022_02.pdf.

Регулюючі заходи, що вживаються на державному рівні, та сприяють мінімізації системного ризику цифрової трансформації, могли б включати: встановлення чітких правил і норм щодо онлайн-контенту, конфіденційності та використання даних; підтримку конкуренції, яка допоможе стимулювати інвестиції та інновації в цифрову інфраструктуру та діяльність, насамперед, у галузі вітчизняних цифрових рішень; припинення спроб встановлення іноземного контролю в українських сегментах цифрової економіки; заохочення спільного інвестування через державно- приватне партнерство; розвиток цифрової інфраструктури державних сервісів та розширення спектру послуг, що надаються онлайн.

Серед негативних наслідків цифровізації, які частково вже виявились у межах окремих національних економік, виділяються: нерівномірність розподілу благ цифровізації, пов'язана з обмеженістю доступу до Інтернету. При цьому 60 % населення планети в даний час його не мають; зростання поляризації ринків праці і, як наслідок, конкуренції серед працівників за низькооплачувані місця через те, що нові технології заміняють стандартні трудові операції. Багато дослідників відзначають, що тотальна роботизація може викликати значні диспропорції між попитом і пропозицією на ринку праці, що призведе до зростання технологічного безробіття, позбавить заробітку багатьох працівників, призведе до втрати або зниження їх соціального статусу; зміцнення позицій природних монополій, що може стати причиною посилення концентрації на ринках. В даний час багато компаній, що вперше застосували принципово нові технології, займають домінуюче становище на ринку. Наприклад, компанія Google отримує майже третину світового доходу від цифрової реклами; посилення проблем, пов'язаних з кібербезпекою, у тому числі із захистом персональних та корпоративних даних[1]; посилення залежності особистості від цифрової інфраструктури.

[1] Див.: Дуравкін П. М., Гафич І. І. Сучасні виклики та майбутнє правового захисту персональних даних: під впливом розвитку цифровізації. *Право та інновації.* 2023. № 3 (43). С. 89–100. URL: https://doi.org/10.37772/2518-1718-2023-3(43)-12; Соснін О. Цифровізація як нова реальність України. *Юридичний вісник України*. 2020. № 1. С. 46. URL: https://lexinform.com.ua/dumka-eksperta/tsyfrovizatsiya-yak-nova-realnist-ukrayiny/.

Крім зазначенного вище, прогресивна автоматизація та використання робототехніки матиме наслідком порушення ринку праці, що характеризуватиметься безробіттям та нерівністю доходів. Через відсутність довіри до цифрових технологій, доступу до них та навичок до їх використання може збільшитися цифровий «розрив». Серед інших викликів

проблема безпеки та порушення конфіденційності, поглиблення соціальної відчуженості, стирання етичних меж (неможливість контролювати у майбутньому штучний інтелект), зниження культурного розвитку[1].

Крім цього виокремлюються і негативні наслідки від цифровізації суспільства та впровадження комп'ютерних технологій в освітнє середовище: 1. Комп'ютери навчають людину діяти на оточення маніпулятивно-директивним, інструментально-силовим чином. Це має тенденцію призводити до насильницьких актів, що рельєфно ілюструється завдяки хакерським технологіям та лавиноподібним потоком комп'ютерних вірусів. 2. Комп'ютери шкідливі через прийняту в них двозначну логіку обробки інформації, яка сприяє формуванню в людини однозначного, «чорно-білого» анти творчого, біполярного мислення. 3. Впровадження комп'ютера як головного провідника видовищних технологій сучасності значно гальмує потребу та процес читання: «у вік електронних засобів масової інформації втратили відмінність періоди дитинства і дорослого життя[2].

Цифровізація кожної галузі економіки та країни в цілому стає невідворотним явищем. Але щоб процеси цифровізації стали корисними для суспільства, необхідно вирішити такі проблеми: низький рівень цифрової грамотності населення; недостатньо розгалужена

[1] Соснін О. Цифровізація як нова реальність України. *Юридичний вісник України*. 2020. № 1. С. 46. URL: https://lexinform.com.ua/dumka-eksperta/tsyfrovizatsiya-yak-nova-realnist-ukrayiny/.

[2] Вознюк О. В. Негативні та позитивні наслідки цифровізації освітнього процесу. *Цифрова трансформація та диджитал технології для сталого розвитку всіх галузей сучасної освіти, науки і практики*: матеріали міжнар. наук.-практ. конф. Житомирський державний університет імені Івана Франка (26 січня 2023 р.). URL: http://eprints.zu.edu.ua/36321/.

ІТ-інфраструктура; недостатня кількість ІТ-фахівців; «традиційна» свідомість, орієнтована працювати з матеріальними, а не цифровими об'єктами; жорсткість корпоративних структур; необхідність радикальної перебудови бізнес- моделей та управлінських парадигм. Процес подолання викликів та негативного впливу цифровізації суспільства повинен бути вирішеним декількома заходами, як то, сприяння створенню єдиної політики цифрової комунікації у світовому просторі та вироблення єдиних вимог і регуляторів з урахуванням політичних, економічних, національних, культурних рис різних держав; цифрові інструменти повинні впроваджуватися для всіх учасників суспільних відносин незалежно від їх статусу, соціальної групи та роду занять з урахуванням їх інтересів та потреб.

Отже, цифровізація є об'єктивною реальністю, в якій існує та буде розвиватися суспільство, особливо у період відновлення. Цифровізація здійснює вплив на всі сфери суспільного життя, що особливо проявляється в корінних перетвореннях. В той же час, вплив цифровізації на подальший розвиток суспільства є неоднозначним та суперечливим, про що свідчить велика кількість загроз, що вона несе. Тому, для отримання позитивних рис від поширення цифровізації необхідними є особливий підхід до впровадження цифрових технологій у всіх сферах, з врахуванням особливостей процесів, що відбуваються та реального стану і особливостей розвитку (освітніх, економічних, політичних, соціальних, національних, культурних та ін.) всіх країн світу, а також взаємовигідна співпраця країн у поширенні та єдиному запровадженні цифрових технологій та здійснесненні контролю за цими процесами.

# 2. ДОСЛІДЖЕННЯ РОЛІ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ НА ЦИФРОВИХ ПЛАТФОРМАХ

## 2.1. Автоматизація саморегулювання в галузі авторського права на цифрових платформах

Процедури припинення порушень авторського права на цифрових платформах у сенсі саморегулювання правовідносин доволі широко запроваджуються постачальниками цифрових послуг. З 1998 року, коли ці процедури вперше з'явились в американському законі Digital Millennium Copyright Act, у різних формулюваннях вони почали проваджуватись в інших юрисдикціях поза межами США[1].

В Законі України «Про авторське право і суміжні права» (далі – Закон № 2811-IX)[2] порядок припинення порушень авторського права і (або) суміжних прав з використанням мережі Інтернет було описано вже двічі (у двох різних редакціях Закону № 2811-IX). Перша редакція містила певні недоліки[3] і, відповідно, з другою редакцію бага-

[1] Gibson J. Notice and Takedown, Here and Abroad. *The Media Institute*. September 15th, 2011. URL: http://www.mediainstitute.org/IPI/2011/091511.php.

[2] Про авторське право і суміжні права : Закон України від 01.12.2022 р. № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text.

[3] Див.: Shmatkov D., Zagalaz A. C. Notice-and-takedown procedures in Ukraine, Spain, China, and the US. *Law & innovative society*. 2022. No. 1 (18). Pp. 22–33. URL: https://doi.org/10.37772/2309-9275-2022- 1(18)-2; Шматков Д. І. Критичний огляд порядку припинення порушень авторського права і (або) суміжних прав з використанням мережі Інтернет в Україні. *Економічна безпека: міжнародний і національний*

то таких недоліків було усунуто. Сьогодні, у частині 2 статті 56 Закону № 2811-IX визначено, що заява про припинення порушення авторського права та/або суміжних прав повинна містити:

– відомості про заявника, необхідні для його ідентифікації: ім'я (найменування), місце проживання (перебування) або місцезнаходження, адреса електронної пошти або поштова адреса, на яку власник вебсайту або інші особи в передбачених Законом № 2811-IX випадках мають направляти інформацію;

– для заявників-юридичних осіб – ідентифікаційні дані про реєстрацію юридичної особи у країні місцезнаходження, зокрема в торговельному, банківському, судовому або державному реєстрі, у тому числі реквізити реєстру, реєстраційний номер;

– вид і назву об'єктів авторського права та/або об'єктів суміжних прав, іншу інформацію, що дає можливість ідентифікувати об'єкт, про порушення права на який йдеться у заяві;

– вмотивоване твердження, зазначене у відповідній заяві, про наявність у заявника майнових прав на об'єкт авторського права або об'єкт суміжних прав чи виключних прав на використання такого об'єкта з посиланням на підстави виникнення таких прав чи виключних прав та строк чинності таких прав (підстави не вказуються, якщо заявник є первинним суб'єктом відповідних майнових прав);

– гіперпосилання на електронну (цифрову) інформацію, розміщену або в інший спосіб використану на вебсайті, або гіперпосилання на вебсторінку, до якої здійснювалося інтерактивне надання доступу об'єкта авторського права або об'єкта суміжних прав, про порушення майнових прав на який йдеться у заяві;

– вимогу до власника вебсайту про унеможливлення доступу до цифрового контенту на вебсайті та/або вимогу до власника вебсайту і провайдера послуг обміну контентом щодо недопущення ними (ним) подальшого розміщення на вебсайті зазначеного цифрового контенту;

---

*рівень*: за матеріалами І-ї науково-практичної конференції (м. Харків, 27 травня 2022 року). С. 187–196. URL: https://ndipzir.org.ua/wp-content/uploads/2022/11/conf_27.05.2022.pdf.

– відомості про постачальника послуг хостингу, який надає послуги та/або ресурси для розміщення відповідного вебсайту або їх частин у мережі Інтернет та забезпечення доступу до них через мережу Інтернет, а саме: найменування; адреса електронної пошти або поштова адреса, на яку в передбачених Законом № 2811-IX випадках власник вебсайту або інші особи мають надсилати інформацію. Власник вебсайту, який розміщує свій вебсайт або його частину в мережі Інтернет на власних ресурсах та/або самостійно забезпечує доступ до нього з використанням мережі Інтернет, який надає можливість іншим особам розміщувати цифровий контент на його вебсайті, є постачальником послуг хостингу;

– твердження заявника, що наведена в заяві інформація є достовірною, а наявність у заявника прав, про порушення яких заявлено, перевірена адвокатом або представником у справах інтелектуальної власності (патентним повіреним), за представництвом (посередництвом) якого подається заява[1].

Також, якщо заявник є юридичною особою, він звертається із заявою про припинення порушення виключно за представництвом (посередництвом) адвоката або представника у справах інтелектуальної власності (патентного повіреного) і у цьому випадку до заяви про припинення порушення додається копія одного з документів, що відповідно до законодавства посвідчує повноваження адвоката або представника у справах інтелектуальної власності (патентного повіреного)[2].

Заява про припинення порушення надсилається власнику вебсайту та/або вебсторінки з одночасним направленням її копії постачальнику послуг хостингу, який надає послуги та/або ресурси для розміщення відповідного вебсайту[3].

Порівняно із Законом України «Про авторське право і суміжні права» DMCA визначає наступні складові заяви:

---

[1] Про авторське право і суміжні права : Закон України від 01.12.2022 р. № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text.

[2] Там само.

[3] Там само.

– фізичний або електронний підпис особи, уповноваженої діяти від імені власника виключного права, яке, ймовірно, порушено;

– ідентифікація захищеної авторським правом роботи, яка, як стверджується, була порушена, або якщо декілька захищених авторським правом робіт на одному вебсайті охоплюються одним повідомленням, репрезентативний список таких робіт на цьому вебсайті;

– ідентифікація матеріалу, який, як стверджується, порушує авторські права або є об'єктом такої діяльності і який має бути видалений або доступ до якого повинен бути закритий, а також інформація, достатня для того, щоб дозволити постачальнику послуг визначити місцезнаходження матеріалу;

– інформація, достатня для того, щоб постачальник послуг міг зв'язатися зі стороною, яка подала скаргу, наприклад, адреса, номер телефону і, за наявності, адреса електронної пошти, за якою можна зв'язатися зі стороною, яка подала скаргу;

– твердження про те, що сторона, яка подала скаргу, сумлінно вважає, що використання матеріалу у спосіб, на який подано скаргу, не дозволено власником авторських прав, його агентом або законом;

– твердження про те, що інформація в повідомленні є точною, і під загрозою покарання за лжесвідчення, що сторона, яка подала скаргу, уповноважена діяти від імені власника виключного права, яке, ймовірно, було порушено[1].

Не порівнюючи детально обидва підходи, можна стверджувати, що такі заяви не потребують ретельної юридичної аргументації та доведення факту порушення, але потребують дотримання усіх формальних вимог, таких як формулювання відповідних тверджень чи чітка ідентифікація твору із використанням гіперпосилань.

З практики саме недотримання формальних вимог, як, наприклад, надання гіперпосилання на сторінку продукту, а не на конкретне фото, що порушує авторські права і має відмінне від сторінки продукту гіперпосилання, або ж ігнорування включення відповідних твер-

[1] The Digital Millenium Copyright Act of 1998. Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998). URL: https://www.copyright.gov/legislation/dmca.pdf.

джень, може стати причиною відмови у видаленні чи блокуванні матеріалу, який порушує авторські права особи. Тому використання автоматичних форм подання заяв значно знижує ймовірність припуститися таких формальних помилок. Крім того, з автоматизацією надсилання заяв їхня кількість у світі зросла з тисяч до сотень мільйонів. Тому цей процес несе як переваги для заявників, так і переваги для електронних платформ, що вже не спроможні використовувати лише людську працю для обробки такої кількості заяв. Загалом швидке впровадження подібних автоматизованих систем тісно пов'язане зі зростанням професіоналізації великомасштабної реалізації права[1].

Для цілей цього дослідження розглянуто ступінь автоматизації надсилання заяв про припинення порушення авторського права та/або суміжних прав на популярних світових та українських цифрових платформах, а саме: Google, App Store, Amazon, Etsy, YouTube, Instagram, Facebook (далі – Світові Платформи), Rozetka, OLX, Епіцентр (далі – Українські Платформи).

Забігаючи на перед, можна сказати, що Світові Платформи знаходяться значно попереду Українських Платформ у контексті імплементації релевантних практик. Кожна зі згаданої Світової Платформи пропонує користувачам заповнити відповідну форму із заздалегідь прописаними розділами і полями, що відповідають вимогам DMCA. Крім того, виявлено окремі додаткові розділи (поза вимог DMCA), які у багатьох випадках можуть бути корисним прикладом для інших платформ.

Так, Google у межах свого проєкту для припинення порушень авторського права Lumen додатково пропонує підписати наступну заяву: «Я розумію, що копія кожного судового повідомлення може надсилатися в проєкт Lumen для оприлюднення й документування. Я також розумію, що команда Lumen вилучає особисту контактну інформацію зі сповіщень, перш ніж їх публікувати, але в багатьох

[1] Urban J. M., Karaganis J., Schofield B. Notice and takedown in everyday practice. *UC Berkeley Public Law Research Paper*. 2017. No. 2755628. URL: http://dx.doi.org/10.2139/ssrn.2755628.

випадках може залишити моє ім'я». Google також пропонує функціонал відстежування статусу розгляду заяви.

App Store надає можливість вказати всі території, на яких оскаржується програма, та території, на яких відстоюються права.

Amazon дозволяє користувачам самостійно визначити тип порушення та зазначити інформацію щодо реєстрації авторського права за її наявності.

Etsy пропонує обрати категорію, що найкраще описує твір, захищений авторським правом.

YouTube дозволяє обрати варіанти видалення (одразу або надання порушнику 7 днів для самостійного видалення) та використати можливість заборонити завантаження копій відео.

Отже, Світові Платформи, окрім того, що пропонують користувачам заповнити формалізовані (згідно з DMCA) заяви онлайн, активно удосконалюють саморегулювання для більш якісного реагування на порушення авторського права.

На момент проведення цього дослідження у жовтні 2023 року Українські Платформи не пропонували користувачам заповнювати формалізовані (Законом України «Про авторське право і суміжні права») заяви онлайн.

Rozetka надає відповідну адресу електронної пошти для надсилання заяв. Маркетплейс доволі неочікувано на сторінці під назвою «Захист авторських прав» описує процедури «подання запитів», пов'язаних з використанням бренду / знака / торгової марки (ТМ) тощо та порушенням прав на промисловий зразок. Також несподівано Rozetka посилається на DMCA за наявності українського Закону № 2811-IX. Ще однією «інновацією» маркетплейсу є вимога надсилати перші дві сторінки паспорта заявника. Також сторінка не містить інформації про право на подання зустрічної заяви та можливість звернення до суду, що є складовою процедур, які прийшли з DMCA[1].

[1] Див.: Захист авторських прав. Зворотний зв'язок та рейтинг. Останнє оновлення: 18.08.2023. URL: https://sellerhelp.rozetka.com.ua/p294-copyright-protection.html.

На OLX звернення відбувається через чат. Епіцентр пропонує звертатися до служби підтримки клієнтів, при чому за релевантними запитами під час пошуку у Google, пошуковий сервіс у першу чергу видає лише книги з інтелектуальної власності, що продаються на маркетплейсі, а не сторінку для подання заяв про порушення прав інтелектуальної власності чи інформацію щодо такої можливості.

Хоча Законом № 2811-IX встановлено, що заява повинна містити конкретні твердження, Українські Платформи про такі твердження в інструкціях не згадують.

Навіщо пропонувати користувачам онлайн форми для припинення порушень авторського права? По-перше, це зручно, адже немає необхідності шукати відповідальну особу на стороні постачальника послуг та вивчати закони на предмет коректного складання заяви. Але зручність електронних платформ не є правовою наукою. З точки зору права, таке рішення значно збільшує масштаби припинення порушень[1], оскільки зручність, про яку мова йшла раніше, дозволяє користувачам легше та швидше надсилати заяви і отримувати зворотний зв'язок, а надавачам послуг – їх обробляти у відповідності із чинним законодавством.

Недостатнє врахування Закону № 2811-IX та ігнорування Українськими Платформами сучасних практик, можливо, є результатом небажання отримувати та обробляти значну кількість повідомлень, або нести додаткові витрати на автоматизації процесів, або результатом недостатнього розуміння положень Закону № 2811-IX, або інших чинників. Законом № 2811-IX встановлено, що власник вебсайту, вебсторінки не несе відповідальності за порушення авторського права та/або суміжних прав, вчинені з використанням мережі Інтернет, якщо він вчасно вчинив відповідні дії (частина 15 статті 56)[2] – саме така «безпечна гавань» є стимулом до впровадження постачаль-

[1] Urban J. M., Karaganis J., Schofield B. Notice and takedown in everyday practice. *UC Berkeley Public Law Research Paper*. 2017. No. 2755628. URL: http://dx.doi.org/10.2139/ssrn.2755628.

[2] Про авторське право і суміжні права : Закон України від 01.12.2022 р. № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text.

никами послуг процедур повідомлення та видалення матеріалу, що, ймовірно, порушує авторські права. Тому недостатнє розуміння положень Закону № 2811-IX через недостатню обізнаність та/або обмежену судову практику у питанні виглядає найочевиднішим поясненням ситуації – у той час, коли науковці сперечаються про впровадження DMCA Plus для керування і автоматизації реагування на заяви, отримані через відповідні форми на Світових Платформах, Українські Платформи ще знаходяться на дуже початковому етапі автоматизації, який ще й недостатньо відображає вимоги чинного законодавства.

## 2.2. Ліцензійні угоди на використання інтелектуальної власності користувачів на цифровому ринку

Сьогодні у цифровому середовищі користувачі продукують значні обсяги інтелектуальної власності. Хоча така інтелектуальна власність на цифрових платформах відноситься до різноманітних об'єктів[1], авторське право тут є домінуючим. В цілому, закони, що охоплюють авторське право, постійно розвиваються, щоб йти в ногу з новими технологіями та інтересами творців, споживачів і посередників у різних галузях[2]. З'являються такі документи, як, наприклад, Закон США про авторське право в цифрову епоху (DMCA) чи Директива ЄС 2019/790 про авторське право і суміжні права на Єдиному цифровому ринку Європейського Союзу (далі – Директива ЄС 2019/790).

[1] Див.: Шматков Д. І. Фан-арт та право інтелектуальної власності на платформах електронної комерції. *Право та інновації.* 2023. № 2 (42). С. 80–85. URL: https://doi.org/10.37772/2518-1718-2023-2(42)-10; Shmatkov D., Hlibko S., Tokarieva K. у Cachón Zagalaz J. On the question of why copyright cannot be synonymous with intellectual property within digital competence frameworks. *Revista La Propiedad Inmaterial*. 2021. No. 32. Pp. 215–231. URL: https://doi.org/10.18601/16571959.n32.07.

[2] Peukert C., Windisch M. The Economics of Copyright in the Digital Age. *Center for Law & Economics Working Paper Series.* 2023. No. 4. URL: https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/639999/CLE_WP_2023_04.pdf?sequence=1.

Стало зрозумілим, що такі процеси потребують встановлення цивільних прав та обов'язків, а саме дозволів на використання об'єктів права інтелектуальної власності, що визначаються відповідними ліцензійними договорами між сторонами (електронною платформою та користувачем).

Електронні платформи широко впроваджують власні стандартні ліцензійні договори, за яким користувачі надають їм деякі майнові права. І знаходячись сьогодні на певному етапі налагодженості цих процесів постає декілька актуальних питань – на скільки зміст таких договорів врегульовано на національних та міжнародному рівні, як положення нормативних документів відображено у ліцензійних договорах між користувачами та платформами, як стандарти щодо цих документів враховують потреби зацікавлених сторін?

Питання використання ліцензійних договорів на цифрових платформах досліджували такі учені, як: Р. Бірстонас, М. Віндіш, Л. Гвібальт, С. ван Гомпель, Дж. Гінсбург, А. Келлі, В. Мантров, К. Пюкерт, О. Саламанка, У. Фургал, Р. Таус та інші автори. У наукових працях широко розкрито застосування норм Директиви ЄС 2019/790 про авторське право на Єдиному цифровому ринку Європейського Союзу та національних законів з авторського права, питання винагороди авторів та припинення строку чинності ліцензійних договорів. Опубліковані праці здебільшого приділяють увагу виключним ліцензіям і лише обмежено розкривають питання невиключних ліцензій та їхнього галузевого застосування, поверхнево порівнюють у цій проєкції договори різних платформ.

Метою представленого дослідження є визначення змісту стандартних положень невиключних ліцензій, що пропонують цифрові платформи, за окремими галузями з урахуванням норм національних та міжнародних нормативно-правових документів і з огляду на балансування потреб зацікавлених сторін.

Для досягнення мети цього дослідження використано метод науково-правового аналізу нормативних документів, літератури та ліцензійних договорів, представлених на електронних платформах, а також наукові методи порівняння та узагальнення.

Для аналізу випадковим чином обрано такі галузі людської діяльності у цифровому просторі, як електронна комерція та пошук роботи. Окрему увагу приділено групі соціальних мереж Meta, пошуковій платформі Google та сервісу розміщення відеоматеріалу YouTube.

Ліцензійні договори, представлені на електронних платформах порівняно за наступними критеріями: вид ліцензії, об'єкти інтелектуальної власності за оригінальною термінологією, надані права, окремо право надання субліцензій (оскільки це значно збільшує можливості використання інтелектуальної власності ліцензіатом), строк чинності, території чинності прав, наявність роялті, можливість відкликання, гарантії чистоти творів від прав третіх осіб. Отримані результати далі згруповано за галузями людської діяльності.

Коротке порівняння змісту ліцензійних договорів маркетплейсів Amazon (Amazon, 2023)[1], Rozetka (Rozetka, 2023)[2] та OLX (OLX Group, 2023)[3] представлено у табл. 1.

**Таблиця 1 – Порівняння змісту ліцензійних договорів маркетплейсів**

| Платформа / Розділи | **amazon.com (далі – Amazon)** | **rozetka.com.ua (далі – Rozetka)** | **olx.ua (далі – OLX)** |
|---|---|---|---|
| Назва документу, де описано ліцензійні умови | Amazon Services Business Solutions Agreement | Умови використання сайту | Правила Сервісу OLX.ua |
| Вид ліцензії | невиключна | невиключна | невиключна |

[1] Amazon (2023). *Amazon Services Business Solutions Agreement*. Retrieved from https://sellercentral.amazon.com/gp/help/1791.

[2] Rozetka (2023). *Умови використання сайту*. Retrieved from https://rozetka.com.ua/ua/pages/terms/.

[3] OLX Group (2023). *Правила Сервісу OLX.ua*. Retrieved from https://help.olx.ua/olxuahelp/s/article/%D0%BF%D1%80%D0%B0%D0%B2%D0%B8%D0%BB%D0%B0-%D1%81%D0%B5%D1%80%D0%B2%D1%96%D1%81%D1%83-olxua-V1.

| **Платформа** / **Розділи** | **amazon.com (далі – Amazon)** | **rozetka.com.ua (далі – Rozetka)** | **olx.ua (далі – OLX)** |
|---|---|---|---|
| Об'єкти інтелектуальної власності | матеріали, торговельні марки | контент | зміст відгуку, контент, що може включати оголошення, незалежно від їх форми, тобто текстові, графічні та відеоматеріали, є об'єктами права інтелектуальної власності, включаючи авторські права і право промислової власності |
| Надані права | використовувати, відтворювати, виконувати, відображати, поширювати, адаптувати, змінювати, переформатувати, створювати похідні роботи та іншим чином комерційно чи некомерційно використовувати будь-яким способом будь-які та всі матеріали | відображати, пересилати, розповсюджувати, відтворювати, публікувати, дублювати, адаптувати, модифікувати, перекладати, створювати похідні дані, і будь-яким іншим способом використовувати будь-який або весь контент користувача в будь-якій формі, що відома або на даний момент невідома, будь-яким чином і для будь-яких цілей, які можуть бути вигідні для нас, функціонування Он-лайн платформи Rozetka, надання/ отримання будь-яких послуг | запис, відтворення і поширення оголошення повністю або частково з метою його відображення на Веб-сайті – OLX Group і партнерам OLX Group, через яких здійснюється просування Веб-сайту, а також в будь-якому місці за допомогою Інтернет, включаючи пошукові системи і соціальні мережі |

| Платформа / Розділи | **amazon.com (далі – Amazon)** | **rozetka.com.ua (далі – Rozetka)** | **olx.ua (далі – OLX)** |
|---|---|---|---|
| Право надання субліцензій | так | так | так |
| Території | весь світ | весь світ | весь світ |
| Роялті | ні | ні | ні |
| Можливість відкликання | ні | ні | ні |
| Строк чинності | безстрокова | безстрокова | обмежена |
| Гарантії чистоти творів від прав третіх осіб | так | так | так |

Зміст ліцензій, що пропонуються вебсайтами пошуку роботи work.ua1 та indeed.com2 представлено у Таблиці 2.

**Таблиця 2 – Порівняння змісту ліцензійних договорів вебсайтів пошуку роботи**

| Платформа / Розділи | **work.ua (далі – Work)** | **ua.indeed.com (далі – Indeed)** |
|---|---|---|
| Назва документу, де описано ліцензійні умови | Правила та умови використання сайту | Умови обслуговування |
| Вид ліцензії | невиключна | невиключна |
| Об'єкти інтелектуальної власності | оголошення, матеріали | користувацький вміст, торговельні марки, відгуки |
| Надані права | Змінювати зовнішній вигляд оголошень (використовувати заголовки, марковані та нумеровані списки); редагувати або видаляти матеріали, опубліковані користувачем на сайті, якщо вони не відповідають умовам цієї угоди, завдають шкоди | Створення, використання, продаж, субліцензування, переформатування, відтворення, розповсюдження, виконання, демонстрація, відображення, використання для похідних робіт та інше застосування всього Користувацького |

[1] Ворк Україна (2023). *Правила та умови використання сайту*. https://www.work.ua/about-us/conditions/.

[2] Indeed (2023). *Умови обслуговування*. Retrieved from https://ua.indeed.com/legal?hl=uk&from=gnav-homepage#employers.

| Платформа / Розділи | **work.ua (далі – Work)** | **ua.indeed.com (далі – Indeed)** |
|---|---|---|
| | компанії або третім особам, а також на свій власний розсуд без зазначення причини; використовувати для своїх цілей матеріали, опубліковані Користувачем на Сайті і що знаходяться у відкритому доступі, зокрема, для розміщення матеріалів на сайтах партнерів | вмісту, який розміщує користувач або надсилає, для публікації матеріалів на вебсайті компанії Indeed або її партнерів чи сайтах третіх осіб, підтримки або вдосконалення вебсайту Indeed, а також просування Indeed і такого Користувацького вмісту без обмежень |
| Право надання субліцензій | так | так |
| Території | Україна | весь світ |
| Роялті | ні | ні |
| Можливість відкликання | так | так |
| Строк чинності | обмежений | обмежений |
| Гарантії чистоти творів від прав третіх осіб | так | так |

Meta[1] пропонує Умови надання послуг, де зазначено, що платформа без надання ліцензійної винагороди ліцензіату отримує невиключну ліцензію на контент користувача, що діє в усьому світі і дозволяє зберігання, використання, розповсюдження, зміну, запуск, копіювання, публічне виконання або показ, переклад контенту та створення похідних робіт на його основі з правом надання субліцензії третім особам. Дія ліцензії припиняється, коли контент видаляється з систем Meta, але ліцензія діятиме доти, доки контент не буде повністю видалений. Угода містить гарантії чистоти творів від прав третіх осіб.

Ліцензію Google[2] викладено у документі під назвою «Загальні Положення та Умови Google», ліцензію YouTube[3] – у документі «Умови

[1] Сайт facebook.com. Умови надання послуг. 26 липня 2022 р. URL: https://uk-ua.facebook.com/legal/terms.

[2] Сайт google.com. Загальні положення та умови Google. Діє з 5 січня 2022 р. Версія країни: Україна. URL: https://policies.google.com/terms?hl=ua.

[3] Сайт youtube.com. Умови користування. 5 січня 2022 р. URL: https://www.youtube.com/t/terms#f617e3e92e.

використання». Ці ліцензії ідентичні Угоді Користувача Meta. Єдиною і дуже важливою особливістю ліцензії YouTube є можливість отримання роялті від інших користувачів за рахунок монетизації їх творів, що включають твір чи твори ліцензіара.

Для аналізу отриманих даних необхідно виходити з потреб зацікавлених сторін. Які вимовлені та невимовлені потреби спонукають користувача та платформу підписувати ліцензійну угоду? Ймовірно, зі сторони користувача це доступ до нового інструменту досягнення бізнес- цілей, збільшення прибутку. Для платформи, скоріш за все, це засіб отримання доходу та конкурентної боротьби з іншими платформами через отримання і представлення нових пропозицій, підсилення органічного просування у мережі за рахунок унікального чи різноманітного вмісту, впевненість у чистоті творів від прав інтелектуальної власності третіх осіб. У пункті 61 преамбули Директиви ЄС 2019/790, зазначено, що важливо сприяти розвитку ринку ліцензування між правовласниками та постачальниками послуг обміну онлайн-контентом. Ці ліцензійні угоди мають бути справедливими та підтримувати розумний баланс між обома сторонами. Розглянуті платформи відповідають статті 17 Директиви ЄС 2019/790 в аспекті надання адекватної інформації користувачам про функціонування їхньої практики[1].

Перше, але не головне, що привертає увагу у проведеному аналізі – ліцензійні угоди є складовою інших документів, назви яких відрізняються від платформи до платформи. Відомо, що використання стандартних угод було б зручним, зрозумілим та ефективним способом повідомити про права та обов'язки обох сторін[2]. Крім того, такі ви-

[1] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market. URL: https://eur-lex.europa.eu/legal- content/EN/ALL/?uri=CELEX:32019L0790.

[2] Див.: Berg J., Furrer M., Harmon E., Rani U., Silberman, M. S. Digital labour platforms and the future of work. Towards decent work in the online world. Geneva, Switzerland: International Labour Office, 2018. URL: https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/--- publ/documents/publication/wcms_645337.pdf; Flick C. Informed consent in information technology: Improving end user licence agreements. *Professionalism in the Information and Communication Technology Industry*. The Australian

моги є особливо актуальними через необхідність легкого знаходження і розуміння усіх умов співробітництва для платформ, що, окрім пошуку роботи, пропонують виконання онлайн-роботи[1].

Усі з проаналізованих вебсайтів просять від користувачів невиключну ліцензію. Відповідно до частини 3 статті 1108 Цивільного кодексу України ліцензія на використання об'єкта права інтелектуальної власності може бути виключною, одиничною, невиключною, а також іншого виду, що не суперечить закону. Невиключна ліцензія не виключає можливості використання ліцензіаром об'єкта права інтелектуальної власності у сфері, що обмежена цією ліцензією, та видачі ним іншим особам ліцензій на використання цього об'єкта у зазначеній сфері[2]. Таке рішення електронних платформ цілком відповідає як їхнім потребам, так і інтересам користувачів. Важливо зазначити, що rozetka.com.ua та work.ua не зазначають вид ліцензії, але відповідно до частини 4 статті 50 Закону України «Про авторське право і суміжні права» у разі відсутності визначення у ліцензійному (субліцензійному) договорі виду ліцензії вважається, що ліцензія є невиключною[3].

Об'єкти інтелектуальної власності, зазначені в ліцензіях описано доволі нетиповими для законів широкими термінами, як, наприклад, контент, користувацький вміст, оголошення, матеріали. З однієї сторони, такий підхід, ймовірно, забезпечує більше розуміння користувачами положень угоди, адже вона написана на «їхній мові». З іншої сторони, такі визначення охоплюють більше, ніж один, об'єкт авторського права – наприклад, в «оголошення» може входити літератур-

National University. 2013. Pp 127–154. URL: https://library.oapen.org/bitstream/handle/20.500.12657/33527/1/459997.pdf#page=135.

[1] Berg J., Furrer M., Harmon E., Rani U., Silberman, M. S. Digital labour platforms and the future of work. Towards decent work in the online world. Geneva, Switzerland: International Labour Office, 2018. URL: https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/--- publ/documents/publication/wcms_645337.pdf.

[2] Цивільний кодекс України : Закон України від 16.01.2003. № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text.

[3] Про авторське право і суміжні права : Закон України від 01.12.2022 р. № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text.

ний твір, твір образотворчого мистецтва, фотографічні твори, аудіовізуальні твори, а іноді і торговельні марки та інші об'єкти промислової власності тощо, на які ліцензіар не бажає надавати права. Приклади додавання торговельних марок до ліцензій, що зазвичай охоплюють авторське право, на OLX, Amazon та Indeed є показовими.

Цифрові платформи намагаються охопити максимальну кількість прав, які їм необхідні для забезпечення власної функціональності та отримання конкурентних переваг. При цьому учені звертають увагу, що одним з фокусів політики у цьому напрямі можуть стати гармонізовані обмеження на обсяг передачі прав на майбутні твори та виконання та майбутні способи використання[1]. Окремим пунктом стоїть право надання субліцензій – іноді така практика є корисною для користувача (наприклад, для просування товару поза межами маркетплейсу із залученням платформою підрядників), але іноді це може зашкодити користувачам, як, наприклад, у випадках, коли маркетплейс переходить від ролі надавача цифрових послуг до ролі продавця[2] і може використовувати отримані права як засіб конкурентної боротьби з ліцензіаром[3].

Майже всі з проаналізованих платформ зазначають, що ліцензія діє в усьому світі. Лише work.ua не викладає цього пункту в договорі, а згідно з частиною 4 статті 50 Закону України «Про авторське право і суміжні права» у разі відсутності визначення у ліцензійному договорі території дії ліцензійного договору (ліцензії) дія ліцензії поши-

[1] Kur A., Schovsbo J. Expropriation or Fair Game for All? The Gradual Dismantling of the IP Exclusivity Paradigm. *Intellectual Property in a Fair World Trade System. Proposals for Reforming TRIPS.* 2011. Pp. 408– 451.URL: https://books.google.com.ua/books?hl=da&lr=&id=hKaeEz6PA8UC&oi=fnd&pg=PA408&ots=_sn41 fbB7v&sig=mlQDGNEQqyHdb2FhFYJzrF7kbuU&redir_esc=y#v=onepage&q&f=false.

[2] Aversa P., Haefliger S., Hueller F., Reza D. G. Customer complementarity in the digital space: Exploring Amazon's business model diversification. *Long Range Planning.* 2021. No. 5. Vol. 54. URL: https://openaccess.city.ac.uk/id/eprint/23775/3/Amazon_LRP_paper%20R2.pdf.

[3] Див.: Дуравкін П. М., Гафич І. І. Сучасні виклики та майбутнє правового захисту персональних даних: під впливом розвитку цифровізації. *Право та інновації.* 2023. № 3 (43). С. 89–100. URL: https://doi.org/10.37772/2518-1718-2023-3(43)-12.

рюється на територію України[1]. Міжнародна дія ліцензії пов'язана як з глобальністю мережі, так і з міжнародною дією авторського права, але відповідні закони різних країн відрізняються один від одного в різних аспектах (наприклад, умови припинення чинності ліцензійного договору, максимальний строк його дії тощо). Крім того, електронні платформи можуть мати регіональні представництва, як, наприклад, amazon.com.br (Бразилія), amazon.cn (Китай), amazon.fr (Франція) тощо, а використання тих же творів на різних територіях може суперечити стратегії та візії ліцензіара (наприклад, нейтральний текст в одній країні може виявитись неконкурентним в іншій, що вплине на репутацію бренду).

Жодна платформа не пропонує користувачу отримання роялті за використання його прав інтелектуальної власності. Indeed особливо ретельно розписує цей пункт, використовуючи такі фрази, як «ви не маєте права на жодну винагороду в жодній формі у зв'язку з реалізацією компанією Indeed своїх прав за дозволом» та «у тих випадках, коли відповідно до чинного законодавства вам належить винагорода у зв'язку з реалізацією компанією Indeed таких прав, ви цим відмовляєтеся від усіх прав на таку винагороду максимальною мірою, якою це дозволено чинним законодавством»[2]. Особливо дискусійним це питання є у контексті надання права субліцензування.

У пункті 3 преамбули Директиви ЄС 2019/790 зазначено, що для того, щоб досягти добре функціонуючого та справедливого ринку авторського права, також повинні існувати правила щодо прав на публікації, щодо використання творів чи інших об'єктів постачальниками онлайн-послуг, які зберігають та надають доступ до завантаженого користувачами вмісту, про прозорість авторських і виконавських договорів, про винагороду авторів і виконавців, а також механізм анулювання прав, які автори і виконавці передали на виключних засадах. У пункті 61 преамбули Директиви ЄС 2019/790 зазначено,

[1] Про авторське право і суміжні права : Закон України від 01.12.2022 р. № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text.

[2] Сайт ua.indeed.com. Умови обслуговування. 1 листопада 2023 р. URL: https://ua.indeed.com/legal?hl=uk&from=gnav-homepage#employers.

що правовласники повинні отримувати відповідну винагороду за використання їхніх творів чи інших об'єктів. Однак, оскільки ці положення не повинні впливати на договірну свободу, правовласники не повинні бути зобов'язані давати дозвіл або укладати ліцензійні угоди. Пункт 82 преамбули Директиви ЄС 2019/790 містить уточнення про те, що ніщо в Директиві ЄС 2019/790 не слід тлумачити як перешкоду власникам виключних прав згідно із законодавством Союзу про авторське право дозволяти використання їхніх творів або інших об'єктів безоплатно, у тому числі через невиключні безкоштовні ліцензії на користь будь-яких користувачів. У статті 18 Директиви ЄС 2019/790 встановлено, що Держави-члени гарантують, що у випадках, коли автори та виконавці ліцензують або передають свої виключні права на використання своїх творів чи інших об'єктів, вони мають право отримувати відповідну та пропорційну винагороду[1].

Як можна побачити вище, питання винагороди у Директиві ЄС 2019/790 розглядається з чітким ухилом у сторону виключних прав, тоді як розглянуті ліцензії є невиключними.

У частині 3 статті 12 Закону України «Про авторське право і суміжні права» встановлено, що незалежно від відчуження права використовувати твір будь-яким способом (способами), а також виключного права дозволяти або забороняти використання твору іншими особами на твір, автор має право на справедливу винагороду за відповідні способи використання твору[2].

Чи доцільно дискутувати про винагороду автору у контексті питання, що розглядається? Окремі учені стверджують, що ексклюзивність повинна бути домінуючою моделлю регулювання тільки там і в тій мірі, в якій інші, неексклюзивні схеми не можуть досягти таких самих або навіть кращих результатів та/або створити більш сприятливі наслідки для суспільства в цілому, що не обов'язково означає

[1] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32019L0790.

[2] Про авторське право і суміжні права : Закон України від 01.12.2022 р. № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text.

безкоштовність доступу або використання, якщо ексклюзивність спричиняє неоптимальні ефекти, натомість елемент власності може зберігатися тому, що користувач зобов'язаний платити за привілей необмеженого доступу[1]. Деякі науковці зазначають, що законодавчо визначені права на винагороду поступово привертають увагу політиків як регуляторні інструменти, оскільки вони становлять середину між ексклюзивністю та безкоштовним використанням[2]. Інші учені бачать недоліки і в системі винагороди, запропонованій Директивою ЄС 2019/790 стосовно ексклюзивних прав[3]. Ефективна система винагороди правовласникам за невиключну ліцензію, яку коментують учені як зразкову[4], діє на платформі YouTube. Тому практика винагороди за невиключну ліцензію не є чимось недоречним у контексті предмету дослідження.

У пункті 80 преамбули Директиви ЄС 2019/790 зазначено, що у випадку, коли автори та виконавці ліцензують або передають свої права, вони очікують, що їхня робота чи виконання будуть використані. Однак, може статися так, що твори чи виконання, які були ліцензовані або передані, взагалі не використовуються. У такому випадку та після закінчення розумного періоду часу автори та виконав-

[1] Kur A., Schovsbo J. Expropriation or Fair Game for All? The Gradual Dismantling of the IP Exclusivity Paradigm. *Intellectual Property in a Fair World Trade System. Proposals for Reforming TRIPS*. 2011. Pp. 408– 451.URL: https://books.google.com.ua/books?hl=da&lr=&id=hKaeEz6PA8UC&oi=fnd&pg=PA408&ots=_sn41 fbB7v&sig=mlQDGNEQqyHdb2FhFYJzrF7kbuU&redir_esc=y#v=onepage&q&f=false.

[2] Geiger, C., & Bulayenko, O. (2022). Creating Statutory Remuneration Rights in Copyright Law: What Policy Options Under the International Legal Framework?. *Centre for International Intellectual Property Studies Research Paper Series,* Research Paper. No. 2020-05. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3927331.

[3] Mantrov, V., Birstonas, R., Karklins, J., Kelli, A., Kull, I., Buka, A., Barkane, I., & Davida, Z. (2022). The implementation of the new consumer sales directives in the baltic states: a step towards further harmonisation of consumer sales. *New Legal Reality: Challenges and Perspectives,* II, 504. URL: https://www.apgads.lu.lv/fileadmin/user_upload/lu_portal/apgads/PDF/Konferences/2022/iscflul-8- 2/iscflul.8.2.36.Mantrov_ea.pdf.

[4] Див.: Boroughf, B. (2015). The next great YouTube: improving content ID to Foster creativity, cooperation, and fair compensation. *Albany Law Journal of Science & Technology,* 25, 95-127. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2492898; Ginsburg, J. C. (2022). Authors' Remuneration: Reforms To Wish For. Columbia Public Law Research Paper, 122-137. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4150857.

ці повинні мати можливість скористатися механізмом анулювання прав, який дозволяє їм передавати або ліцензувати свої права іншій особі. Тому у статті 22 Директиви ЄС 2019/790 визначено, що Держави-члени повинні забезпечити, щоб у випадках, коли автор або виконавець ліцензував або передав свої права на твір або інший об'єкт, що охороняється, на ексклюзивній основі, автор або виконавець міг повністю або частково відкликати ліцензію або передачу прав, якщо немає використання такого твору чи іншого захищеного об'єкта[1]. У Директиві ЄС 2019/790 мова йде про виключні права.

Чи існує практика відкликання неексклюзивних прав у цифровому світі? Розробники ліцензії Creative Commons, «вірусний» вплив якої не завжди має позитивний ефект на матеріальному добробуті правовласників[2], не вважають таку практику доречною і пропонують невідкличні ліцензії[3], на що часто не звертають уваги користувачі. Google, YouTube, Meta, Work та Indeed обрали іншу тактику і пропонують можливість відкликання ліцензії разом із видаленням творів. Допоки залишається нерозкритим питання чи існують ефективні інструменти видалення вмісту, що розповсюдився. Тому, скоріш за все, раціонально покладати відповідальність на користувача за таке видалення.

Строк чинності ліцензій визначений безстроковим (тобто є строком чинності прав інтелектуальної власності) такими платформами, як Amazon та Rozetka. Хоча такий строк може тлумачитись і як невизначений і тоді будуть включатися положення національних законів, де подібні аспекти врегульовано (про це мова піде далі.) Позиція Rozetka, ймовірно, не містить протиріч із Законом України «Про авторське право і суміжні права», але оскільки платформа отримує

[1] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market. URL: https://eur-lex.europa.eu/legal- content/EN/ALL/?uri=CELEX:32019L0790.

[2] Ginsburg, J. C. (2022). Authors' Remuneration: Reforms To Wish For. *Columbia Public Law Research Paper,* 122-137. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4150857.

[3] Creative Commons (2023). *Frequently asked questions*. URL: https://creativecommons.org/faq/.

всесвітню ліцензію, в інших юрисдикціях можуть виникнути проблеми.

У США (юрисдикції вирішення спорів, зокрема, з Amazon) 17 U.S. Code § 203 встановлює, що припинення дії ліцензії може бути здійснено в будь-який час протягом п'ятирічного періоду, починаючи з кінця 35 років із дати укладання угоди; або, якщо ліцензія охоплює право на публікацію твору, період починається після закінчення 35 років з дати публікації твору за ліцензією або після закінчення 40 років з дати виконання договору, незалежно від того, який термін закінчується раніше. Звичайно, строк у 35 років для цифрових відносин недалеко відійшов від безстроковості. Крім того, цей Закон не охоплює твори, створені за наймом, а припинення не є автоматичним і вимагає відповідного інформування ліцензіата ліцензіаром[1].

Як і Rozetka, Amazon просить всесвітню ліцензію і, як і Rozetka, ця платформа стикнеться із законодавчими обмеженнями за межами США: в Австрії якщо право на використання твору не використовується взагалі або лише в такому недостатньому обсязі, що завдає шкоди важливим інтересам автора, автор може достроково припинити договірні відносини, що стосуються права використання твору; у Болгарії встановлено максимальний термін дії ліцензії, що складає 10 років; у Данії угода припиняється за відсутності використання твору протягом 3-х років після виконання передачі твору, якщо ліцензіат не почне використання протягом 6 місяців з дати отримання відповідного повідомлення; у Франції строк ліцензії на використання твору для рекламних цілей може складати лише від 1-го до 5-ти років; у Нідерландах автор може розірвати угоду повністю або частково, якщо інша сторона не використовує авторське право на твір у достатньому обсязі протягом розумного періоду часу після укладення угоди (творець повинен письмово встановити розумний термін для використання твору в достатньому обсязі) тощо[2]. Крім того, у законах

[1] Termination of Transfers and Licenses Under 17 U.S.C. §203. URL: https://www.copyright.gov/docs/203.html.

[2] Furgal, U. (2020). Reversion rights in the European Union Member States. CREATe Working Paper 2020/11. URL: https://zenodo.org/records/4281035.

країн ЄС можуть застосовуватися (і точково застосовуються) положення Директиви 2011/77/EU Європейського Парламенту та Ради від 27 вересня 2011 року про внесення змін до Директиви 2006/116/ЄС про термін охорони авторського права та деяких суміжних прав.

Work та OLX (цілеспрямовано чи ні) не зазначають такого строку, тому відповідно до абзацу 3 частини 4 статті 50 Закону України «Про авторське право і суміжні права» договір вважається укладеним на строк, що залишився до спливу строку чинності виключного майнового права на визначений у договорі об'єкт права інтелектуальної власності, але не більше ніж на п'ять років. Якщо за шість місяців до спливу зазначеного п'ятирічного строку жодна із сторін не повідомить письмово другу сторону про відмову від договору, договір вважається продовженим на невизначений строк. У такому разі кожна із сторін може в будь-який час відмовитися від договору, письмово повідомивши про це другу сторону за шість місяців до розірвання договору, якщо більший строк для повідомлення не встановлений за домовленістю сторін[1]. Звичайно, ці положення повинен знати користувач для ефективного управління правами інтелектуальної власності, тому бажано було б зазначати таку інформацію у договорі, особливо із урахуванням не завжди достатнього рівня обізнаності неспеціалістів у питаннях інтелектуальної власності[2].

Строк чинності ліцензій на інших проаналізованих платформах закінчується разом із відкликанням творів.

Усі платформи встановлюють неприйнятність порушення прав третіх осіб матеріалами користувача, що можна оцінювати лише позитивно.

Таким чином, ліцензійна угода на електронній платформі, ймовірно, може викладатися у трьох варіантах.

---

[1] Про авторське право і суміжні права : Закон України від 01.12.2022 р. № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text.

[2] Див.: Lin, C. (2021). Exploration of intellectual property protection strategies for cross-border e- commerce. In *E3S Web of Conferences* (Vol. 245, p. 01062). EDP Sciences. URL: https://www.e3s- conferences.org/articles/e3sconf/abs/2021/21/e3sconf_aeecs2021_01062/e3sconf_aeecs2021_01062.html; Popova, K., & Nacka, M. (2017). Intellectual property rights knowledge and awareness–academic level empirical analysis and recommendations. *Journal of Contemporary Economic and Business Issues*, 4 (1), 41-54. URL: https://www.econstor.eu/handle/10419/193473.

Варіант 1 – бачення платформи:

• зручна для платформи назва документу (найчастіше – угода користувача), де окремим пунктом описується ліцензійна угода;

• невиключна ліцензія (менший обсяг, але дає можливість не сплачувати роялті);

• максимальна кількість об'єктів інтелектуальної власності «під соусом» оголошення / контент / матеріали;

• максимальна кількість прав, включаючи право надання субліцезій;

• всесвітнє охоплення;

• відсутність можливості відкликання;

• строк чинності, що дорівнює строку чинності прав інтелектуальної власності;

• відсутність роялті;

• гарантії від ліцензіара щодо чистоти творів від прав третіх осіб.

Варіант 2 – бачення користувача:

• зрозуміла і зручна для виявлення ліцензія окремим документом;

• невиключна ліцензія (менший обсяг прав, порівняно з виключною ліцензією, можливість надати таку ж ліцензію іншим платформам);

• мінімальний законодавчо визначений перелік об'єктів авторського права;

• мінімально необхідна для просування товару чи послуги користувача кількість прав, виключаючи право надання субліцезій без чіткого лімітування такого права;

• охоплення лише цільових для бізнесу країн;

• можливість відкликання, покладення відповідальності за видалення творів на платформу;

• чітко визначений строк чинності, що дорівнює строку очікуваної бізнес-активності;

• роялті, обумовлений нецільовим для бізнесу користувача використанням інтелектуальної власності, а також роялті за схемою YouTube, де платформа виступає технічним посередником;

• відсутність гарантій чистоти творів від прав третіх осіб від ліцензіара.

Варіант 3 – законодавчо та технічно обґрунтована з використанням досвіду позитивних практик площина:

• зрозуміла і зручна для виявлення ліцензія окремим документом;

• невиключна ліцензія;

• законодавчо визначений перелік об'єктів авторського права, обсяг якого обумовлений режимом найефективнішого функціонування платформи;

• мінімально необхідна для просування товару чи послуги користувача кількість прав та отримання конкурентних переваг платформою, при чому право надання субліцензій законодавчо обмежено певним переліком активностей (наприклад, у цілях маркетингу, реклами та просування);

• охоплення лише цільових для бізнесу країн за наявності таких можливостей на платформі (наприклад, регіональні вебсайти Amazon);

• можливість відкликання за схемою Google, YouTube та Meta;

• чітко визначений законодавчо строк чинності, з можливістю пролонгації за згодою сторін;

• роялті, обумовлений нецільовим для бізнесу користувача використанням інтелектуальної власності, а також роялті за схемою YouTube, де платформа виступає технічним і фінансовим (за наявності відповідних дозволів) посередником;

• гарантії чистоти творів від прав третіх осіб від ліцензіара.

Очевидно, що сьогодні перший варіант, скоріш за все побачать користувачі на платформі, але третій найкраще враховує інтереси усіх сторін за відповідності законам та технічним потребам, як і можливостям платформ. Все ще залишаються неврегульовані аспекти з перерахованих, у тому числі на міжнародному рівні – ці питання можуть стати предметом подальших досліджень. Але і надмірне регулювання може стати зайвим, коли окремі практики саморегулювання у галузі авторського права у цифровому просторі демонструють свою ефективність[1]. Закони про авторське право працюють через

[1] Див.: Shmatkov D., Zagalaz A. C. Notice-and-takedown procedures in Ukraine, Spain, China, and the US. *Law & innovative society*. 2022. No. 1 (18). Pp. 22–33. URL: https://doi.org/10.37772/2309-9275-2022- 1(18)-2.

ринкові стимули[1]. Тут позитивний досвід відомих платформ стане в нагоді. Хоча проаналізовані цифрові платформи характеризуються різними функціональними особливостями, вмістом, цільовою аудиторією тощо, викладені пропозиції можуть бути імплементовані без огляду на ці відмінності, але з додаванням релевантних специфіці платформи положень.

## 2.3. Фан-арт та право інтелектуальної власності на платформах електронної комерції

Фан-арт є розповсюдженим явищем і, ймовірно, виходить із природи імітування культури консюмеризму. Подібно до фанфіків та мемів, фан-арт полягає у створенні фанатами продуктів, що імітують оригінальні продукти, які є популярними на ринку – персонажів, сцен, книг, зображень, дизайнів, творів мистецтва тощо. У більшості випадків фан-арт продукує похідні твори, що, наприклад, у Законі України «Про авторське право і суміжні права», визначені як твори, що є результатом творчої переробки іншого твору без завдання шкоди його охороні (анотація, адаптація, аранжування, кавер-версія, обробка нематеріальної культурної спадщини тощо) чи його творчим перекладом на іншу мову (частина 1 статті 17)[2]. Подібні визначення зустрічаються і в законах інших країн. Тому трансформаційні роботи фан-арту є похідними роботами від оригінального твору[3], автор якого залишає за собою майнові права інтелектуальної власності на оригінальний

[1] Див.: Towse, R. (2018). Copyright Reversion in The Creative Industries: Economics and Fair Remuneration. *The Columbia Journal of Law & The Arts*, 41 (3), 467–489. URL: https://doi.org/10.7916/jla.v41i3.2023.

[2] Про авторське право і суміжні права : Закон України від 01.12.2022 р. № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text.

[3] Див.: Shmatkov D. Copyright Issues in Digital Society: Sports Video Games. *Intellectual Systems and Information Technologies*: International Scientific and Practical Conference (Odesa, Ukraine, 13-19 September 2021). 2021. P. 310–316. URL: https://ceur-ws.org/Vol-3126/paper45.pdf.

твір, у тому числі право забороняти чи дозволяти використовувати похідні роботи. У той час, як питання слідування кумирам є актуальним предметом психології, соціології та інших наук, комерційно-правові аспекти фан-арту також мають важливе значення.

Електронні маркетплейси є стандартом сучасності[1]. Зокрема, з розвитком електронної комерції у Цифрову Епоху бізнеси, що концентруються на виготовленні та продажі фанатських товарів, сьогодні широко розповсюджують свої продукти у мережі Інтернет. З огляду на визначені аспекти розподілу, використання та управління правами інтелектуальної власності на фан-арт, проблема потребує відповідних досліджень.

Поєднання фан-арту та прав інтелектуальної власності здебільшого аналізується ученими у наступних трьох проєкціях[2]:

1. розподіл прав інтелектуальної власності між авторами оригінальних творів та фанатами / особами, які використовують твір;

2. економічний та репутаційний ефект від трансформаційного використання прав інтелектуальної власності авторів популярних творів;

3. адекватність сучасного законодавства, що регулює питання.

У цілому науковці підтверджують те, що трансформація і використання твору з комерційною метою без згоди правовласника є у будь-якому випадку порушенням його прав. При цьому зазначається, що заохочення залучення шанувальників, не жертвуючи здатністю авто-

[1] Див.: Shmatkov D., Zagalaz A. C. Notice-and-takedown procedures in Ukraine, Spain, China, and the US. *Law & innovative society*. 2022. No. 1 (18). Pp. 22–33. URL: https://doi.org/10.37772/2309-9275-2022-1(18)-2.

[2] Див.: Morgan R. Conventional Protections for Commercial Fan Art Under the U.S. Copyright Act. *Fordham Intellectual Property Media and Entertainment Law Journal*. 2021. No. 2. Vol. 31 XXXI. Article 4. Pp. 514–573. URL: https://ir.lawnet.fordham.edu/iplj/vol31/iss2/4; Guerra-Pujol F. E. Of Coase and Copyrights: *The Law and Economics of Literary Fan Art. Journal of Intellectual Property and Entertainment Law*. New York University. 2019. No. 1. Vol. 9. Pp. 91–106. URL: https://jipel.law.nyu.edu/vol-9-no-1-3-guerrapujol/; Edwards L., Schafer B., Harbinja E. Future Law: Emerging Technology, Regulation and Ethics. Edinburgh University Press, 2020. URL: https://etica.uazuay.edu.ec/sites/etica.uazuay.edu.ec/files/public/Future%20Law%20Emerging%20Technology%2C%20Ethics%20and%20Regulation%20by%20Lilian%20Edwards.pdf.

рів отримувати прибуток від своїх оригінальних творів, сприяє розвитку галузей[1]. Фан-арт завдає шкоди творцям, які бажають зберегти контроль або накласти право вето на похідні твори, але потенційні переваги фан-арту значно переважають ці потенційні збитки[2]. Часто правовласники не переслідують своїх шанувальників, а навпаки, дозволяють такій креативності діяти як інструмент залучення клієнтів і оцінюють масштаби творчості фанатів як ознаку власної популярності. Учені також підіймають питання включення фан-арту у перелік практик добросовісного використання, визначених законами[3].

Варто зазначити, що у дослідженнях обговорюються широкі питання, проте деталі та практична реалізація теорії поки залишаються поза увагою учених. Чи достатньо говорити про авторське право та інколи про торговельні марки, коли мова йде про порушення прав інтелектуальної власності творцями продуктів фан-арту? Яку інфраструктуру пропонують платформи комерції (зокрема електронної) задля правомірного використання популярних творів? Ці питання є актуальними, але поки відповіді на них недостатньо розкриті у науковій літературі.

Мета підрозділу полягає у визначенні складових інфраструктури платформ електронної комерції, що забезпечує правомірне використання інтелектуальної власності творців популярних продуктів.

Для підсилення розуміння актуальності представленого дослідження і вимог, які можуть висуватися відповідній інфраструктурі маркетплейсу, далі наведено кейс з юридичної практики автора.

---

[1] Див.: Morgan R. Conventional Protections for Commercial Fan Art Under the U.S. Copyright Act. *Fordham Intellectual Property Media and Entertainment Law Journal.* 2021. No. 2. Vol. 31 XXXI. Article 4. Pp. 514–573. URL: https://ir.lawnet.fordham.edu/iplj/vol31/iss2/4.

[2] Див.: Guerra-Pujol F. E. Of Coase and Copyrights: The Law and Economics of Literary Fan Art. *Journal of Intellectual Property and Entertainment Law*. New York University. 2019. No. 1. Vol. 9. Pp. 91–106. URL: https://jipel.law.nyu.edu/vol-9-no-1-3-guerrapujol/.

[3] Див.: Edwards L., Schafer B., Harbinja E. Future Law: Emerging Technology, Regulation and Ethics. Edinburgh University Press, 2020. URL: https://etica.uazuay.edu.ec/sites/etica.uazuay.edu.ec/files/public/Future%20Law%20Emerging%20Techno logy%2C%20Ethics%20and%20Regulation%20by%20Lilian%20Edwards.pdf.

E-commerce-підприємець створив у вигляді раритетного засобу для освітлення копію культового взуття всесвітньо відомого бренду. Він певний час успішно продавав цей продукт, отримуючи багато позитивних відгуків від покупців, підвищуючи рейтинг акаунту та його місце у пошуковій видачі. Через декілька років після початку продажів, ставши помітним, за зверненням юридичної компанії, яка представляла інтереси правовласника, акаунт і лістинг було заблоковано через порушення прав інтелектуальної власності на торговельну марку та дизайн. E-commerce-підприємець, отримавши скаргу, намагався зв'язатись з правовласником чи будь-яким представником правовласника. Першою знахідкою був пункт в Політиці управління інтелектуальною власністю, в якому йшла мова про те, що ця всесвітньо відома компанія взагалі прямо не відповідає на запити щодо надання прав інтелектуальної власності третім особам і не обговорює такі запити. Контактів представників не містилось на відповідних сторінках вебсайту. Через місяць була отримана відповідь від однієї з багатьох юридичних компаній, які, на думку E-commerce-підприємця, могли представляти всесвітньо відому компанію і яким він попередньо надсилав листи, про те, що запит не може бути задоволений.

Які факти, порівняно з фактами, представленими у проаналізованих наукових дослідженнях, відкрив цей кейс?

По-перше, фан-арт може порушувати не лише авторське право у вигляді похідних робіт. Хоча порушення прав на дизайн (чи промислові зразки, як їх прийнято називати в Україні) у позовах до суду йдуть часто поряд із порушенням авторського права, особливо коли це стосується креативних індустрій[1]. Можна дискутувати чи було у кейсі порушення прав на дизайн, оскільки у США (маркетплейс зареєстровано у США) він потребує обов'язкової реєстрації, а також він повинен відноситись до конкретного «корисного» продукту, проте платформа електронної комерції не уповноважена в цьому роз-

[1] Див.: Woods M., Monroig M. Fashion Design and Copyright in the US and EU. World Intellectual Property Organization. IPR. Geneva, November, 17. 2015. URL: https://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ipr_ge_15/wipo_ipr_ge_15_t2.pdf.

биратись, а акаунт та лістинг продукту залишились заблокованими. Також тут правовласники можуть апелювати до порушення прав на знаки для товарів та послуг – про це згадується у відомих дослідженнях, але доволі рідко, порівняно з авторським правом.

По-друге, стає зрозумілим, що власники популярних товарів не завжди бачать або розуміють переваги фан-арту для їхнього бізнесу і не завжди толерують його.

По-третє, платформи електронної комерції не завжди забезпечують зручність та правомірність займатися фан-артом або «мерчем» – порушення прав інтелектуальної власності тривалістю у декілька років, неусвідомлення підприємцем правових ризиків, нерозуміння умов можливої ліцензії, декілька місяців безрезультатних пошуків контактів та комунікацій – усе це призвело до великих фінансових та репутаційних втрат E-commerce-підприємця та, виходячи зі скарги, певних втрат правовласника.

Проаналізуємо інфраструктуру, що забезпечує правомірне використання інтелектуальної власності творців популярних продуктів, яку пропонують відомі маркетплейси. Для аналізу обрано такі платформи, як eBay (загальна спеціалізація), Etsy (загальна спеціалізація), Amazon (загальна спеціалізація та спеціалізація на фан-арті), Redbubble (спеціалізація на фан-арті) та Teepublic (спеціалізація на фан-арті, належить Redbubble).

Результати аналізу узагальнено і представлено у Таблиці 3.

Таблиця 3. Складові інфраструктури платформ електронної комерції, що забезпечують правомірне використання інтелектуальної власності творців популярних продуктів

| **Складові інфраструктури** | **Платформи електронної комерції** | | | | |
|---|---|---|---|---|---|
| | **eBay** | **Etsy** | **Amazon Merch on Demand** | **Redbubble** | **Teepublic** |
| Політика інтелектуальної власності | Так | Так | Так | Так | Так |

| Складові інфраструктури | Платформи електронної комерції | | | | |
|---|---|---|---|---|---|
| | **eBay** | **Etsy** | **Amazon Merch on Demand** | **Redbubble** | **Teepublic** |
| Залучення правовласника | Так | Ні | Так | Так | Так |
| Залучення творця фан-арту | Ні | Ні | Так | Обмежено | Обмежено |
| Перелік компаній, відкритих до співробітництва | Так | Ні | Так | Так | Так |
| Комунікація з правовласником | Так | Ні | Так | Так | Так |
| Стандартні ліцензійні угоди | Обмежено | Ні | Так | Обмежено | Обмежено |
| Укладання ліцензійних угодчерез платформу | Ні | Ні | Так | Так | Так |
| Доступне портфоліо інтелектуальної власності | Обмежено | Ні | Ні | Ні | Ні |
| Перенесення домовленостей на інші платформи | Ні | Ні | Ні | Обмежено | Обмежено |

Ознайомлення і надання згоди з політиками інтелектуальної власності на платформах електронної комерції є однією з відправних точок запуску електронного бізнесу. Як раніше було обґрунтовано, для забезпечення правомірного використання інтелектуальної власності творців популярних продуктів правовласники повинні бути залучені до процесу формулювання вимог та умов використання такої інтелектуальної власності. Оскільки попередні дослідження[1]

[1] Див.: Morgan R. Conventional Protections for Commercial Fan Art Under the U.S. Copyright Act. *Fordham Intellectual Property Media and Entertainment Law Journal*. 2021. No. 2. Vol. 31 XXXI. Article 4. Pp. 514–573. URL: https://ir.lawnet.fordham.edu/iplj/vol31/iss2/4; Guerra-Pujol F. E. Of Coase and Copyrights: The Law and Economics of Literary Fan Art. *Journal of Intellectual Property and Entertainment Law*. New York University. 2019. No. 1. Vol. 9. Pp. 91–106. URL: https://jipel.law.nyu.edu/vol-9-no-1-3-guerrapujol/; Edwards L., Schafer B., Harbinja E. Future Law: Emerging Technology, Regulation and Ethics.

свідчать про те, що правовласники мають пряму зацікавленість в існуванні фан-арту, творці таких продуктів також можуть мати можливість формувати свої пропозиції на платформах. Наявність стандартних ліцензій відомих компаній на платформах дають можливість пришвидшити процес досягнення цілей сторін, а творцям фан-арту порівняти умови та обрати найкращу пропозицію, оцінити ризики, побудувати бізнес-план тощо. Ті ж переваги для творців фан-арту несуть і списки відкритих до співробітництва компаній. Крім того, така взаємодія є корисною і для електронних платформ, оскільки, очевидно, знижує ризики отримання судових позовів щодо порушення прав інтелектуальної власності від таких компаній. Укладання ж ліцензійних угод через платформу є стандартом Цифрової Епохи. Опис доступного портфоліо інтелектуальної власності, з однієї сторони, може дозволити розширити співпрацю, а з іншої сторони, надасть творцю фан-арту розуміння усіх бар'єрів використання інтелектуальної власності третьої сторони. Останньою типовою складовою такої інфраструктури є можливість перенесення домовленостей на інші платформи, що дає переваги обом сторонам та у деяких випадках і маркетплейсу.

Кожен з представлених у таблиці маркетплейсів ознайомлює користувачів з політиками інтелектуальної власності, які легко знайти на вебсайтах компаній, а також пропонує різноманітні програми для боротьби з порушеннями прав інтелектуальної власності.

Хоча фан-арт і не є основною спеціалізацією eBay, у проєкції забезпечення правомірного використання інтелектуальної власності творців популярних продуктів програма компанії VeRO (Verified Rights Owner Program) пропонує задовільні можливості. VeRO дозволяє власникам прав інтелектуальної власності та їхнім уповноваженим представникам повідомляти про лістинги на платформі, які можуть порушувати ці права[1]. Відповідно до Програми учасники

Edinburgh University Press, 2020. URL: https://etica.uazuay.edu.ec/sites/etica.uazuay.edu.ec/files/public/Future%20Law%20Emerging%20Technology%2C%20Ethics%20and%20Regulation%20by%20Lilian%20Edwards.pdf.

[1] eBay. Verified Rights Owner Program. URL: https://www.ebay.com/sellercenter/ebay-for-business/verified-rights-owner-program.

у вільному форматі описують власні політики інтелектуальної власності (незалежно від політики eBay), куди можуть входити, наприклад, умови ліцензійних угод, доступне портфоліо інтелектуальної власності, контакти відповідальних осіб тощо. Але зміст таких політик тут не регламентується, тому уся необхідна інформація як може міститися у цих документах, так може бути і відсутньою. Перелік компаній, включених у програму, знаходиться у вільному доступі.

Etsy, хоча і спеціалізується на творах ручної роботи, що потенційно можуть містити одразу декілька видів інтелектуальної власності, окрім політики інтелектуальної власності, пропонує користувачам лише платформу подання скарг на порушення прав інтелектуальної власності, для чого необхідно додати онлайн власну зареєстровану торговельну марку[1]. Перелік компаній, включених у програму, поки не знаходиться у вільному доступі. Іншого функціоналу у контексті цього дослідження Etsy не пропонує.

Amazon Merch on Demand пропонує ліцензійну програму Merch Collab[2] для створення колаборацій через ліцензії між Amazon, власниками брендів, кваліфікованими дизайнерами та виробниками. Особливістю програми у контексті дослідження є те, що Amazon є стороною ліцензійних угод, та, відповідно, тут не передбачена можливість перенесення умов використання продукту на інші маркетплейси. Ще однією особливістю програми є те, що предметом угоди є використання дизайну, що підтверджує тезу про те, що фан-арт охоплює не лише авторське право (звичайно, дизайн може охоплюватися, у тому числі, і авторським правом). З проаналізованих складових на платформі також поки відсутня інформація про доступне портфоліо інтелектуальної власності залучених компаній.

Fan Art Program, представлена на Redbubble[3] та Teepublic[4], є ідентичною для обох платформ, ймовірно, через те, що Teepublic належить

[1] Etsy. Etsy Reporting Portal. URL: https://www.etsy.com/ipreporting.

[2] Amazon. Merch Collab. URL: https://sell.amazon.com/programs/collab.

[3] Redbubble. Fan Art Program. URL: https://help.redbubble.com/hc/en-us/articles/360000938143-Fan-Art- Program.

[4] Teepublic. Fan Art Program Overview. URL: https://teepublic.zendesk.com/hc/en-us/articles/360022642254-Fan-Art-Program-Overview.

Redbubble. Тому головною особливістю тут є можливість перенесення домовленостей між ліцензіаром та ліцензіатом від одного маркетплейсу до іншого. Процес автоматичного отримання ліцензії складається з декількох простих етапів і заснований на ознайомленні творцями фан-арту з вимогами брендів, після чого E-commerce-підприємці завантажують продукт на платформу, позначають його відповідним тегом і очікують на підтвердження або відмову від потенційного ліцензіара. При цьому кожна відома компанія висуває власні умови до змісту угоди. На сьогодні на платформах не передбачено наявність інформації про повне портфоліо інтелектуальної власності компаній. Також творці фан-арту не можуть завантажити свої пропозиції для одночасно усіх потенційних партнерів, таку можливість мають лише великі компанії.

З короткого аналізу можна побачити, що більша спеціалізація на фан- арті обумовлює більші зусилля на створенні інфраструктури правомірного використання інтелектуальної власності творців популярних продуктів. У той же час, на погляд автора, такі платформи могли б, у першу чергу, додатково зробити ширшими можливості використання ліцензійних угод за межами платформ та підсилити залучення творців фан-арту до двосторонньої взаємодії з правовласниками.

Отже, отримані результати підтверджують актуальність вивчення та удосконалення правових відносин між великими компаніями та творцями фан-арту, встановлену попередніми дослідженнями. Представлене дослідження також розширює попередні розробки у контексті використання різних видів інтелектуальної власності у відповідній комерційній діяльності. Суттєвим науковим внеском є розгляд проблеми в контексті електронної комерції (E-commerce) – такий підхід дозволив опонувати прихильникам думку про те, що власники популярних продуктів схильні дозволяти використання похідних від таких продуктів задля цілей ще більшої популяризації. Ймовірно, ця думка у попередніх дослідженнях здебільшого відносилась до некомерційного використання, але межа з комерційним використанням фан-арту є надзвичайно тонкою – цей аспект може

бути перспективним для подальших досліджень. Тому саме з огляду на природу електронної комерції, що детермінує комерційне використання продуктів, питання створення ефективної інфраструктури платформ електронної комерції, які забезпечують правомірне використання інтелектуальної власності творців популярних продуктів, було розкрито у цьому дослідженні.

## 2.4. Правові аспекти демонстрування винаходів оборонного призначення на українських краудфандингових платформах

У воєнний час суспільства концентрують усі свої можливості задля надання відсічі ворогові. В Україні одним з найяскравіших прикладів такої концентрації зусиль є краудфандинг. Зазначений метод залучення коштів став масовим[1] і дуже активно використовується, серед іншого, для покупки обладнання для Збройних Сил України[2]. Окрім купівлі готового військового обладнання, краудфандинг використовується для підтримки розроблення інноваційного озброєння національними виробниками[3] – особливості правового регулювання цього підходу потребують аналізу з огляду на наступні питання:

– чи можуть власники вебсайту демонструвати продукти, називаючи їх винаходами, якщо ці продукти не пройшли офіційну екс-

[1] Див.: Kunertova, D. (2023). The war in Ukraine shows the game-changing effect of drones depends on the game. *Bulletin of the Atomic Scientists, 79*(2), 95-102. URL: https://doi.org/10.1080/00963402.2023.2178180.

[2] Див.: Amdal, A. S. D. (2022). Civilian and Private Actors' Support of Ukrainian National Resistance. FFI-Note. External note 22/02157. URL: https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/3076/(U)%2022-02157%20-%20Eksternnotat.pdf; Redko, O., Moskalenko, O., & Vdodovych, Y. (2022). The Role of Crowdfunding Systems During Crises and Military Actions. *Baltic Journal of Economic Studies*, 8(4), 117-121. URL: https://doi.org/10.30525/2256-0742/2022-8-4-117-121.

[3] Національна платформа винахідників та винаходів воєнного часу. URL: https://braveinventors.com.

пертизу Українського національного офісу інтелектуальної власності та інновацій?

– чи можуть зазначені продукти відноситись до секретних винаходів та які обмеження це накладає на відповідне розкриття?

Далі наведено аналіз, що надає детальні та обґрунтовані відповіді на ці питання.

Варто зазначити, що, хоча краудфандинг прямо не згадується в українському законодавстві, наприклад, Закон України «Про платіжні послуги», надає багато положень, що можуть застосовуватися для регулювання галузі. Виходячи з піднятих питань у цьому дослідженні, необхідно звернути увагу на статтю 33 згаданого Закону, якою забороняються поширення в будь-якій формі та в будь-який спосіб надавачами платіжних послуг (іншими особами від імені та/або за дорученням надавачів платіжних послуг) неповної, неточної або недостовірної інформації (у тому числі в рекламі) про їхню діяльність у сфері надання платіжних послуг, про платіжні послуги, які вони надають, про умови отримання таких платіжних послуг, а також недобросовісна реклама у сфері платіжних послуг[1]. У частині 1 статті 27 Закону України

«Про рекламу» зазначено, що особи, винні у порушенні законодавства про рекламу, несуть дисциплінарну, цивільно-правову, адміністративну та кримінальну відповідальність відповідно до закону[2]. У статті 27 Регламенту ЄС 2020/1503 Про європейських постачальників послуг краудфандингу для бізнесу визначено, що інформація, що міститься в маркетинговому повідомленні, має бути достовірною, ясною і не вводити в оману[3].

Чи є достовірною інформація про те, що гроші збираються на винахід, але такий продукт не пройшов офіційну експертизу Україн-

[1] Про платіжні послуги: Закон Уркаїни від 30.06.2021 № 1591-IX. URL: https://zakon.rada.gov.ua/laws/show/1591-20#Text

[2] Про рекламу : Закону України від 03.07.1996 р. № 270/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/270/96-вр#Text.

[3] Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32020R1503.

ського національного офісу інтелектуальної власності та інновацій і не отримав патент на винахід? Загалом питання промислової власності не є простими[1] і потребують певних знань[2]. Тут необхідно розглянути два етапи – визнання експертизою винахідницького рівня, новизни та промислової придатності, а також безпосереднє отримання патенту та правового захисту.

Розглянемо у цьому контексті Закон України «Про охорону прав на винаходи і корисні моделі»[3]. У тексті Закону постійно використовується фраза «патент на винахід» – це є доказом того, що створення винаходу передує отриманню патенту на нього. Та сама фраза використовується і в Паризькій конвенції з охорони промислової власності від 20 березня 1883 р.[4] У словнику Європейського патентного відомства зазначено, що для того, щоб бути патентоспроможним, винахід має бути новим, включати винахідницький рівень (тобто не бути очевидним для тих, хто має звичайні навички у певній галузі винаходу) і бути придатним для промислового застосування[5] – «винахід» і його «патентоспроможність» є термінами, що можна розділити.

Необхідно навести ще декілька очевидних прикладів, з яких стає зрозуміло, що відсутність патенту не обмежує використання слова «винахід» поряд із продуктом:

– винахід отримав патент в одній країні, але не отримав в Україні – це все ще винахід;

---

[1] Див.: Shmatkov, D. (2021, October). Intellectual Property Management of Industrial Software Products: The Case of Triol Corp. In 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T) (pp. 108-112). URL: https://doi.org/10.1109/PICST54195.2021.9772237.

[2] Див.: Shmatkov D., Hlibko S., Tokarieva K., Zagalaz J. C. On the question of why copyright cannot be synonymous with intellectual property within digital competence frameworks. *Revista La Propiedad Inmaterial*. 2021. No. 32. Pp. 215–231. URL: https://doi.org/10.18601/16571959.n32.07.

[3] Про охорону прав на винаходи і корисні моделі : Закон України від 15.12.1993 р. № 3687-XII. URL: https://zakon.rada.gov.ua/laws/show/3687-12#Text.

[4] Paris Convention for the Protection of Industrial Property of March 20, 1883. WIPO Database of Intellectual Property Legislative Texts. URL: https://www.unido.org/sites/default/files/2014- 04/Paris_Convention_0.pdf.

[5] EPO. Glossary. URL: https://www.epo.org/service-support/glossary.html#i.

– винахід пройшов експертизу в Україні, яка підтвердила наявність у ньому новизни, винахідницького рівня та промислової придатності, але заявник не сплатив збір за видачу патенту і не отримав правового захисту – це все ще винахід;

– продукт пройшов би експертизу в Україні, яка б підтвердила наявність у ньому новизни, винахідницького рівня та промислової придатності, але таку заявку не було подано (або подано несвоєчасно) – це все ще винахід;

– винахід пройшов експертизу в Україні, заявник отримав патент, але не сплатив збори за підтримання чинності або обмежений термін чинності патенту сплив – це все ще винахід.

Другим аспектом, який потребує розгляду у цьому контексті є питання

«Чи є достовірною інформація про те, що гроші збираються на винахід, але такий продукт не пройшов офіційну експертизу Українського національного офісу інтелектуальної власності та інновацій?» (незалежно від наявності патенту). Відповідно до словника Європейського патентного відомства[1], винаходом є новий продукт, процес або апарат або будь-яке нове їх використання – тут чітко висувається умова наявності новизни для того, щоб називати продукт, процес або апарат винаходом.

У статті 1 Закону України «Про охорону прав на винаходи і корисні моделі» зазначено, що винаходом є результат інтелектуальної, творчої діяльності людини в будь-якій сфері технології[2] – навіть вимоги наявності новизни тут немає. Тобто в українських реаліях винаходом може вважатися, наприклад, творчий зворотний інжиніринг або творче копіювання запатентованого винаходу. Але, оскільки предметом дослідження є демонстрування винаходів оборонного призначення саме на українських краудфандингових платформах, необхідно прийняти визначення, представлене саме в Законі України «Про охорону прав на винаходи і корисні моделі» і зробити висновок

[1] EPO. Glossary. URL: https://www.epo.org/service-support/glossary.html#i.

[2] Про охорону прав на винаходи і корисні моделі : Закон України від 15.12.1993 р. № 3687-XII. URL: https://zakon.rada.gov.ua/laws/show/3687-12#Text.

про те, що не встановлено порушення жодного зі згаданих законів через демонстрування продукту з використанням слова «винахід».

Останнім правовим аспектом, який необхідно тут розглянути, є питання віднесення продуктів оборонного призначення до секретних винаходів.

Відповідно до статті 8 Закону України «Про державну таємницю» до такої таємниці, серед іншого, у сфері оборони відноситься інформація про винаходи, дослідження і розробку нових зразків озброєння в інтересах забезпечення національної безпеки і оборони та про результати таких досліджень і розробок[1].

У статті 1 Закону України «Про охорону прав на винаходи і корисні моделі» зазначено, що секретним винаходом є винахід, що містить інформацію, віднесену до державної таємниці, права на який засвідчуються патентом на секретний винахід[2]. Відповідно до частини 8 статті 16 цього ж Закону державний експерт приймає рішення про віднесення винаходу до секретних винаходів[3]. Стаття 10 Закону України «Про державну таємницю» описує порядок віднесення інформації до державної таємниці, яке здійснюється мотивованим рішенням державного експерта з питань таємниць за його власною ініціативою, за зверненням керівників відповідних державних органів, органів місцевого самоврядування, підприємств, установ, організацій чи громадян[4]. Очевидно, що секретні винаходи не можуть вільно демонструватися на краудфандингових платформах.

Оскільки згідно із частиною 4 статті 23 Закону України «Про охорону прав на винаходи і корисні моделі» відомості про державну реєстрацію секретного винаходу не публікуються[5], важко перевірити

[1] Про державну таємницю : Закон України від 21.01.1994 р. № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text.

[2] Про охорону прав на винаходи і корисні моделі : Закон України від 15.12.1993 р. № 3687-XII. URL: https://zakon.rada.gov.ua/laws/show/3687-12#Text.

[3] Там само.

[4] Про державну таємницю : Закон України від 21.01.1994 р. № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text.

[5] Про охорону прав на винаходи і корисні моделі : Закон України від 15.12.1993 р. № 3687-XII. URL: https://zakon.rada.gov.ua/laws/show/3687-12#Text.

чи віднесено продукти, представлені на українських краудфандингових платформах, до секретних винаходів, але можна спробувати покластися на правову обачність власників відповідних вебсайтів та ініціативність (про яку мова йде в законодавстві) державних експертів, які б, ймовірно, віднесли винаходи до секретних, якщо б у цьому була потреба і для цього були підстави.

Окрім того, варто звернути уваги на ще декілька положень: відповідно до статті 27 Закону України «Про охорону прав на винаходи і корисні моделі» володілець патенту на секретний винахід має право внести відповідному Державному експертові пропозицію про розсекречування винаходу (корисної моделі) чи зміну встановленого ступеня секретності[1]. У свою чергу, згідно із частиною 1 статті 29 Закону України «Про інформацію» інформація з обмеженим доступом може бути поширена, якщо вона є суспільно необхідною, тобто є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення[2]. Другу норму, звичайно, значно важче застосувати у контексті питання, ніж першу, але загалом необхідно зафіксувати як можливість переходу винаходу до секретного винаходу, так і руху у зворотному напрямі.

Отже, використання слова «винахід» під час демонстрування продуктів оборонного призначення на українських краудфандингових платформах не порушує норм розглянутих законів. Ризики порушення режиму секретності винаходів під час такого демонстрування є невисокими.

[1] Про охорону прав на винаходи і корисні моделі : Закон України від 15.12.1993 р. № 3687-XII. URL: https://zakon.rada.gov.ua/laws/show/3687-12#Text.

[2] Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

# 3. РЕГУЛЮВАННЯ ПЕРСОНАЛЬНИХ ДАНИХ: ПРАВО ТА ЦИФРОВІЗАЦІЯ

## 3.1. Базові засади регулювання персональних даних

Можна стверджувати, що новий етап регулювання даних на рівні ЄС почався зі скасування Директиви про захист даних 95/46/EC (DPD) та прийняття General Data Protection Regulation (GDPR). Даний акт, з одного боку, спрямовано на підвищення прав осіб при опрацюванні їх персональних даних приватним сектором і більшою частиною державного сектору. А, з іншого боку, на забезпечення незалежного моніторингу як за захистом даних, так й за вільним обігом даних, коли це не шкодить правам та інтересам пов'язаних с такими з даними осіб.

Загалом однією з причин розробки GDPR, що був прийнятий на заміну Директиви про захист даних 95/46/EC (DPD), можна вважати надмірну прив'язку застарілого акту до технічної інфраструктури, яка зазнала суттєвих змін у наступні роки після прийняття DPD. Відзначається, що «ландшафт даних» був повністю змінений вибуховим розповсюдженням повсюдних і мобільних обчислень та вступом в еру великих даних. Втім не менш важливим недоліком DPD називалася й недостатня узгодженість його правового регулювання на території різних європейських країн, оскільки в процесі імплементації його норм до місцевого законодавства національні регулятори отримали чималий простір для вільного тлумачення окремих положень[1].

[1] Politou E., Alepis E., Patsakis C. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*. 2018. Vol. 4, Issue 1. Art. tyy001. https://doi.org/10.1093/cybsec/tyy001.

Варто відзначити, що впровадження вимог щодо захисту даних через Регламент, а не Директиву, само по собі підвищує уніфікованість правової бази та свідчить про те, що регулювання персональних даних виходить з рівня держав-членів на рівень ЄС (а, як мова піде далі – навіть за межі ЄС). Будучи «директивою», законодавча ефективність DPD значною мірою залежала від бажання окремих держав-членів імплементувати її норми в національне законодавство.

Окрім того, прагнучі не повторювати помилок попереднього акту, європейський законодавець змістив увагу з технічних вимог та докладних стандартів до більш абстрактного опису, що, перш за все, позначає кінцеву мету, а не технічні інструменти її досягнення. У той же час це зробило GDPR здебільшого суто юридичним документом, який майже не надає технічних вказівок суб'єктам, що зобов'язані впроваджувати його положення. Хоча такий підхід є свідомим вибором та дозволяє якомога довше залишатися акту актуальним, він має й негативні сторони.

Наприклад, серйозні труднощі та технічні занепокоєння викликала відповідність існуючих процедур резервного копіювання у контексті задоволення вимог на забуття. При використанні інформаційно-комунікаційних технологій установи повинні регулярно зберігати резервні копії своїх даних на випадок збоїв, кіберзагроз або фізичних пошкоджень. Велике питання, яке виникає в рамках права на видалення даних (право на забуття) згідно GDPR, полягає в тому, як організації мають опрацьовувати свої резервні копії, коли користувач просить видалити його дані. Пряме трактування GDPR може привести до висновку, що цю дію видалення також потрібно виконувати в резервних копіях, що може відкрити двері для потенційних зловживань даними, а також створення навмисних чи випадкових помилок. Такі проблеми можуть стати більш очевидними у фінансових установах, де записи завжди повинні відповідати принципам надійності, цілісності та прозорості інформації. Наприклад, надання фінансовим установам та їх клієнтам можливості маніпулювати цілісністю даних відповідно до їхніх потреб, може призвести до приховування транзакцій від засобів аудиту. Окрім того, залежно від

політики організації та законодавчої бази, записи даних користувачів можуть зберігатися в енергонезалежному сховищі. Тому, як тільки користувач подає запит на видалення своїх даних, необхідно виконати неавтоматизовані дії, що призводять до додаткових витрат і можливих юридичних тупиків[1].

Таким чином, деякі технічні питання не знаходять прямої відповіді у GDPR та мають покладатися на їх розв'язання юридичною практикою (зокрема й в межах національних органів). Так, наприклад, наглядовий орган Франції щодо GDPR – Commission Nationale de l'Informatique et des Libertés (CNIL) у відповіді на запит[2] щодо роз'яснення умов видалення даних, відповів, що організаціям не потрібно видаляти резервні копії для дотримання права на забуття. Тим не менш, вони повинні чітко пояснити суб'єкту даних, що резервні копії зберігатимуться протягом визначеного періоду часу, викладеного у політиці компанії. При цьому позицію CNIL не слід вважатися імперативною та остаточною, оскільки наглядові органи інших держав можуть виявитися більш суворими, зокрема вимагати обґрунтування недоцільності видалення резервних копій даних у конкретному випадку. Для цього, щонайменше, може бути затребувана оцінка ризиків, оцінка впливу на бізнес і оцінка впливу на захист даних, а також документування правил та процедури захисту даних резервного копіювання, які включатимуть інструкції щодо шифрування конфіденційної інформації та місця зберігання пристроїв резервного копіювання[3]. Це демонструє, що практична реалізація окремих положень GDPR викликає чимало практичних питань.

[1] Politou E., Alepis E., Patsakis C. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*. 2018. Vol. 4, Issue 1. Art. tyy001. https://doi.org/10.1093/cybsec/tyy001.

[2] Backup Administrators: The #1 Advice to Deal with GDPR and the Right of Erasure. *Quantum Blog*. 2018, January 26. URL: https://blog.quantum.com/2018/01/26/backup-administrators-the-1-advice-to-deal-with-gdpr-and-the-right-of-erasure/#.Wv7qy0xFwy9.

[3] Irwin L. The GDPR: How the right to be forgotten affects backups. *IT Governance Blog*. 2020, August 27. URL: https://www.itgovernance.eu/blog/en/the-gdpr-how-the-right-to-be-forgotten-affects-backups-2.

Структурно GDPR складається з одинадцяти глав. Глава I окреслює загальні положення, такі як предмет і цілі, матеріальну сферу дії, територіальну сферу дії, терміни та означення. Глава II встановлює принципи, на яких будується GDPR. Глава III присвячена правам суб'єкта даних. Глава IV встановлює регулювання для контролера і оператора даних, зокрема їх загальні обов'язки, вимоги щодо безпеки даних, процедуру оцінювання впливу на захист даних, призначення співробітника з питань захисту даних, а також прийняття кодексів поведінки та сертифікацію. Глава V встановлює особливості передавання персональних даних до третіх країн або міжнародних організацій. Глава VI присвячена впровадженню незалежних наглядових органів (зокрема їхньому статусу, завдань, компетенції, повноваженням та звітуванню). Глава VII містить положення про співпрацю, зокрема взаємодію з Європейською радою із захисту даних та співпрацю між керівним наглядовим органом (Lead Supervisory Authority) і іншими відповідними наглядовими органами. Глава VIII встановлює гарантії щодо засобів правового захисту як судового, так і несудового характеру, а також відповідальність та санкції за порушення. Глава IX встановлює положення про спеціальні ситуації опрацювання (зокрема, коли мова заходить про свободу вияву поглядів, доступ громадськості до офіційних документів, опрацювання національного ідентифікаційного номеру, опрацювання в контексті зайнятості, відступи задля досягнення цілей суспільного інтересу, цілей наукового чи історичного дослідження або статистики, обов'язки збереження таємниці, правила захисту даних церков і релігійних асоціацій). Глава X делегує Комісії повноваження для прийняття делегованих та імплементаційних актів (з приводу технічних стандартів для механізмів сертифікації та штампів і знаків захисту даних). Глава XI, що являє собою прикінцеві положення, містить статті щодо скасування Директиви 95/46/ЄС, взаємозв'язку із Директивою 2002/58/ЄС та попередньо укладеними Угодами, а також норми щодо звітів Комісії, перевірки застосування інших нормативно-правових актів Союзу щодо захисту даних та набуття чинності й застосування GDPR.

Загалом вплив GDPR можна умовно поділити на два напрямки: закріплення прав фізичних осіб та встановлення правил для бізнесу. Перший напрямок передбачає, що GDPR посилює існуючі права, надає нові права та гарантії, а також дає людям більше контролю над своїми особистими даними, зокрема через спрощення доступу особи до власних даних. Якщо підсумувати, то GDPR передбачає наступний перелік суб'єктивних прав: 1. Право бути поінформованим (про обсяг та цілі опрацювання даних, про загрозу даним, зокрема витоки, тощо); 2. Право доступу до даних; 3. Право на виправлення даних; 4. Право на видалення даних (також відоме як «право на забуття»); 5. Право на обмеження опрацювання даних; 6. Право на портативність даних; 7. Право на заперечення проти опрацювання даних; 8. Права, пов'язані з автоматизованим прийняттям рішень, включаючи профілювання.

Однак, оскільки суб'єктивне право на захист персональних даних не є абсолютним, воно може бути обмежено на підставі статті 23 GDPR та відповідних законодавчих інструментів національного рівня, якщо таке обмеження зберігає сутність фундаментальних прав і свобод та є необхідним й пропорційним заходом у демократичному суспільстві для забезпечення: національної безпеки, здійснення розслідування для виконання кримінальних покарань, виконання цивільно-правових позовів тощо. При цьому національні законодавчі інструменти також повинні відповідати ряду вимог: наприклад, прямо окреслювати цілі чи категорій опрацювання даних, обсяг введених обмежень, гарантії запобігання зловживанню чи незаконному доступу або передаванню тощо.

Другий напрямок впливу GDPR, що встановлює правила для бізнесу, відштовхується від прагнення створити рівні умови для всіх компаній, які працюють на внутрішньому ринку ЄС, а також сприяти прийняттю технологічно-нейтрального підходу та стимулювати інновації. Досягнення названих цілей, зокрема, передбачається за рахунок наступних кроків: впровадження уніфікованого набору правил для всього ЄС; вимоги до бізнесу щодо введення посади Спеціаліста із захисту даних (Data Protection Officer або DPO); спрощення обміну даними за допомогою системи «Єдиного вікна» (One Stop

Shop), що дозволяє мати справу з єдиним головним наглядовим органом (Lead Supervisory Authority) для більшості дій з опрацювання персональних даних[1]); розповсюдження правил ЄС для компаній, що не входять до ЄС; впровадження правила, що сприяють інноваціям; регулювання технічних питань, що забезпечують конфіденційність. (зокрема псевдонімізація і шифрування); вимоги щодо оцінки впливу акту на захист даних; облік діяльності з опрацювання даних; сприяння розвитку сучасного інструментарію для міжнародної передачі даних.

Закріплення принципів, яким повністю присвячено Главу II GDPR, є важливим досягненням GDPR, оскільки, окрім встановлення певних векторів розвитку, Регламент також встановлює ідеологічну основу для трактування положень щодо захисту персональних даних за наявності колізій, прогалин або інших суперечливих моментів. Перелік цих принципів наводиться у статті 5 GDPR та передбачає: (a) законність, справедливість та прозорість; (b) обмеження мети; (c) мінімізацію даних; (d) точність; (e) обмеження зберігання; (f) цілісність і конфіденційність. При цьому, хоча пункт «a» частини 1 статті 5 містить відразу декілька вимог («…опрацьовуватися законно, справедливо та прозоро щодо суб'єкта даних»), кожна з них фактично є окремим принципом зі своїм змістовним наповненням.

Реалізація цих принципів вимагає також свідомого планування та впровадження стандартів конфіденційності за замовчуванням для будь-якого збирання даних. Таке планування, серед іншого, має відбуватися ще на етапі проектування будь-якої IT-архітектури або дослідницьких чи підприємницьких проектів. Забезпечення дотримання цих принципів на практиці забезпечується з одного боку, прозорістю (через надання повної інформації особам зручним для них способом), а з іншого боку – підзвітністю. Вимога підзвітності вимагає від організацій запровадити відповідні технічні та організаційні заходи, а також бути в змозі продемонструват, що вони зроби-

[1] One Stop Shop (OSS). An Coimisiún um Chosaint Sonraí (Data Protection Commission). URL: https://www.dataprotection.ie/en/organisations/international-transfers/one-stop-shop-oss.

ли для його ефективності, коли це буде потрібно. Це також може включати використання оцінки впливу на конфіденційність для опрацювання з високим ризиком. Окрім того, GDPR також вводить обов'язковий режим сповіщення про порушення даних[1].

Важливою ознакою GDPR є екстратериторіальний характер дії GDPR, який передбачається у частині 1 статті 3, де зазначено, що цей Регламент застосовують до опрацювання персональних даних в контексті діяльності осідку контролера або оператора в Союзі, незалежно від того, чи відбувається власне опрацювання в межах Союзу чи ні.

Постачальник товарів або послуг онлайн може стати суб'єктом Регламенту ЄС у тій мірі, в якій він активно продає в певній географічній зоні, а не якщо він просто надає веб-сайт, який доступний особам у певній географічній зоні. Однак такі фактори, як використання мови чи валюти, яка зазвичай використовується в державах-членах ЄС та відповідно полегшить надання товарів і послуг європейським клієнтам, також братимуться до уваги. Наприклад, якщо компанія електронної комерції, що базується в США, не доставляє свої товари споживачам у ЄС і не забезпечує конвертацію валюти чи мовні параметри для обслуговування ринку ЄС, то, імовірно, вона не буде зобов'язана дотримуватися Регулювання. Однак для багатьох організацій ситуація не буде такою однозначною.

Для організацій, розташованих у юрисдикціях, які встановили закони про захист даних, узгоджені зі стандартами ЄС, необхідно проаналізувати місцеві закони на відповідність GDPR, щоб визначити прогалини та відповідно адаптувати існуючу політику та практику. Підприємствам також потрібно розглянути свою внутрішню здатність адекватно керувати ризиками невідповідності, із загальною тенденцією до інвестування в покращення управління інформацією. Безсумнівно, цей процес має об'єднати юридичну експертизу з операційними сферами IT, безпеки та управління даними, дозволяючи

[1] Goddard M. The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal of Market Research*. 2017. Vol. 59, Issue 6. P. 703–705. https://doi.org/10.2501/IJMR-2017-050.

своєчасно виявляти ризики та узгоджено керувати ними, гарантуючи, що організація буде попереду цього все більш складного та мінливого нормативного середовища. Звичайно, існують проблеми із застосуванням і можливі конфлікти між Регламентом і місцевими законами держав, що не є членами ЄС, які може буде непросто вирішити[1].

У першому звіті про оцінку та перегляд Загального регламенту захисту даних було відмічено, що GDPR уже став ключовим орієнтиром на міжнародному рівні та виявився каталізатором для багатьох країн у всьому світі, щоб розглянути можливість запровадження сучасних правил конфіденційності. Ця тенденція до глобальної конвергенції є дуже позитивною подією, яка дає нові можливості для кращого захисту осіб у ЄС, коли їхні дані передаються за кордон, а водночас полегшує потоки вільного руху даних[2].

Втім ставлення щодо екстратериторіального характеру GDPR з боку дослідників, юристів та різноманітних зацікавлених сторін є неоднозначним. З одного боку, це регулювання було сприйнято як новий глобальний «золотий стандарт». З іншого боку, розгляд положень GDPR у ширшому контексті історичного розвитку міжнародно-правових відносин, ставить під сумнів юридичну коректність та доцільність його розширеної дії.

Існує теза, що подібне одностороннє встановлення стандартів неминуче стикається з серйозними обмеженнями та проблемою перевантаження влади, а отже має потенціал завдати шкоди предмету регулювання в довгостроковій перспективі[3]. Особливо, коли з таким

[1] Brown A. Territorial scope and application. Simmons & Simmons. URL: https://www.simmons-simmons.com/en/features/european-data-protection-regulation/ck0zgby4r57zf0b239bit3gc4/european-data-protection-regulation-territorial-scope-and-application-test

[2] Communication from the Commission to the European Parliament and the Council Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation. COM(2020) 264 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0264&rid=5

[3] Gstrein O. J., Zwitter A. Extraterritorial Application of the GDPR: Promoting European Values or Power? *Internet Policy Review*. 2021. Vol. 10 Issue 3. DOI: 10.14763/2021.3.1576. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3940596

широким охопленням важко уявити операцію з персональними даними, яка виконується значущим учасником міжнародної сфери даних та не входить до територіальної сфери дії GDPR. У той же час ЄС вже зіткнулося з проблемами щодо налагодження вільного руху даних з іншими країнами через необхідність визнання «адекватного» рівня захисту даних. Так, до прийняття рішення про адекватність захисту даних у США від 10 липня 2023 року, передача даних до цієї країни протягом багатьох країн була вельми ускладненою. Великобританія після виходу зі складу ЄС 31 січня 2020 року й до 28 червня 2021 року також очікувала рішення Комісії щодо адекватності передачі персональних даних. Крім того, з великими проблемами стикається інтенсивне економічне співробітництво багатьох країн ЄС з КНР.

Втім, якщо оцінювати положення GDPR виключно з юридичної точки зору, без політико-дипломатичного та економічного аспекту, то таке регулювання може вважатися правомірним. Згідно з міжнародним публічним правом, щоб держава могла стверджувати наказову або судову юрисдикцію над чимось, має існувати «достатній зв'язок» суб'єкта з об'єктом регулювання. Як правило, до загальних принципів, на яких може ґрунтуватися претензія щодо юрисдикції, включають п'ять положень: 1) принцип територіальності (об'єктивний і суб'єктивний); 2) принцип громадянства (активний чи пасивний); 3) принцип ефектів; 4) захисний принцип; 5) принцип універсальності[1]. Й, хоча принцип територіальності, що дозволяє державам реалізовувати владу на своїх території, є основним, він не є єдиним, а держави все частіше беруться за регулювання поведінки за кордоном, використовуючи для цього різноманітні виправдання.

У будь-якому разі на сьогодні Україні слід продовжувати адаптацію законодавчих положень до вимог GDPR, однак юристи, дослідники та політики мають обережно відстежувати та аналізувати розповсюдження європейських стандартів захисту даних у світі та ті перешкоди й опір, з якими це стикається. Зокрема, увага повинна

[1] Van Alsenoy B. Reconciling the (extra)territorial reach of the GDPR with public international law. Maklu, 2017. ISSN: 978-90-466-0910-1. URL: https://lirias.kuleuven.be/1711958?limo=0

бути приділена ризику поляризації світу, за якого ми можемо мати декілька неузгоджених глобальних актів щодо захисту даних (наприклад, європейський та китайський). За умов, коли держава постає перед вибором «повністю прийняти» або «повністю відхилити» стандарти GDPR, такий ризик лише підвищується, на відміну від міжнародних договорів, які можна адаптувати (зокрема прийняти з застереженням).

## 3.2. Окремі положення захисту персональних даних

Для побудови цифрового суспільства потрібно розвивати правові норми та регулятори, спрямовані на захист приватності та контроль над персональними даними. Крім того, актуалізується необхідність забезпечення ефективного та надійного захисту персональних даних в умовах швидкого розвитку технологій, глобалізації та зростаючої загрози кіберзлочинності. Необхідність розвитку правових норм, впровадження інноваційних технологій та підвищення громадської свідомості стають важливими завданнями для забезпечення приватності та захисту персональних даних. Дослідження також спрямовано на виявлення та аналіз основних викликів, з якими стикається сфера захисту персональних даних, таких як кіберзлочинність, хакерські атаки, глобалізація та перетин кордонів. Аналізуються також правові норми та регулятори, спрямовані на захист приватності, а також потенційні можливості нових технологій, які можуть підвищити рівень захисту персональних даних.

Проблеми правового захисту персональних даних останнім часом стають предметом дослідження все більшої кількості науковців, при чому як правників, так і представників інших галузей знань. Зокрема, дослідженню цих питань присвячують свою увагу такі вчені, як: С. В. Глібко, Т. П. Єгорова-Луценко, К. В. Єфремова, О. В. Корват, В. П. Кохан, М. Г. Хаустова та інші.

Для вироблення можливих шляхів нормативно-правового захисту персональних даних з огляду на виклики сьогодення, пов'язані з цією проблематикою, необхідно розглянути розвиток технологій та зростання обсягу персональних даних як основних чинників, що впливають на необхідність ефективного захисту приватності та безпеки цих даних, розширити розуміння проблеми та надати рекомендації для покращення захисту приватності та безпеки персональних даних у майбутньому[1].

23 лютого 2023 року було ратифіковано Угоду між Україною та Європейським Союзом про участь України у програмі Європейського Союзу «Цифрова Європа» (2021-2027), учинену 5 вересня 2022 року. Зокрема, згідно із преамбулою до цієї Угоди визнається важлива допоміжна роль цифрової інфраструктури у таких сферах, як високопродуктивний комп'ютинг, штучний інтелект, хмарні обчислення та масиви даних, а також кібербезпека, для забезпечення нерозривно пов'язаних процесів трансформації та цифрового лідерства Європейського Союзу. Крім того, укладання Угоди має на меті налагодження взаємовигідного співробітництва з метою зміцнення та підтримки розгортання надійних і безпечних цифрових можливостей у Союзі в сфері високопродуктивного комп'ютингу; штучного інтелекту, кібербезпеки; передових цифрових навичок; та розгортання й оптимального використання цифрових потужностей та інтероперабельності, а також сприяння впровадженню та доступності цифрових рішень зі сторонами. Також визнається, що взаємна участь у програмах один одного з впровадження цифрових технологій має забезпечувати взаємні вигоди для Сторін з дотриманням високого рівня захисту даних, цифрових прав, основоположних прав і етичних стандартів, та визнаючи, що Сторони залишають за собою право обмежувати або обумовлювати участь у певних діях на підставі належним чином виправданих міркувань безпеки[2].

[1] Глібко С. В., Мамаєв І. О. Огляд та порівняльна характеристика сервісів, що сприяють інформаційному забезпеченню інноваційної діяльності. *Право та інновації.* 2023. № 2 (42). С. 46–54. URL: https://doi.org/10.37772/2518-1718-2023-2(42)-6.

[2] Угода між Україною та Європейським Союзом про участь України у програмі Європейського Союзу «Цифрова Європа» (2021-2027) від 05.09.2022 р. : ратифікова-

Так, відповідно до пункту 12 статті 2 додатку III до Угоди, обмін інформацією між Європейською комісією або OLAF та компетентними державними органами України має відбуватись із належним урахуванням вимог щодо конфіденційності. Персональні дані, включені до обміну інформацією, мають передаватись відповідно до чинних правових норм щодо захисту даних тієї Сторони, яка здійснює передачу[1]. Отже, згідно із цією нормою передбачається, що обмін інформацією, яка містить персональні дані, має відбуватися згідно із чинними національними нормативно-правовими вимогами щодо захисту (персональних) даних.

У зв'язку з цим варто зазначити, що, скажімо, відповідно до статті 32 Конституції України ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України, а також не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної без пеки, економічного добробуту та прав людини[2]. Тим самим ще у 1996 році в Україні на конституційному рівні було закладено основу для захисту персональних даних, яка на сьогодні звісно ж проектується у тому числі й на захист цифрових прав, пов'язаних з обігом персональних даних.

Що ж стосується Регламенту (ЄС) 2021/694 Європейського Парламенту та Ради від 29 квітня 2021 року про створення Програми цифрової Європи, то згідно із пунктом 49 преамбули цього Регламенту цифрова трансформація повинна дозволити громадянам мати доступ до своїх персональних даних, використовувати та безпечно керувати ними через кордони, незалежно від їхнього місцезнаходження чи місцезнаходження даних. Крім цього, відповідно до пункту 60 преамбули забезпечуючи єдиний набір правил, які безпосередньо

но Законом України від 23.02.2023 р. № 2926-IX. URL: https://zakon.rada.gov.ua/laws/show/984_005-22#Text.

[1] Там само.

[2] Конституція України від 28.06.1996 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

застосовуються у правових системах держав-членів, Регламент (ЄС) 2016/679 гарантує вільний потік персональних даних між державами-членами та зміцнює довіру та безпеку осіб, два незамінні елементи справжнього Єдиного Цифрового Ринку. Тому всі дії, вжиті в рамках Програми, які передбачають обробку персональних даних, повинні сприяти безперебійному виконанню цього Регламенту, наприклад, у сфері штучного інтелекту та технологій розподіленого реєстру (наприклад, блокчейн). Ці дії мають підтримувати розвиток цифрових технологій, які відповідають зобов'язанням щодо захисту даних як за задумом, так і за замовчуванням. До того ж, згідно із пунктом 69 преамбули цей Регламент поважає основні права та дотримується принципів, визнаних у Хартії основоположних прав Європейського Союзу, зокрема щодо захисту персональних даних та ін. Держави-члени повинні застосовувати цей Регламент відповідно до цих прав і принципів[1]. Отже, вказані положення преамбули до Регламенту (ЄС) 2021/694 щодо використання, керування та доступу до персональних даних, їх вільного потоку між державами, а також обробки, захисту тощо, відображають керівні ідеї, принципи, те, з метою чого поряд з іншим було розроблено та затверджено цей Регламент.

У свою чергу, у Хартії основоположних прав Європейського Союзу (2016/C 202/02) від 7 червня 2016 року у розділі II «Свободи» міститься стаття 8, яка має назву «Захист персональних даних», згідно із якою передбачається, що кожен має право на захист персональних даних, які його стосуються. При цьому такі дані повинні оброблятися справедливо для певних цілей і на основі згоди відповідної особи або на іншій легальній основі, встановленій законом. Кожен має право на доступ до даних, які були зібрані стосовно нього, і право на їх виправлення. Дотримання цих правил підлягає контролю з боку незалежного органу[2]. Ось ті права та принципи, які дотриму-

[1] Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (Text with EEA relevance). URL: https://eur-lex.europa. eu/legal-content/EN/ALL/?uri=CELEX%3A32021R0694.

[2] Charter of Fundamental Rights of the European Union (2016/C 202/02). URL: https://eur-lex.europa.eu/legal-content/ EN/TXT/?uri=CELEX:12016P/TXT.

ються в Регламенті (ЄС) 2021/694, зокрема, щодо захисту персональних даних. Відтак, враховуючи ратифікацію Угоди між Україною та Європейським Союзом про участь України у програмі Європейського Союзу «Цифрова Європа» (2021-2027), вони є актуальними і для України.

Крім того, є окремий Регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних і про вільний рух таких даних, який встановлює правила, що стосуються захисту фізичних осіб щодо обробки персональних даних, а також правила, що стосуються вільного руху персональних даних, та захищає основоположні права і свободи фізичних осіб і, зокрема, їх право на захист персональних даних[1]. Авжеж положення цього Регламенту мають бути орієнтиром при розробленні українського законодавства, зокрема при виробленні норм, якими мають встановлюватися правила поведінки у сфері обігу та захисту персональних даних. На сьогодні в Україні основним законодавчим актом у цій сфері є Закон від 1 червня 2010 року № 2997-VI «Про захист персональних даних», який регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних. Цей Закон поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містять ся у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів [12].

При цьому у статті 11 Закону України «Про інформацію» зазначається, що інформація про фізичну особу (персональні дані) – це відомості чи сукупність відомостей про фізичну особу, яка ідентифі-

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

кована або може бути конкретно ідентифікована. Так, до конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження. Кожному забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законом. При цьому не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. Зокрема, центральний орган виконавчої влади, що забезпечує формування та реалізує державну фінансову та бюджетну політику, під час здійснення повноважень щодо верифікації та моніторингу державних виплат не потребує згоди фізичних осіб на отримання та обробку персональних даних[1].

У свою чергу, правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки визначено у Законі України «Про основні засади забезпечення кібербезпеки України» [15]. До того ж відносини у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах регулюються Законом України «Про захист інформації в інформаційно-комунікаційних системах»[2].

Однак, однією з ключових проблем нормативно-правового регулювання суспільних відносин, пов'язаних із обігом персональних даних є той факт, що технології часто випереджають право. Законо-

[1] Про інформацію : Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

[2] Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text.

давець повинен постійно змінювати і адаптувати законодавство, щоб відповідати новим викликам, з якими стикається суспільство. Навіть за наявності ефективного законодавства, реальний захист персональних даних залежить від багатьох факторів, таких як підвищення обізнаності громадян, відповідальність компаній та ефективність правоохоронних органів.

Так, В. П. Кохан та Т. П. Єгорова-Луценко слушно звертають увагу на те, що розвиток електронних сервісів вимагає особливої уваги до інформаційної безпеки, що передбачає захист від несанкціонованого використання та доступу до персональних даних. У зв'язку з цим, в якості однієї зі складових електронного урядування вчені цілком логічно пропонують розроблення спеціалізованого нормативно-правового акту, спрямованого на захист громадян від несанкціонованого використання та несанкціонованого доступу до їх персональних даних, визначивши у ньому єдині правила такого використання та доступу, забезпечивши конфіденційність та контроль за цілісністю інформації, підвищення і зміцнення інформаційної безпеки сучасного суспільства[1].

Погоджуючись із цією пропозицією, варто зазначити, що такий акт має бути розроблений та затверджений скажімо Міністерством цифрової трансформації України, як органом який забезпечує формування та реалізацію державної політики у сферах цифровізації, цифрового розвитку, електронного урядування та електронної демократії, розвитку інформаційного суспільства, впровадження електронного документообігу, розвитку цифрових навичок та цифрових прав громадян, відкритих даних, публічних електронних реєстрів, розвитку національних електронних інформаційних ресурсів та інтероперабельності, надання електронних та адміністративних послуг, електронних довірчих послуг та електронної ідентифікації тощо[2].

[1] Кохан В. П., Єгорова-Луценко Т. П. Умови розвитку електронних послуг в Україні. *Право та інновації.* 2019. № 2 (26). С. 37. URL: https://pti.org.ua/index.php/ndipzir/article/view/531/475.

[2] Положення про Міністерство цифрової трансформації України : затв. постановою Кабінету Міністрів України від 18.09.2019 р. № 856. URL: https://zakon.rada.gov.ua/laws/show/856-2019-п#Text.

Зокрема, захист персональних даних варто віднести до цифрових прав людини і громадянина (суб'єктів персональних даних). Доцільно закріпити норму, в якій би містився перелік таких цифрових прав, із кореспондуванням їм, на скільки це можливо, обов'язків уповноваженого органу (уповноважених органів) щодо їх забезпечення та захисту. Відтак, на нормативному рівні має бути визначено перелік та механізм(и) набуття цифрових прав, їх реалізації, захисту, компенсації та відповідальності за їх порушення. Адже належне існування у цифровому суспільстві, у цифровому просторі передбачає не лише оцифрування персональних даних, але ще й їх подальше законне використання, що у тому числі передбачає визначення та захист цифрових прав суб'єктів цих персональних даних.

Так, характеризуючи цифрові платформи як інструмент цифрової економіки, В. П. Кохан, наводячи приклади комерційних цифрових платформ, таких як Amazon, eBay, Uber, Google, AliExpress, Facebook та інші, слушно зазначає, що функціонування цифрових платформ призвело до появи низки правових проблем, що потребують вирішення, однією із яких є збереження конфіденційних та персональних даних, недопущення їх витоку при збиранні інформації за допомогою технологій великих даних. Вирішення, у тому числі цієї проблеми, вчена цілком обґрунтовано бачить у формуванні законодавства про цифрові платформи, встановленні ключових принципів правового регулювання їх діяльності, які потім мають знайти своє відображення у корпоративних нормативних актах операторів платформ[1].

Дійсно, надаючи свої персональні дані при реєстрації на відповідних електронних платформах та під час подальшого користування ними, користувачі (фізичні та юридичні особи) не завжди чітко розуміють правовий режим подальшого зберігання та використання таких даних. У зв'язку з цим, важливо щоб нормативно-правове та нормативно-корпоративне регулювання цього питання відбувалося у режимі взаємозалежності, при цьому забезпечуючи правовий та

[1] Кохан В. П. Цифрова платформа як інструмент цифрової економіки. *Право та інновації.* 2021. № 1 (33). С. 31. URL: https://doi.org/10.37772/2518-1718-2021-1(33)-4.

технічний захист персональних даних користувачів, навіть за обставин, коли ці дані надаються користувачами самостійно і добровільно. Адже треба враховувати, що із достатньо швидким розвитком процесів цифровізації користувачі цифрових послуг, у тому числі цифрових платформ, не завжди можуть вчасно та чітко розуміти можливі наслідки надання своїх персональних даних, а тому вони потребують як визначення та закріплення, так і захисту своїх цифрових прав.

При цьому треба враховувати ще два аспекти функціонування цифрових платформ, на які звертає увагу О. В. Розгон. Так, характеризуючи цифрову платформу вчена зазначає, що це бізнес-модель зі складною системою інформаційних технологій, яка надає можливість користуватися не тільки функціями самої платформи, а й додатковими продуктами, технологіями, послугами, додатками, що створені незалежними третіми сторонами[1]. Тобто з технічної точки зору процес користування цифровими платформами на стільки складний, що доступ до персональних даних може мати необмежена кількість третіх сторін. Це відповідно ускладнює і механізм захисту самих персональних даних, при чому як з технічної, так і з правової сторони.

Крім цього, не менш важливим є й те, що «традиційний» бізнес тактично дуже виграє від появи цифрових платформ, але у стратегічному плані наражається на небезпеку втрати каналів збуту і потрапляння в цілковиту залежність від власників платформ[2]. Відтак захист персональних даних переходить у площину захисту цифрової конкуренції, коли володіння або контроль над популярною цифровою платформою – маркетплейсом надає можливість диктувати свої умови та впливати на конкурентоздатність учасників цифрового ринку. Все це свідчить про виключну важливість захисту даних, зокрема цифрових комерційних даних, які використовуються під час функціонування e-commerce.

[1] Розгон О. В. Цифрова платформа як інструмент функціонування мережі трансферу технологій. *Право та інновації.* 2023. № 2 (42). С. 23, 24. URL: https://doi.org/10.37772/2518-1718-2023-2(42)-3.

[2] Розгон О. В. Цифрова платформа як інструмент функціонування мережі трансферу технологій. *Право та інновації.* 2023. № 2 (42). С. 24. URL: https://doi.org/10.37772/2518-1718-2023-2(42)-3.

У зв'язку з цим варто зазначити, що провідні маркетплейси ознайомлюють користувачів з політиками інтелектуальної власності, які розміщуються на веб-сайтах компаній, а також пропонують різноманітні програми для боротьби проти порушень прав інтелектуальної власності[1]. Тобто захист цифрових прав інтелектуальної власності є хоча і похідним але обов'язковим елементом нормативно-правового регулювання діяльності маркетплейсів. При цьому вже на сьогодні захистом таких прав опікуються самі власники інтернет майданчиків, адже захист прав інтелектуальної власності як такої охоплює у тому числі і захист об'єктів інтелектуальної вартості виражених у цифровому вигляді. Можливо у чомусь це спричинюється достатньо розробленими технічними механізмами виявлення таких порушень, а також активною судовою практикою стягнення з порушників досить великих сум компенсацій за порушення прав інтелектуальної власності у цифровій сфері. Тож, захист цифрових персональних даних (які до речі теж можуть виступати об'єктом права інтелектуальної власності, напр., зібрана легальними способами якоюсь компанією база персональних даних клієнтів та ін.) також потребує вироблення належного як технічного, так і нормативно-правового інструментарію, а також судової практики притягнення до відповідальності за порушення порядку їх використання.

Поряд із цим окрему нішу електронних послуг займають legal tech, перетворюючи надання юридичних послуг на надання цифрових юридичних послуг. Так, С. В. Глібко та І. О. Мамаєв дуже влучно звертають увагу на те, що утворення відповідних онлайн-сервісів адвокатськими фірмами є очікуваною та позитивною тенденцією, зокрема створення повноцінних інформаційно-комунікаційних платформ значно спрощує процес звернення та комунікації клієнта з адвокатом[2]. При цьому треба враховувати, що надання таких послуг

[1] Шматков Д. І. Фан-арт та право інтелектуальної власності на платформах електронної комерції. *Право та інновації*. 2023. № 2 (42). С. 82. URL: https://doi.org/10.37772/2518-1718-2023-2(42)-10.

[2] Глібко С. В., Мамаєв І. О. Огляд та порівняльна характеристика сервісів, що сприяють інформаційному забезпеченню інноваційної діяльності. *Право та інновації.* 2023. № 2 (42). С. 48. URL: https://doi. org/10.37772/2518-1718-2023-2(42)-6.

також ставить під загрозу захист персональних даних клієнтів, адже отримання цих даних з одного боку необхідне для надання послуг, а з іншого – ці дані опиняються у відповідній цифровій базі, а отже потребують захисту. Відтак, цифровим правам клієнтів мають відповідати цифрові обов'язки надавачів юридичних послуг, зокрема щодо збереження цифрової адвокатської таємниці.

Ще одним проявом використання наданих персональних даних є функціонування електронного урядування. Так, згідно із Концепцією розвитку електронного урядування в Україні електронне урядування – це форма організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян[1]. Майже повністю наведене визначення дублюється у пункті 7 частини 1 статті 1 Закону України «Про Національну програму інформатизації», згідно із яким електронне урядування – це форма організації державного управління, що сприяє підвищенню ефективності, відкритості та прозорості діяльності державних органів та органів місцевого самоврядування з використанням інформаційно-комунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян[2].

При цьому варто відмітити той позитивний момент, що одним із основних принципів за якими здійснюється реалізація Концепції є використання органами влади інформації, поданої до них фізичними та юридичними особами, для надання публічних послуг та надання інших владних повноважень з дотриманням вимог захисту інформації та персональних даних. До того ж одним із завдань забезпечення розвитку електронного урядування в Україні є надійний захист пер-

[1] Концепція розвитку електронного урядування в Україні : схвал. розпорядженням Кабінету Міністрів України від 20 вересня 2017 р. № 649-р. URL: https://zakon.rada.gov.ua/laws/show/649-2017-р#Text.

[2] Про Національну програму інформатизації : Закон України від 01.12.2022 р. № 2807-IX. URL: https://zakon. rada.gov.ua/laws/show/2807-20#Text.

сональних даних та прав на приватність особи з метою зміцнення довіри до онлайн середовища[1].

Нормативно-правове закріплення цих положень звичайно ж є схвальним, однак не достатньо лише прийняти певну норму права, яка б закріплювала принцип захисту персональних даних, зокрема у сфері функціонування електронного урядування, необхідним є ще й розроблення та затвердження інших положень, які б визначали конкретний та дієвий механізм такого захисту. Так, скажімо можливим є створення бази або реєстру електронних/цифрових платформ, за допомогою якої або якого відбувався би контроль за їх діяльністю, у тому числі щодо захисту персональних даних.

У зв'язку з цим варто зазначити, що у 2021 році було прийнято Закон України «Про публічні електронні реєстри», згідно із пункту 2 частини 1 статті 2 якого Державна електронна платформа ведення публічних електронних реєстрів, – це інформаційно-комунікаційна система, призначена для уніфікованого, автоматизованого та стандартизованого процесу створення, адміністрування та ведення публічних електронних реєстрів з використанням загальних принципів проектування, програмування та захисту інформації в публічних електронних реєстрах[2]. У свою чергу, 18 квітня 2023 року постановою Кабінету Міністрів України було затверджено Положення про інформаційну систему «Програмна платформа для розгортання та супроводження державних електронних реєстрів», а також Порядок використання програмного забезпечення «Програмна платформа для розгортання та супроводження державних електронних реєстрів»[3] [4].

---

[1] Концепція розвитку електронного урядування в Україні : схвал. розпорядженням Кабінету Міністрів України від 20 вересня 2017 р. № 649-р. URL: https://zakon.rada.gov.ua/laws/show/649-2017-р#Text.

[2] Про публічні електронні реєстри : Закон України від 18.11.2021 р. № 1907-IX. URL: https://zakon.rada.gov.ua/ laws/show/1907-20#Text.

[3] Положення про інформаційну систему «Програмна платформа для розгортання та супроводження державних електронних реєстрів» : затв. постановою Кабінету Міністрів України від 18.04.2023 р. № 356. URL: https:// zakon.rada.gov.ua/laws/show/356-2023-п#Text.

[4] Порядок використання програмного забезпечення «Програмна платформа для розгортання та супроводження державних електронних реєстрів» : затв. поста-

Так, Положення визначає механізм функціонування інформаційної системи, а також процедуру та вимоги щодо створення або замовлення на створення, адміністрування та ведення публічних електронних реєстрів, інформаційно-комунікаційних систем шляхом використання програмних засобів зазначеної інформаційної системи у разі прийняття такого рішення їх держателем (власником). Згідно із пунктом 4 Положення власником інформаційної системи є держава, а технічним адміністратором – державне підприємство «Українські спеціальні системи», що належить до сфери управління Адміністрації Держспецзв'язку[1]. У свою чергу, Порядок визначає механізм використання програмного забезпечення інформаційної системи органами державної влади, державними підприємствами, установами, організаціями для створення, адміністрування та ведення публічних електронних реєстрів та інформаційно-комунікаційних систем[2].

На підставі цього можна запропонувати створення такої бази/ реєстру й для приватних електронних/ цифрових платформ. При цьому на нормативно-правовому рівні варто передбачити, що обов'язковою умовою створення та функціонування платформи є її реєстрація у такій базі / такому реєстрі, а обов'язковою умовою реєстрації – є підтвердження технічних можливостей щодо забезпечення захисту персональних даних користувачів платформи. Адже, як відбувається ліцензування та реєстрація банків, як юридичних осіб, які на підставі банківської ліцензії мають виключне право надавати банківські послуги, так має відбуватися і ліцензування та реєстрація електронних/цифрових платформ, які по суті є «банками» електронних/цифрових даних.

новою Кабінету Міністрів України від 18.04.2023 р. № 356. URL: https://zakon.rada.gov.ua/laws/show/356-2023-п#Text.

[1] Положення про інформаційну систему «Програмна платформа для розгортання та супроводження державних електронних реєстрів» : затв. постановою Кабінету Міністрів України від 18.04.2023 р. № 356. URL: https:// zakon.rada.gov.ua/laws/show/356-2023-п#Text.

[2] Порядок використання програмного забезпечення «Програмна платформа для розгортання та супроводження державних електронних реєстрів» : затв. постановою Кабінету Міністрів України від 18.04.2023 р. № 356. URL: https://zakon.rada.gov.ua/laws/show/356-2023-п#Text.

У зв'язку з цим варто погодитися із О. В. Корват стосовно того, що уряд має нести відповідальність за безпеку та контроль над даними і послугами в цифровій екосистемі, а законодавство і нормативно-правові акти стосовно інформатизації та цифровізації урядування, економіки та суспільства в Україні потребують оновлення з урахуванням пріоритетних цілей розвитку людини, необхідності підвищення рівня кібербезпеки та захисту даних[1]. При цьому варто додати, що цифрова екосистема, за безпеку та контроль над даними в якій має нестися відповідальність, повинна включати в себе не тільки електронне урядування, а й загалом всі цифрові платформи, які бажають легально діяти у цифровому просторі України. І знову ж таки все це неможливо без належного нормативно-правового регулювання та підґрунтя, яке має враховувати технічні вимоги до захисту та забезпечувати захист у тому числі персональних даних.

Так само заслуговує на погодження точка зору М. Г. Хаустової відносно того, що в умовах правової держави та розвитку інформаційного суспільства мають бути законодавчо визначені обмеження довільного поводження з правами людини, зокрема в інформаційній сфері. Вчена цілком вірно звертає увагу на те, що цифрова трансформація суспільних відносин привела до формування інститутів цифрового права, а технологічні платформи на принципах розподіленого реєстру, штучний інтелект, хмарні сервіси тощо створило нові умови для адаптації традиційних правових інститутів до нових реалій технологічного існування людства – цифрової екосисте ми. Крім того, науковиця слушно підкреслює, що активне використання цифрових технологій в різних сферах життєдіяльності зумовило постановку питання про необхідність та достатність прав і свобод людини і громадянина, та виокремило поняття циф рові права і свободи людини[2].

[1] Корват О. В. Розвиток електронного урядування до цифрової екосистеми. *Право та інновації.* 2023. № 2 (42). С. 43. URL: https://doi.org/10.37772/2518-1718-2023-2(42)-5.

[2] Хаустова М. Г. Права людини в інфомаційному суспільстві в умовах глобалізаційних процесів. *Право та інновації.* 2021. № 3 (35). С. 95–96. URL: https://doi.org/10.37772/2518-1718-2021-3(35)-13.

Так, дійсно розвиток цифровізації у правовій державі неминуче має супроводжуватися розвитком правової бази, зокрема появою, закріпленням, визначенням та захистом цифрових прав фізичних та юридичних осіб. При цьому такі права мають стосуватися як свободи доступу до цифрової інформації, так і захисту своїх персональних даних, які стають доступними іншим користувачам під час або в результаті доступу до цифрової інформації, користування відповідними цифровими платформами, базами (банками) даних. Правовий захист має бути направлений як на етап передачі персональних даних, так і на етапи їх подальшого зберігання та використання. Відтак, цілком природною має бути поява окремого елементу у загальній системі права, такого як – цифрове право, як сукупності правових норм, що регулюють суспільні відносини пов'язані із обігом, у тому числі персональних, даних у цифрових мережах.

Поряд із захистом персональних даних, не менш важливим та в чомусь похідним від цього є захист фінансових даних, зокрема із застосуванням FinTech. Так, К. В. Єфремова доречно зазначає, що розповсюдження фінансових технологій тягне за собою збір і обробку значної кількості персональних і фінансових даних, неналежний захист або порушення яких можуть призвести до крадіжки особистих даних, фінансового шахрайства та порушення конфіденційності. У зв'язку з цим вчена дає цілком корисний посил, що захист персональних даних і впровадження ефективних правил захисту даних є обов'язковими для забезпечення фінансової безпеки в епоху фінансових технологій[1].

Отже, варто зазначити, що в епоху цифровізації та розвитку цифрових технологій, проникнення та використання останніх у різних сферах суспільного життя цифрові права стають багатогранною категорією. Зокрема, вони стають пов'язаними та переплітаються з іншими правами, визначеними та закріпленими у нормах різних галузях права. Зокрема, захист цифрових прав стосується не тільки персональних, а й фінансових даних, що у свою чергу є умовою забезпечен-

[1] Єфремова К. В. Технології цифрової економіки та фінансова безпека. *Право та інновації.* 2023. № 2 (42). С. 9. URL: https://doi.org/10.37772/2518-1718-2023-2(42)-1.

ня фінансової безпеки. До того ж, багатогранність категорії «цифрові права» передбачає виокремлення та розмежування різних категорій цифрових прав, їх розподіл на відповідні види, скажімо «особисті цифрові права», «фінансові цифрові права» та інше.

Жити в сучасному світі часто означає, що повна анонімність майже неможлива. Однак, заборона на зберігання, обробку і використання персональних даних без згоди особи, до якої вони відносяться, є як цілком можливою, так і вкрай необхідною. З огляду на це, надзвичайно важливо зосередити увагу на правовому регулюванні цієї проблеми.

Це законодавство потребує оновлення з огляду на Угоду про асоціацію між Україною та ЄС, що має на меті узгодити законодавство про захист даних із підходами ЄС, а також із зобов'язаннями згідно з Конвенцією 108. Державна політика щодо цифровізації суттєво інтегрувала реформу у сфері захисту даних та підвищила роль Офісу Омбудсмана в цьому процесі, наділивши його повноваженнями здійснювати контроль за дотриманням законодавства у цій сфері.

Завдяки швидкому розвитку технологій, індивіди повинні бути особливо уважними щодо викликів, які ставить перед ними неналежне використання та зберігання персональних даних. Підходи до захисту даних, які використовуються бізнесом та урядами, можуть бути недостатніми для захисту особистої інформації від неправомірного використання. Крім того, важливо враховувати, що правові норми, що регулюють використання персональних даних, можуть бути складними та недостатніми. Прозорість щодо використання персональних даних, повага до права на приватність та адекватне регулювання є ключовими елементами для захисту персональних даних.

Аналізуючи специфіку права на захист персональних даних, стає очевидним, що його значення не обмежується простим врахуванням приватності або виключно окремих індивідуальних інтересів. Захист персональних даних вимагає спільних зусиль та співпраці між урядовими органами, приватним сектором та громадським суспільством. Розвиток міжнародних стандартів і правових норм, спрямованих на

захист персональних даних, є важливим кроком для створення єдиного набору принципів та стандартів. Ми стикаємося з новими, невідомими до цього викликами, які не можна просто вирішити, розширивши старі норми і методи. Таким чином, нам потрібно розробляти та впроваджувати нові правові структури, а також приєднуватися до формування нових універсальних стандартів інформаційних прав людини. Проте, враховуючи сучасні світові тренди нестримного збирання та використання особистої інформації, посилюється ризик для права на захист персональних даних, яке, не встигнувши належним чином впорядкуватися на глобальному рівні, може зникнути. Таким чином, важливим завданням є виявлення компромісних варіантів правового регулювання, які б з одного боку, врахували всі вищезгадані аспекти, а з іншого – були у відповідності із законами розвитку суспільства, економіки та технологій.

Враховуючи ратифікацію Угоди між Україною та Європейським Союзом про участь України у програмі Європейського Союзу «Цифрова Європа» (2021-2027), права та принципи, які поважаються та дотримуються Регламентом (ЄС) 2021/694 Європейського Парламенту та Ради від 29 квітня 2021 року про створення Програми цифрової Європи, зокрема щодо захисту персональних даних є актуальними і для України. При цьому положення Регламенту (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних і про вільний рух таких даних мають бути орієнтиром при розробленні вітчизняного законодавства, зокрема при регулюванні обігу та захисту персональних даних.

Доцільно закріпити норму, в якій би містився перелік цифрових прав, а також норму, в якій би містився перелік повноважень відповідних органів щодо забезпечення захисту таких цифрових прав. Цифровим правам клієнтів мають відповідати цифрові обов'язки надавачів юридичних послуг, зокрема щодо збереження цифрової адвокатської таємниці. Нормативно-правове та нормативно-корпоративне регулювання обігу персональних даних, які надаються при реєстрації на відповідних інтернет платформах та під час подальшо-

го користування ними, має відбуватися у режимі взаємозалежності, при цьому забезпечуючи правовий та технічний захист персональних даних користувачів, навіть за обставин, коли ці дані надаються користувачами самостійно і добровільно.

Захист цифрових персональних даних потребує вироблення належного як технічного, так і нормативно-правового інструментарію, а також судової практики притягнення до відповідальності за порушення порядку їх використання. Можливим є створення бази або реєстру для приватних електронних/цифрових платформ, за допомогою якої або якого відбувався би контроль за їх діяльністю, у тому числі щодо захисту персональних даних. При цьому на нормативно-правовому рівні варто передбачити, що обов'язковою умовою створення та функціонування інтернет платформи є її реєстрація у такій базі / такому реєстрі, а обов'язковою умовою реєстрації – є підтвердження технічних можливостей щодо забезпечення захисту персональних даних користувачів платформи.

Необхідним є визначення на нормативному рівні переліку та механізмів набуття цифрових прав, їх реалізації, захисту, компенсації та відповідальності за їх порушення. Захист персональних даних варто віднести до цифрових прав людини і громадянина. Розвиток цифровізації у правовій державі неминуче має супроводжуватися розвитком правової бази, зокрема появою, закріпленням, визначенням та захистом цифрових прав фізичних та юридичних осіб. Цифрові права є багатогранною категорією, вони стають пов'язаними та переплітаються з іншими правами, визначеними та закріпленими у нормах різних галузях права. Багатогранність категорії «цифрові права» передбачає виокремлення та розмежування різних категорій цифрових прав, їх розподіл на відповідні види, зокрема «особисті цифрові права», «фінансові цифрові права» тощо. Цілком природнім має бути формування окремого елементу у загальній системі права, такого як – цифрове право, як сукупності правових норм, що регулюють суспільні відносини пов'язані з обігом (у тому числі персональних) даних у цифрових мережах.

# 4. УЗАГАЛЬНЕННЯ ЄВРОПЕЙСЬКОГО ДОСВІДУ ЩОДО ВІЛЬНОГО РУХУ ТА ЗАХИСТУ ДАНИХ В ЦИФРОВІЙ СФЕРІ

## 4.1. Актуальні питання опрацювання та вільного руху даних у цифрових інфраструктурах: досвід Німеччини

Одна з попередніх робіт автора була присвячена питанням опрацювання та вільного руху даних, зокрема, в ній приділялася увага досвіду Німеччини[1] та її прогресивним змінам у антимонопольному законодавстві. Було відзначено, що у сучасному світі розвиток цифрових ринків все більш активізує появу бізнес-моделей, заснованих на даних, що вносить свої корективи до усталеного сприйняття персональних даних та їх опрацювання. У зв'язку з цим, німецький законодавець констатував встановлення все тіснішого зв'язку між сферою захисту даних та антимонопольним законодавством. У наші дні стає все більш очевидно, що агрегування великих масивів даних та їх концентрація в руках Інтернет-гігантів перешкоджає виходу нових підприємств (особливо МСП) на цифрові ринки. Фактично це порушує фундаментальні питання інституційного впровадження державного нагляду та є однією з найбільш нагальних проблем нашого часу.

[1] Мамаєв І. О. Розділ 4: Актуальні питання обробки та обігу даних у цифрових інфраструктурах: досвід Німеччини. Базові аспекти цифровізації та їх правове забезпечення : монографія / за ред. К. В. Єфремової. Харків: НДІ прав. забезп. інновац. розвитку НАПрН України, 2021. 180 с. URL: https://ndipzir.org.ua/archives/7511.

Десята поправка до німецького Акту проти обмеження конкуренції (Gesetz gegen Wettbewerbsbeschränkungen або GWB) однією з перших внесла у сферу законодавчого регулювання проблему влади, пов'язаної з агрегованими даними. Так, нова редакція GWB розширила повноваження антимонопольних органів за допомогою впровадження концепції «превентивного підходу». Відтак Федеральне антимонопольне бюро ФРН почало вважати критерій «стратегічного позиціонування компанії» предметом особливо антимонопольного нагляду. Під наглядом опинилися й «майбутні очікування» від компанії задля того, щоб держава мала можливість оперативно протидіяти будь-якій майбутній експлуатації економічної потужності на динамічних ринках або ринках, що нещодавно формуються.

Разом з тим, незважаючи на всі переваги та внесок GWB, він мав й деякі концептуальні недоліки. Перш за все, врегулювання окремих питань захисту та опрацювання даних за допомогою національного законодавства не може повністю розв'язати проблему, що пов'язана з транскордонними бізнес-моделями, а у довгостроковій перспективі призводить до фрагментації регулювання, необхідності пристосовуватися до вимог кожної країни, й, як наслідок, локалізація даних на певній території. Окрім того, проблемним моментом GWB було слабке розмежування таких юридичних термінів як «персональні», «неперсональні», «агреговані» та «змішані» дані. Нарешті, потенційною проблемою та значним ризиком стало надмірне підвищення повноважень виконавчої влади.

## 4.2 Роль інноваційних платформ в інноваційному та цифровому розвитку ЄС на прикладі Спільнот знань та інновацій (KIC)

Наступне тематичне дослідження автора було присвячено Спільнотам знань та інновацій (Knowledge and Innovation Communities або

КІС)[1], а саме виявленню аспектів, які роблять КІС ефективним засобом інноваційного та цифрового зростання, до якого активно звертаються у ЄС. Й, хоча дана праця не стосувалася питань опрацювання даних безпосередньо, вона продемонструвала важливість синергічного ефекту при об'єднанні знань різних суб'єктів.

Серед конкретних прикладів подібної синергічної взаємодії можна назвати, зокрема, утворення альянсів для інновацій закладами вищої освіти та бізнесом. Важливість такої кооперації та обміну можна зрозуміти, відштовхуючись від інформації Європейської комісії, за якою близько 80 % промислових даних ніколи не використовуються, що поєднується з постійно зростаючим обсягом даних – з 33 зетабайт, згенерованих у 2018 році, до 175 зетабайт, які очікуються у 2025 році[2].

Окрім того, важливим принципом КІС є раціоналізація спільного використання існуючої інфраструктури, такої як ресурси даних, бібліотеки алгоритмів штучного інтелекту, центри компетентності високопродуктивних обчислень тощо. Подальший аналіз нормативно-правових актів, здійснений в актуальній роботі, підкреслить значення повторного використання даних для розвитку науки та появи інновацій.

Втім, якщо КІС залучають дані від бізнесу на договірних засадах (фактично розраховуючи на їх свідомість чи «добру волю»), сучасне законодавство ЄС все більше говорить про необхідність мобільності даних та недопустимість їх концентрації та локалізації під контролем окремих Інтернет-гігантів та інших суб'єктів, що контролюють великі потоки даних. При цьому емпіричні дослідження у деяких наукових

[1] Див.: Мамаєв І. О. Роль інноваційних платформ в інноваційному та цифровому розвитку ЄС на прикладі спільнот знань та інновацій (КІС). Шляхи імплементації європейської політики впровадження цифрових технологій: монографія / за ред. К. В. Єфремової. Харків: НДІ прав. забезп. інновац. розвитку НАПрН України, 2022. Розд. 4. С. 162–198. URL: https://ndipzir.org.ua/wp-content/uploads/2023/05/monografiya.pdf.

[2] Data Act: Commission proposes measures for a fair and innovative data economy. Press release, 23 February 2022. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.

сферах (особливо у соціальних науках), наразі майже неможливі без наявності доступної інфраструктури даних[1].

Такі зміни можна розглядати як позитивні, оскільки раніше небажання великих контролерів даних йти на контакт з дослідникам знаходило виправдання через несумлінне трактування законодавства про дані. Концентруючи величезні масиви даних, ці компанії були схильні до блокування їх вільного руху, використовуючи привід «захисту персональних даних» як засіб уникнення відповідальності. Про це, як й про необхідність дотримання FAIR-принципів дослідницьких даних та формування доступних централізованих інфраструктур дослідницьких даних, вже говорилося в іншій роботі автора[2].

## 4.3. Питання нормативно-правового забезпечення опрацювання даних

На сьогоднішній день нормативно-правова база ЄС, що прямо чи опосередковано регулює питання опрацювання даних, є доволі широкою та розгалуженою, оскільки включає акти різної юридичної сили та сфери застосування. Окрім того, чимало правових актів, чиїм прямим предметом регулювання не є захист чи опрацювання даних, усе одно впливають на нього.

Так, наприклад, складно уникнути питання захисту та опрацювання даних при встановленні вимог до штучного інтелекту, антимонопольного законодавства чи навіть вирішення питань національ-

[1] Любчич А. М., Мамаєв І. О. Поняття та особливості європейських дослідницьких інфраструктур для гуманітарних і соціальних наук України. *Актуальні питання розбудови науково-дослідницької інфраструктури* : за матеріалами інтернет-конференції (м. Харків, 28 лютого 2022 року). URL: https://ndipzir.org.ua/wp-content/uploads/2022/11/lyubchich_mama%D1%94v.pdf.

[2] Любчич А. М., Мамаєв І. О. Актуальні питання інформаційного забезпечення дослідницьких інфраструктур. *Право та інновації*. 2022. N 2 (38). С. 35–41. DOI 10.37772/2518-1718-2022-2(38)-4. URL: https://pti.org.ua/index.php/ndipzir/article/view/837/648.

ної безпеки. Це пов'язано з тим, що хоча «інформаційне право» виокремлюють в окрему «комплексну галузь права», дані мають прикладне значення у різноманітних сферах суспільного життя з принципово різними методами правового регулювання.

Варто відмітити, що наукові погляди щодо можливості упорядкування та систематизації норм інформаційного права є дискусійними. Так, у 2000-х роках активним був дискурс щодо створення єдиного Інформаційного кодексу України. Загальна частина кодексу за такого підходу могла б містити основні поняття, принципи, форми й методи діяльності в інформаційній сфері. Особлива частина – окремі інститути інформаційного права, у яких були б згруповані близькі за значенням і сутністю інформаційно-правові норми. На думку деяких дослідників, такі кодифіковані акти поряд з міжнародними нормами могли б дати повну, логічну і юридично виважену систему інформаційно-процесуальних норм, які забезпечили б реалізацію інформаційних норм матеріального права[1].

Втім, як продемонстрував час, цей нормативно-правовий акт так і не було створено, незважаючи на чисельні розпорядження «приступити», «розробити» та «завершити розробку» проєкту Інформаційного кодексу України, які протягом двох десятиліть містили постанови Верховної Ради України, послання Президента України, програми та розпорядження Кабінету Міністрів України, рішення і накази Держкомтелерадіо, Держкомзв'язку, Мінюсту, Державної ради з питань європейської і євроатлантичної інтеграції України та ін. Іноземний досвід також демонструє, що майже ніхто в жодній іншій країні не кодифікує інформаційні закони, оскільки акти, що регулюють сферу інформації, стосуються різних галузей права та змішують і приватно-правові, і публічно-правові питання, і авторське право, і конституційні гарантії, тощо[2].

[1] Коваленко Л. П. Інформаційне право України: проблеми становлення та розвитку: автореф. дис. ... д-ра юрид. наук. Харків, 2014. 33 с. URL: https://library.nlu.edu.ua/POLN_TEXT/AFTOREF/Kovalenko_2014.pdf.

[2] Ганжа Л. Інформаційний кодекс: реанімація привиду, який харчується мільйонами. Українська Правда. 26 червня 2015. URL: https://www.pravda.com.ua/columns/2015/06/26/7072512/.

Отже, задля того, щоб уникнути зайвих теоретичних дискусій, доцільно відштовхуватися від існуючої в ЄС системи, яка не має концепції Інформаційного кодексу, однак містить цілий комплекс нормативно-правових актів.

## 4.4. Зародження та становлення нормативно-правового регулювання даних в ЄС

Право на захист персональних даних є фундаментальним правом, дотримання якого визнано важливою метою для усього Європейського Союзу. Формально це право закріплено в Хартії основоположних прав Європейського Союзу[1], зокрема, у статті 8 передбачено, що кожен має право на захист персональних даних, які його стосуються; такі дані повинні оброблятися справедливо, у відповідності до визначених цілей і на основі згоди відповідної особи чи на іншій законній основі; при цьому кожна людина має право на доступ до даних, які були зібрані стосовно неї, а також право на їх виправлення; дотримання цих правил має підлягати контролю з боку незалежного органу.

Виходячи зі сформульованих норм, ми можемо побачити, що людина наділяється рядом прав та гарантії щодо своїх персональних даних. Так, ми можемо виокремити «право на захист персональних даних», «право на справедливу опрацювання даних», що, серед іншого, включає у себе вимоги щодо пропорційності та законності опрацювання даних певним цілям, а також отримання згоди чи іншої законної підстави. Додатково ми маємо змогу сформулювати «право на доступ до власних персональних даних», а також «право на виправлення власних персональних даних». Окремим пунктом закрі-

[1] Charter of Fundamental Rights of the European Union. Official Journal of the European Union. 26.10.2012. C 326/391. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT.

плюється гарантія, за якої дотримання встановлених правил забезпечується контролем незалежного органу.

Що стосується вторинного законодавства, Європейське співтовариство з середини 1990-х років розробило ряд інструментів для забезпечення захисту персональних даних. Одним з перших базових актів такого роду стала Директива 95/46/ЕС (DPD) про захист осіб у зв'язку з опрацюванням персональних даних та про вільний рух таких даних[1]. Й, хоча нині вона замінена на Загальний регламент про захист даних, про який мова піде далі, цей акт заклав такі важливі засади як загальні вимоги щодо законності опрацювання даних, права суб'єктів даних, створення незалежних наглядових органів тощо.

Звісно, за час існування ЄС було прийнято та скасовано чимало нормативно-правових актів у сфері даних. Так, наприклад, для врегулювання опрацювання персональних даних інституціями та органами ЄС було прийнято Регламент № 45/2001, що вже був скасований Регламентом 2018/1725 для адаптації положень до вимог Загального регламенту про захист даних. В подальшому робота більшою мірою зосередиться на аналізі найбільш значних та актуальних документів для формування уявлення про сучасні європейські практики.

В інституційному плані важливим рішенням було створення органу Європейського інспектору із захисту даних (EDPS) у 2004-му році. Названий орган очолюється супервайзером та підтримується офісом (секретаріатом) досвідчених юристів, ІТ-фахівців та адміністраторів, що працюють для реалізації визначених цілей: контроль та забезпечення захисту персональних даних і конфіденційності, коли інституції та органи ЄС опрацьовують персональну інформацію; консультування інституцій та органів ЄС з усіх питань, пов'язаних з опрацюванням персональних даних, за запитом або за нашою власною ініціативою; відстеження нових технологій, які можуть вплинути на захист персональних даних; комунікація з Судом ЄС для надан-

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046.

ня експертних порад щодо тлумачення законодавства про захист даних; співпраця з наглядовими органами для покращення узгодженості захисту персональних даних.

Положення щодо захисту та опрацювання персональних даних розширила Директива 2002/58/ЄС про конфіденційність та електронні комунікації[1], яка залишається чинною й станом на 2023-й рік. За своїм призначенням та регуляторним впливом її можна розглядати як безпосереднє продовження та доповнення Директива 95/46/ЄС. До сфери її регулювання попали такі важливі питання як конфіденційність даних, опрацювання даних про трафік, проблеми спаму та файлів cookie. У подальшому декілька важливих змін, зокрема щодо вимоги запитувати попередню згоду на збереження файлів cookie, були принесені Директивою 2009/136.

Навіть незважаючи на такі корективи, нормативно-правове регулювання 2000-х років поступово проявляє ознаки морального старіння, а тому чимало дослідників та юристів очікували скасування Директиви 2002/58/ЄС та прийняття Регламенту електронної конфіденційності (ePrivacy Regulation або ePR). Названий нормативно-правовий акт міг бути прийнятий незабаром після Загального регламенту про захист даних. Так, перший офіційний проєкт постанови був представлений Європейською комісією 10 січня 2017 року, а у першій половині 2018 року завершилися тристоронні переговори з Комісією, парламентом та Радою, після чого вже проголосований акт мав набрати чинності вже у травні того ж року. Втім дискусії щодо ePR продовжують тривати й у наші дні.

[1] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058.

## 4.5. Базові засади регулювання неперсональних даних

Базові засади регулювання персональних даних були розглянуті автором у підрозділі 3.1, що рекомендується до ознайомлення для формування комплексного уявлення про регулювання даних. Даний підрозділ зосередиться на такій сфері як неперсональні дані.

У той час як важливість захисту персональних даних не викликає питань майже ні в кого, важливість регулювання опрацювання неперсональних даних часто недооцінюється. Стрімкий розвиток цифрових технологій та нових ринків породжують чимало правових проблем, пов'язаних з даними. Серед них питання доступу та повторного використання даних, проблема локалізації та обмеженої мобільності даних, ризики монополізації великих наборів даних в руках Інтернет-гігантів, стимулювання приватного та державного секторів до передання цінних наборів даних для наукової мети, а також інші питання, зокрема й етичного характеру (наприклад, щодо соціальної відповідальності бізнесу).

При цьому частина з цих проблем утворена на національному, регіональному або навість приватному рівні через правовий вакуум. Так, приватні компанії можуть обмежувати можливості клієнтів шляхом укладання договорів або проектування технологічних систем таким чином, що не дозволяє користувачу послуг опрацювання даних переносити створені неперсональні дані від одного постачальника послуг до іншого. Звісно, що такої ситуації не склалося, якщо б існувала пряма юридична вимога забезпечити можливість перенесення даних (а отже й вимога проєктувати технології таким чином, що зроблять можливою таку мобільність).

У цьому контексті Європейська Комісія зробила важливий наголос на тому, що спільне використання даних не завдає ним ніякої шкоди: «Дані є неконкурентним товаром, так само, як вуличне освітлення чи мальовничий краєвид: багато людей можуть отримати до них доступ одночасно, і їх можна споживати знову і знову, не впли-

ваючи на їх якість і не піддаючись ризику того, що джерело буде скорочено чи виснажено»[1].

У той час як GDPR є комплексним актом, що встановлює розгалужену систему нормативних вимог та обмежень, Регламент (ЄС) 2018/1807 від 14 листопада 2018 року встановлює рамки для вільного потоку неперсональних даних у Європейському Союзі[2]. Загалом цей акт є доволі компактним та складається лише з 9 статей: (1) предмет, (2) область застосування, (3) визначення, (4) вільний рух даних у межах Союзу, (5) доступність даних для компетентних органів, (6) перенесення даних, (7) порядок взаємодії органів влади, (8) оцінка та рекомендації, а також (9) заключні положення.

Як зазначалося вище, потреба у регулюванні даних стикається з двома протилежними факторами, що мають бути враховані. Перший – це потреба захисту даних, зокрема встановлення відповідних прав у суб'єктів цих даних. Другий – забезпечення вільного руху даних, необхідного для економічного зростання, формування обґрунтованої політики та сприяння науково-технічним дослідженням й інноваційному розвитку країни.

Разом з тим Європейською Комісією було відзначено появу нового «цифрового розриву», що відтепер викликаний не лише різницею між добре зв'язаними міськими районами та сільськими й віддаленими територіями, а й між тими, хто може повною мірою скористатися перевагами збагаченого, доступного та безпечного цифрового простору з повним спектром послуг, і тими, хто не може. Подібний розрив виник між тими підприємствами, які вже можуть використовувати весь потенціал цифрового середовища, і тими, хто ще не повністю оцифрований[3]. Й, хоча «використання потенціалу цифрового

[1] Data Act: Commission proposes measures for a fair and innovative data economy. Press release, 23 February 2022. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.

[2] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. URL: https://eur-lex.europa.eu/legal- content/EN/TXT/?uri=celex%3A32018R1807.

[3] Communication: 2030 Digital Compass: the European way for the Digital Decade. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en.

середовища» є широким поняттям, справедливо вважати, що воно включає у себе й використання потенціалу накопичених даних. На додаток до того, що ринкова влада деяких онлайн-платформ потенційно викликає занепокоєння, особливо щодо найпотужніших платформ, значення яких для інших учасників ринку стає дедалі критичнішим.

Громадянам слід надати можливість приймати кращі рішення на основі інформації, отриманої з неособистих даних. І ці дані мають бути доступними для всіх – державних чи приватних, великих чи малих, стартапів чи гігантів. Це допоможе суспільству отримати максимальну віддачу від інновацій і конкуренції та гарантувати, що кожен отримає вигоду від цифрового дивіденду[1].

Юридичне визначення поняття «неперсональних даних», що вже неодноразово згадувалося в роботі, закріплюється відсильною нормою та через негативне формулювання: так, неперсональними даними у значенні Регламенту (ЄС) 2016/679 вважаються будь-які дані, відмінні від персональних даних, як вони визначені в пункті 1 статті 4 Регламенту (ЄС) 2016/679 Про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних[2].

Пункт 1 статті 4 Регламенту (ЄС) 2016/679 надає «персональним даним» таку ж дефініцію, як й пункт 1 статті 4 GDPR, за яким це будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи яку можна ідентифікувати («суб'єкт даних»); фізична особа, яку можна ідентифікувати, є такою особою, яка може бути ідентифіковано, прямо чи опосередковано, зокрема, за такими ідентифікаторами як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи декількома факторами, що є визна-

[1] 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/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679.

чальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи.

Пункт 9 Передмови до Регламенту (ЄС) 2018/1807 наводить конкретні приклади неособистих даних, що включають у сукупні та анонімні набори даних, які використовуються для аналітики великих даних, дані про точне землеробство, які можуть допомогти контролювати та оптимізувати використання пестицидів і води, або дані про потреби в обслуговуванні промислових машин. Відзначається, що основними джерелами неособистих даних можна вважати розширення Інтернету речей, штучного інтелекту та машинного навчання (наприклад, у результаті їхнього розгортання в автоматизованих процесах промислового виробництва).

При цьому дане поняття не слід вважати статичним. Якщо технологічний розвиток робить можливим перетворити анонімні дані на персональні дані, такі дані повинні розглядатися як персональні дані, і Регламент (ЄС) 2016/679 повинен застосовуватися відповідно.

Як і GDPR, даний Регламент має екстериторіальний характер, що випливає зі статті 2, яка розширює область застосування цього нормативно-правого акту до випадків, коли: (а) надання електронних даних здійснюється як послуга користувачам, що проживають або мають представництво в Союзі, незалежно від того, зареєстрований постачальник послуг у Союзі чи ні; (б) здійснюється фізичною або юридичною особою, яка проживає або має установу в Союзі для власних потреб.

Відповідно до статті 1 Регламенту (ЄС) 2018/1807, акт має на меті встановлення правил щодо вимог щодо локалізації даних, доступності даних для компетентних органів та перенесення даних для професійних користувачів. Окремо слід відмітити впровадження саморегулятивних «кодексів поведінки» та встановлення правил взаємодії між державами-членами.

Одним з основних досягнень Регламенту (ЄС) 2018/1807 можна вважати закріплення вільного руху даних у межах Союзу. Так, частина 1 статті 4 прямо закріплю заборону висувати вимоги щодо локалізації даних, якщо вони не виправдані міркуваннями громадської

безпеки з дотриманням принципу пропорційності. Існуючі вимоги щодо локалізації повинні були бути скасовані до 30 травня 2021 року, а процедура встановлення нових передбачає ряд обмежень: зокрема, частина 2 статті 4 закріплює обов'язок негайного повідомлення Комісії про будь-який проект акту, що стосується запровадження нових чи зміни існуючих вимог до локалізації даних. А частина 4 статті 4 зобов'язує оприлюднювати деталі будь-яких вимог щодо локалізації даних через єдиний національний інформаційний пункт, який повинен постійно оновлювати актуальну інформацію про будь-які вимоги такого роду, повідомляючи центральний інформаційний пункт Союзу.

Пункт 4 Передмови Регламенту (ЄС) 2018/1807визнає проблему правової невизначеності щодо законних і нелегітимних вимог щодо локалізації даних. Описана ситуація ще більше обмежує можливості вибору, доступні гравцям ринку та державному сектору щодо місця опрацювання даних. Втім введений нормативно-правовий акт не обмежує свободу бізнесу укладати договори, у яких вказується, де мають бути дані, а лише має на меті захистити цю свободу, гарантуючи, що узгоджене місце може бути розташоване будь-де в межах Союзу.

Варто відмітити, шо «вимога локалізації даних» розуміється у значення пункту 5 статті 3 Регламенту (ЄС) 2018/1807, та означає будь-які зобов'язання, заборони, умови, обмеження чи інші вимоги, що передбачені законами, нормативними або адміністративними положеннями держави-члена або випливають із загальної та послідовної адміністративної практики в державі-члені та в органах, що регулюються публічним правом.

Інший важливий блок нормативного регулювання стосується забезпечення доступності даних для компетентних органів. Зокрема, встановлюється норма, за якої компетентним органам не може бути відмовлено у доступі до даних на підставі того, що дані опрацьовуються в іншій державі-члені. При чому, якщо між двома країнами не існує міжнародних угод, що встановлювали б спеціальний механізм співпраці для обміну даними, Регламент (ЄС) 2018/1807 передбачає можливість звернутися до компетентного органу іншої держави, що

має відповідні механізми співпраці з потрібним суб'єктом. Невиконання законних вимог або зловживання правами користувача, тягне за собою несприятливі наслідки, як це зазначено у статті 5.

Пункт 6 статті 3 Регламенту (ЄС) 2018/1807роз'яснює, що таким органом може вважатися орган держави-члена або будь-яка інша установа, уповноважена національним законодавством виконувати публічну функцію або виконувати офіційні повноваження, яка має повноваження отримувати доступ до даних, опрацьованих фізичною або юридичною особою для виконання свої офіційні обов'язки, як це передбачено законодавством Союзу або національним законодавством. Варто також зробити зауваження, що механізм «Єдиного вікна» (One-Stop-Shop), який передбачає можливість взаємодіяти з єдиним головним наглядовим органом (Lead Supervisory Authority) для більшості дій з опрацювання персональних даних, не застосовується до неперсональних даних.

Важливим напрямом опрацювання неперсональних даних, що може дати значний позитивний ефект, є використання інформації, яка фінансується державами-членами. Так, в пункті 8 Преамбули до Директиви (ЄС) 2019/1024 про відкриті дані та повторне використання інформації державного сектору[1], Європейська Комісія наголосила, що державний сектор збирає, виробляє, відтворює та поширює широкий спектр інформації в багатьох сферах діяльності, таких як соціальна, політична, економічна, юридична, географічна, екологічна, метеорологічна, сейсмічна, туристична, бізнес, патентна та освітні галузі. Документи, створені органами виконавчої, законодавчої чи судової влади державного сектору, становлять величезний, різноманітний і цінний фонд ресурсів, які можуть принести користь суспільству.

Пункт 4 Преамбули до Директиви (ЄС) 2019/1024 роз'яснює, що зміни в правовому регулюванні мають за мету повне використання потенціалу інформації державного сектору для європейської еконо-

[1] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L1024.

міки та суспільства, та повинні зосереджуватися на таких сферах як забезпечення доступу до динамічних даних у режимі реального часу за допомогою відповідних технічних засобів; збільшення надання цінних загальнодоступних даних для повторного використання, в тому числі від державних підприємств, дослідницьких організацій та організацій, що фінансують дослідження; боротьба з появою нових форм ексклюзивних угод; використання принципу стягнення граничної вартості за доступ до даних та винятки з нього, а також встановлення гармонізованих зв'язків між цією Директивою та пов'язаними правовими інструментами (такими як GDPR).

## 4.6. Актуальні зміни у законодавстві ЄС про дані

20 червня 2019 року Європейська Рада погодила порядок денний для ЄС на наступні п'ять років. Новий стратегічний порядок денний на 2019-2024 рр [1] визначає пріоритетні сфери, які керуватимуть роботою Європейської Ради та забезпечуватимуть керівництво для робочих програм інших установ ЄС. Так, шість пріоритетів Комісії на 2019-2024 роки складають: «Європейська зелена угода» «Європа, придатна для цифрової ери», «Економіка, яка працює для людей», «Сильніша Європа у світі», «Просування нашого європейського способу життя» та «Новий поштовх для європейської демократії».

Хоча питання захисту та опрацювання даних так чи інакше зачіпають правовідносини в усіх названих сферах, найбільш актуальним для поставленої теми є пріоритет «Європа, придатна для цифрової ери» («A Europe fit for the digital age»). В рамках названого пріоритету було прийнято чимало нормативно-правових актів та проведено інші супутні дії, узагальненому огляду яких буде присвячено наступну частину роботи.

[1] A new Strategic Agenda 2019-2024. URL: https://era.gv.at/policies/strategic-agenda-2019-24/.

Так, 19 лютого 2020 року було опубліковано Порядок денний для формування цифрового майбутнього Європи[1], а також Стратегію щодо даних[2] та Білу книги щодо штучного інтелекту[3]. Стратегія щодо даних, зокрема, відмітила потребу у формуванні певної структури, яка дозволить підприємствам створювати, об'єднувати та використовувати дані для вдосконалення продуктів і конкурувати на міжнародному рівні таким чином, щоб підтримувати європейські цінності та поважати права осіб на конфіденційність. Для цього вона спрямувала свій вплив на утворення «єдиного європейського простору даних» – справжнього єдиного ринку даних, а також десяти галузевих спільних європейських просторів даних, які мають відношення до подвійного зеленого та цифрового переходу. Для всіх цих пріоритетів ключовою є чітка та працездатна структура для безпечного обміну даними та підвищення доступності даних. У Стратегії щодо даних також оголошено про намір дослідити в майбутньому законодавстві питання, які дозволять використання даних із загальнодоступних баз даних, для наукових дослідницьких цілей відповідно до GDPR. Окрім того, було визначено, що простори даних мають підтримуватися Європейською хмарною федерацією, зокрема через надання послуг опрацювання даних та хмарної інфраструктури, які відповідають GDPR[4].

10 березня 2020 року представлено Нову промислову стратегію[5], що ставить за мету «допомогти європейській промисловості очолити

[1] Communication: Shaping Europe's digital future. 2020, February 19. URL: https://commission.europa.eu/document/84c05739-547a-4b86-9564-76e834dc7a49_en.

[2] 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/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066.

[3] White Paper on Artificial Intelligence: a European approach to excellence and trust. 2020, February 19. URL: https://commission.europa.eu/document/d2ec4039-c5be-423a-81ef-b9e44e79825b_en.

[4] Communication from the Commission to the European Parliament and the Council Data protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition - Two Years of Application of the General Data Protection Regulation. COM(2020) 264 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0264&rid=5.

[5] Making Europe's businesses future-ready: A new Industrial Strategy for a globally competitive, green and digital Europe.: Press release, 2020, March 10. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_416.

подвійний перехід до кліматичної нейтральності та цифрового лідерства» за допомогою трьох ключових пріоритетів: (1) підтримання глобальної конкурентоспроможності європейської промисловості та рівних умов гри вдома та в усьому світі, (2) створення кліматично нейтральної Європи до 2050 року та (3) формування цифрового майбутнього Європи. У сфері даних Нова промислова стратегія не стала вводити багато нових зобов'язань: в параграфі 3.1 вона наголосила на необхідності продовжувати існуючу Європейську стратегію даних для розвитку економіки даних ЄС, включаючи запуск спільних європейських просторів даних у певних секторах і ланцюжках створення вартості; а в параграфі 3.3 було проголошено, що Загальний європейський енергетичний простір даних має використовувати потенціал даних для підвищення інноваційного потенціалу енергетичного сектора. Окрім того, була відзначена потреба у прискоренні інвестицій в дослідження та розгортання технологій у таких сферах, як штучний інтелект, 5G, аналітика даних і метаданих. Висловлено очікування, що успішне розгортання високозахищеної мережі 5G стане основним фактором розвитку майбутніх цифрових послуг та центром розповсюдження промислових даних. Високопродуктивні обчислення та хмарна інфраструктура даних названі «ключовими базовими технологіями, які є стратегічно важливими для промислового майбутнього Європи». Разом з тим акт відзначив необхідність переглянути й оновити законодавство про єдиний ринок, щоб переконатися, що воно відповідає епосі цифрових технологій. Як таке, що також потребує перегляду, було оцінено й законодавство про інтелектуальну власність.

24 вересня 2020 року було ухвалено так званий «Пакет цифрових фінансів», що включає Стратегію цифрових фінансів[1], законодавчі пропозиції щодо криптоактивів і цифрової стійкості[2], пропозиції

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU. COM/2020/591 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0591.

[2] Digital finance package. By Directorate-General for Financial Stability, Financial Services and Capital Markets Union. 2020, September 24. URL: https://finance.ec.europa.eu/publications/digital-finance-package_en.

щодо нормативно-правової бази ЄС щодо цифрової операційної стійкості та оновлену Стратегію сучасних і безпечних роздрібних платежів. Стратегія цифрових фінансів, зокрема, закріпила чотири пріоритети, третім з яких є створення європейського простору фінансових даних, що забезпечить розширений доступ до даних та обмін даними у фінансовому секторі. Це сприятиме створенню інноваційних продуктів для споживачів і підприємств, а також підтримуватиме ширші політичні цілі, такі як створення єдиного ринку даних. Це також сприятиме полегшенню доступу до даних, необхідних для спрямування фінансування на підтримку сталих інвестицій. Наявність цифрових даних дозволяє точніше прогнозувати майбутні події, а аналіз об'єднаного набору даних дає більше інформації, ніж аналіз кожного набору даних окремо. При цьому економічні вигоди, отримані від певного набору даних, вищі, коли до нього мають одночасний доступ кілька сторін. Окрім того, цифровізація фінансових даних має сприяти й обміну даними між наглядовими органами.

Пропозиції щодо криптоактивів і цифрової стійкості також містять примітні положення щодо даних. Так, наприклад, частина 2 статті 4 встановлює, що криптоактиви не вважаються такими, що пропонуються безкоштовно, якщо від покупців вимагається надати персональні дані емітенту в обмін на ці криптоактиви. Такий підхід можна вважати прогресивним, оскільки багато послуг, що є умовно-безкоштовними, використовують персональні дані осіб для комерціалізації. А частина 8 статті 40 вимагає від емітентів токенів, пов'язаних із активами, встановити політику безперервності бізнесу, яка забезпечує, у разі порушення певних систем або процедур, збереження важливих даних для підтримки діяльності, або, якщо це неможливо, своєчасне відновлення таких даних.

15 грудня 2020 року було запропоновано проєкт Закону про цифрові ринки та проєкт Закону про цифрові послуги. Втім перший набрав чинності лише 1-го листопада 2022 року, а другий – 16 листопада 2022 року, у зв'язку з чим вони будуть розглянуті далі.

16 грудня 2020 року прийнято Нову стратегія кібербезпеки ЄС[1], яка стала ключовим компонентом Формування цифрового майбутнього Європи, Плану відновлення Європи та Стратегії Союзу безпеки ЄС. Стратегія містить конкретні пропозиції щодо регуляторних, інвестиційних і політичних ініціатив у трьох сферах діяльності ЄС: 1. «Стійкість, технологічний суверенітет і лідерство»; 2. «Розбудова оперативного потенціалу для запобігання, стримування та реагування»; 3. «Розвиток глобального та відкритого кіберпростору шляхом посилення співпраці». Відзначається, що поліпшення кібербезпеки є важливим для того, щоб люди довіряли, використовували та отримували користь від інновацій, зв'язку та автоматизації. Окрім того, це стосується й захисту основних прав та свобод, включаючи права на конфіденційність, захист персональних даних, свободу вираження поглядів та інформацію. Кіберпростір все частіше використовується для політичних та ідеологічних цілей, а посилення поляризації на міжнародному рівні перешкоджає ефективній багатосторонності. Гібридні загрози поєднують дезінформаційні кампанії з кібератаками щодо інфраструктури, економічних процесів та демократичних інститутів, з потенціалом для заподіяння фізичної шкоди, отримання незаконного доступу до особистих даних, крадіжки промислових або державних таємниць, посіву недовіри та послаблення соціальної когезії. Ці заходи підривають міжнародну безпеку та стабільність та переваги, які кіберпростори приносять для економічного, соціального та політичного розвитку. У зв'язку з цим нова Стратегія поставила за мету зміцнити колективну безпеку Європи та посилити лідерство щодо міжнародних норм і стандартів у кібербезпеці, зміцнивши співпрацю з партнерами для просування глобального, відкритого, стабільного та безпечного кіберпростору, заснованого на верховенстві права, основних правах та свободах людини та демократичних цінностях.

9 березня 2021 року була представлена програма «Цифрове десятиліття Європи», якою Європейська Комісія встановила курс на роз-

[1] New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. Press release, 16 December 2020. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391.

виток цифрової Європи до 2030 року[1] Серед іншого Комісія утвердила Цифровий компас, щоб перевести цифрові амбіції у конкретні етапи та цілі. Вони розвиваються навколо чотирьох напрямів: (1) «Цифрові громадяни» та висококваліфіковані «цифрові професіонали» – до 2030 року принаймні 80% усіх дорослих мають мати базові цифрові навички, а в ЄС має бути 20 мільйонів спеціалістів з ІКТ, при цьому більше жінок мають виконувати такі роботи; (2) Безпечні, ефективні та стійкі цифрові інфраструктури – до 2030 року всі домогосподарства ЄС повинні мати гігабітне підключення, а всі населені пункти повинні бути покриті 5G; виробництво передових та екологічно чистих напівпровідників у Європі має становити 20% світового виробництва; 10 000 кліматично нейтральних високозахищених периферійних вузлів мають бути розгорнуті в ЄС; і Європа повинна мати свій перший квантовий комп'ютер; (3) Цифрова трансформація бізнесу – до 2030 року три з чотирьох компаній повинні використовувати послуги хмарних обчислень, великі дані та штучний інтелект; більше 90% МСП мають досягти принаймні базового рівня цифрової інтенсивності; і кількість єдинорогів ЄС має подвоїтися; (4) Цифровізація державних послуг – до 2030 року всі ключові державні послуги мають бути доступні онлайн; всі громадяни матимуть доступ до своїх електронних медичних карток; і 80% громадян повинні використовувати рішення eID.

21 квітня 2021 року були запропоновані нові Правила та дії для досконалості та довіри до штучного інтелекту[2] та Узгоджений план зі штучного інтелекту[3]. Враховуючи, що навчання штучного інтелекту зазвичай передбачає використання певного масиву даних (зокрема

[1] Europe's Digital Decade: Commission sets the course towards a digitally empowered Europe by 2030. Press release, 9 March 2021. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_983.

[2] Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence. Press release, 21 April 2021. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682.

[3] Coordinated Plan on Artificial Intelligence 2021 Review. 21 April 2021. URL: https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review.

таких, що можуть мати персональний, комерційних чи інший характер), питання врегулювання штучного інтелекту тісно пов'язано з питанням опрацювання та захисту даних. Європейська декларація цифрових прав і принципів від 25 січня 2022 року[1] також приділяє увагу питанню штучного інтелекту, присвячуючи йому окремий третій розділ – «Свобода вибору». Постулюється, що кожна людина повинна мати можливість користуватися перевагами штучного інтелекту, роблячи власний усвідомлений вибір у цифровому середовищі, захищаючись від ризиків і шкоди своєму здоров'ю, безпеці та основним права. Задля цього Декларація передбачає такі зобов'язання ЄС, як: 1) забезпечення прозорості використання алгоритмів і штучного інтелекту, а також того, що люди мають повноваження та інформацію під час взаємодії з ними; 2) забезпечення того, щоб алгоритмічні системи базувалися на відповідних наборах даних, щоб уникнути незаконної дискримінації та дозволити людині контролювати результати, які впливають на людей; 3) забезпечення того, щоб технології, такі як алгоритми та штучний інтелект, не використовувалися для попереднього визначення вибору людей, наприклад, щодо здоров'я, освіти, працевлаштування та їхнього приватного життя; 4) забезпечення гарантій, щоб штучний інтелект і цифрові системи були безпечними та використовувалися з повною повагою до основних прав людей.

11 травня 2021 року була оновлена Промислова стратегія ЄС[2], яка має гарантувати, що європейські промислові амбіції повністю враховують нові обставини після кризи COVID-19. Відмічено, що оновлений варіант стратегії приділяє МСП ще більше уваги, зокрема у підвищеному фокусі на регуляторному тягарі для МСП. Окрім того, стратегія зосереджена на забезпеченні стійкості Єдиного ринку, підтримці відкритої стратегічної автономії Європи через вирішення проблем залежностей, а також підтримці бізнес- обґрунтованих по-

[1] Declaration on European Digital Rights and Principles. 25 January 2022. URL: https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles#Communication.

[2] European industrial strategy. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy_en.

двійних переходів. Нажаль, Стратегія не приділяє питанню даних багато уваги, проте стосується опрацювання неперсональних даних, зокрема моніторингу ринків, та оцифровування інспекцій продукції та збору даних із залученням найсучасніших технологій для відстеження невідповідних та небезпечних продуктів. Окрім того, Стратегія звернула увагу на децентралізовані хмарні обчислення та передбачила запуск Альянсів з питань процесорів і напівпровідникових технологій, промислових даних та хмарних послуг.

3 червня 2021 року Комісія запропонувала Структуру для надійної та безпечної європейської цифрової ідентифікації[1]. Оновлення правил цифрової ідентифікації пов'язано, зокрема, з прийняттям Цифрового компасу до 2030 року, який встановив ряд цілей і етапів для покращення європейської цифрової ідентифікації. Очікується, що до 2030 року всі ключові державні послуги мають бути доступні онлайн, усі громадяни матимуть доступ до електронних медичних карт, а 80% громадян повинні використовувати рішення eID. Для реалізації цієї ініціативи Європейська Комісія спирається на існуючу транскордонну правову базу для надійних цифрових ідентифікацій, Європейську електронну ідентифікацію та ініціативу довірчих послуг (Регламент eIDAS)[2]. Прийнятий у 2014 році, він забезпечує основу для транскордонної електронної ідентифікації, автентифікації та сертифікації веб-сайтів у межах ЄС. Вже близько 60% європейців можуть скористатися поточною системою. Однак раніше від держав-членів не вимагалося розробляти національний цифровий ідентифікатор сумісним із документами інших держав-членів, що призводило до великих розбіжностей між країнами. Поточна пропозиція має усунити ці недоліки шляхом підвищення ефективності структури та поширення її переваг на приватний сектор і мобільне використання.

[1] Commission proposes a trusted and secure Digital Identity for all Europeans. Press release, 3 June 2021. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663.

[2] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG.

16 вересня 2021 року Європейська Комісія запропонувала «Шлях до цифрового десятиліття»[1] – конкретний план досягнення цифрової трансформації суспільства та економіки до 2030 року. Запропонований шлях до цифрового десятиліття має перетворити цифрові амбіції ЄС на 2030 рік у конкретний механізм реалізації. Він створить структуру управління на основі щорічного механізму співпраці з державами-членами для досягнення цілей цифрового десятиліття до 2030 року на рівні Союзу в сферах цифрових навичок, цифрової інфраструктури, цифровізації бізнесу та державних послуг. Він також спрямований на визначення та реалізацію великомасштабних цифрових проєктів за участю Європейської Комісії та держав-членів, а серед пріоритетів визначено: хмарні технології, розвиток інфраструктури даних, 5G зв'язок, високопродуктивні обчислення, центри цифрових інновацій, кібербезпеку та інше (що прямо чи опосередковано пов'язано з питанням опрацювання даних, їх вільного обігу та захисту).

18 листопада 2021 року Європейська Комісія прийняла Повідомлення про політику конкуренції, яка відповідає новим викликам[2], у якій визначено важливу роль політики конкуренції на шляху Європи до відновлення, зеленого та цифрового переходу, а також для стійкого єдиного ринку. Окремі національні закони, такі як німецький Акт проти обмеження конкуренції (Gesetz gegen Wettbewerbsbeschränkungen), вже давно розширили повноваження антимонопольних органів проти Інтернет-гігантів, запровадивши принципи «превентивного підходу» та нагляд за «майбутніми очікуваннями» компанії, щоб оперативно протидіяти загрозам на сучасних динамічних ринках[3]. Додаток до Повідомлення про політику конкуренції, яка відпо-

[1] Policy Programme: a Path to the Digital Decade - factsheet. 15 September 2021. URL: https://digital-strategy.ec.europa.eu/en/library/policy-programme-path-digital-decade-factsheet.

[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions a Competition Policy Fit for New Challenges. URL: https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2021)713&lang=en.

[3] Мамаєв І. О. Розділ 4: Актуальні питання обробки та обігу даних у цифрових інфраструктурах: досвід Німеччини. Базові аспекти цифровізації та їх правове

відає новим викликам[1] роз'яснює, що ініціатива Європейської Комісії стосується перегляду правил конкуренції, які застосовуються до угод про співпрацю між конкурентами. Мова йде про два регламенти про групові виключення 2010 року, що передбачають «безпечні гавані» для певних категорій угод про дослідження та розробки та для певних категорій угод про спеціалізацію (виробництво), а також супровідні керівні принципи щодо застосування правил конкуренції до різних видів угод про співпрацю (обмін інформацією, дослідження та розробки, спільне виробництво, спільна комерціалізація, спільні закупівлі, стандартизація). Дана ініціатива має на меті переконатися, що надані вказівки враховують нові тенденції ринку, такі як більш часте використання пулів даних, розширення співробітництва в дослідженнях і розробках, а також угоди щодо сталого розвитку.

26 січня 2022 року Європейська Комісія запропонувала Європейському парламенту та Раді підписати Декларацію цифрових прав і принципів[2][3]. Структурно акт складається з преамбули та шести глав. Питання захисту та вільного руху даних знаходить своє відображення у декількох з них. Так, Глава II «Солідарність та інклюзивність» містить підрозділ «Цифрові публічні послуги онлайн». Відповідно до нього, кожен повинен мати доступ до всіх ключових державних послуг онлайн по всьому Союзу. Від нікого не можна вимагати надавати дані частіше, ніж це необхідно, під час доступу та використання цифрових публічних послуг. Декларація, зокрема, передбачає такі

забезпечення : монографія / за ред. К. В. Єфремової. Харків: НДІ прав. забезп. інновац. розвитку НАПрН України, 2021. 180 с. URL: https://ndipzir.org.ua/archives/7511.

[1] Annex to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions a Competition Policy Fit for New Challenges. URL: https://ec.europa.eu/transparency/documents-register/detail?ref=COM(2021)713&lang=en.

[2] Commission puts forward declaration on digital rights and principles for everyone in the EU. Press release, 26 January 2022. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_452.

[3] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Establishing a European Declaration on Digital Rights and Principles for the Digital Decade. URL: https://ec.europa.eu/newsroom/dae/redirection/document/82699.

зобов'язання підписантів: 1) забезпечення того, щоб усім європейцям була запропонована доступна, безпечна та надійна цифрова ідентифікація, яка надає доступ до широкого спектру онлайн-послуг; 2) забезпечення широкого доступу та повторного використання урядової інформації; 3) сприяння та підтримка безперебійного, безпечного та сумісного доступу по всьому Союзу до цифрових послуг охорони здоров'я та догляду, включаючи медичні записи, призначених для задоволення потреб людей.

Глава III «Свобода вибору», що стосується штучного інтелекту, вже було розглянути вище.

Глава V: Безпека, охорона та розширення можливостей. Захищене, безпечне та таке, що знаходиться під охороною онлайн-середовище. Кожен повинен мати доступ до цифрових технологій, продуктів і послуг, які за своєю природою є безпечними, такими, що знаходяться під охороною та захищають конфіденційність. Ми зобов'язуємося: – захищати інтереси людей, підприємств і державних установ від кіберзлочинності, включаючи витік даних і кібератаки. Це включає захист цифрової ідентифікації від крадіжки або маніпулювання особистими даними; – протидіяти та притягати до відповідальності тих, хто прагне підірвати безпеку в Інтернеті та цілісність європейського онлайн-середовища або пропагує насильство та ненависть за допомогою цифрових засобів. Конфіденційність та індивідуальний контроль над даними передбачає, що кожен має право на захист своїх персональних даних в Інтернеті. Це право включає контроль над тим, як використовуються дані та з ким вони діляться. Кожен має право на конфіденційність своїх повідомлень та інформації на своїх електронних пристроях, і ніхто не може бути підданий незаконному онлайн-спостереженню або заходам перехоплення. Кожна людина повинна мати можливість визначити свою цифрову спадщину та вирішити, що станеться із загальнодоступною інформацією, яка її стосується, після її смерті. Ми зобов'язуємося: – забезпечити можливість легкого переміщення персональних даних між різними цифровими службами.

8 лютого 2022 року було запропоновано European Chips Act[1] (Європейський закон про чіпи), покликаний пом'якшити наслідки «кризи напівпровідників», що може використовуватися як гібридна загроза через критичну важливість напівпровідників для мікросхем. Регулювання вільного руху неперсональних даних також отримало відображення в цьому акті та представляє інтерес як приклад регулювання даних в екстремальних умовах. Так, пункт 47 European Chips Act окреслив процедуру запитів на інформацію від підприємств уздовж ланцюга постачання напівпровідників, створених у ЄС на стадії кризи, що має сприяти поглибленій оцінці кризи задля визначення потенційних заходів пом'якшення чи надзвичайних заходів на рівні Союзу чи національному рівні. Така інформація може включати виробничі можливості, виробничі потужності, а також поточні первинні збої та «вузькі місця». Названі аспекти додатково можуть включати типові та поточні фактичні запаси продуктів, що мають відношення до кризи; типовий і поточний фактичний середній час виробництва найпоширеніших продуктів, що випускаються; очікуваний обсяг виробництва протягом наступних трьох місяців для кожного виробничого об'єкта Союзу; причини, що перешкоджають заповненню виробничих потужностей; або інші наявні дані, необхідні для оцінки характеру напівпровідникової кризи або потенційного пом'якшення чи надзвичайних заходів на національному рівні чи рівні Союзу. Будь-який запит має бути пропорційним, враховувати законні цілі підприємства та витрати та зусилля, необхідні для надання даних, а також встановлювати відповідні часові обмеження для надання запитуваної інформації. Підприємства повинні бути зобов'язані виконати запит і можуть бути піддані штрафам, якщо вони не виконали або надали невірну інформацію. Будь-яка отримана інформація повинна дотримуватися вимог, встановлених правилами конфіденційності. Якщо підприємство має запит на інформацію, пов'язану з його напівпровідниковою діяльністю, з третьої країни, воно має повідомити про це Європейську Комісію, щоб дати змогу оцінити, чи запит на інформацію з боку Комісії є виправданим.

[1] European Chips Act. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en.

23 лютого 2022 року було запропоновано Закон про дані ЄС[1], що має стати останнім горизонтальним блоком Стратегії даних. Пропозиція щодо Закону про дані передбачає декілька важливих напрямів впливу. По-перше, заходи, які дозволять користувачам підключених пристроїв вільно отримувати доступ до даних, створених ними, а також ділитися такими даними з третіми особами для надання післяпродажних або інших інноваційних послуг на основі даних. На сьогодні клієнт зазвичай позбавлений такої можливості. Зміна цієї ситуації має підтримати стимули для виробників, зокрема виключає використання спільних даних для прямої конкуренції та стимулює інвестувати у високоякісну генерацію даних. По-друге, Закон про дані передбачає заходи для відновлення балансу переговорних можливостей МСП шляхом запобігання зловживанню контрактними дисбалансами в контрактах про обмін даними. Закон про дані захистить їх від несправедливих договірних умов, нав'язаних стороною зі значно сильнішою позицією на переговорах. Комісія також розробить типові договірні умови, щоб допомогти таким компаніям розробити та узгодити справедливі контракти на обмін даними. По-третє, Закон про дані надає засоби для органів державного сектору, які дозволять оперативно отримати доступ до даних приватного секторі у разі виняткових обставин (зокрема для швидкого та безпечного реагування на надзвичайні ситуації). Тягар для компаній при цьому має бути мінімізовано. Нарешті, нові правила дозволять клієнтам ефективно переходити між різними постачальниками хмарних послуг опрацювання даних і встановлюють засоби захисту від незаконної передачі даних.

11 травня 2022 року було прийнято Повідомлення Комісії «Цифрове десятиліття для дітей та молоді: нова європейська стратегія кращого Інтернету для дітей (BIK+)»[2]. Дійсно, при опрацюванні та

[1] The European Data Act. URL: https://www.eu-data-act.com/.

[2] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Decade for Children and Youth: the New European Strategy for a Better Internet for Kids (BIK+). COM/2022/212 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:212:FIN.

захисті персональних даних названої категорії осіб варто звернути увагу на особливі правила та додаткові гарантії, які на них розповсюджуються. Стратегія BIK+ констатує, що цифрові служби постійно збирають і обмінюються даними про дітей, а «датафікація» починається ще до народження . Хоча агреговані великі дані можуть дозволити отримати новаторську інформацію, наприклад, щодо здоров'я та освіти дітей, дані про дитинство також можуть мати потенційно несприятливий вплив на благополуччя та розвиток дітей протягом усього життя. Часто ні діти, ні батьки не усвідомлюють широкого обміну персональними даними, що може виникнути в результаті використання цифрових послуг.

Окремо Стратегія BIK+ наголошує на парадоксальній проблемі, що в той час як бізнес збирає великі масиви даних про дітей при використанні ними цифрових послуг, науковці не мають або мають дуже обмежений доступ до цих важливих наборів даних. У зв'язку з цим Європейська Комісія закликала бізнес надати доступ академічним дослідникам до відповідних даних та інформації про можливості та ризики для дітей у повній відповідності до правил захисту даних; а також співпрацювати з довіреними особами, які позначають інформацію як небезпечну, щоб швидко оцінювати та видаляти незаконний вміст, а також реагувати на сповіщення про шкідливий вміст.

Звісно, додатковий захист дітей встановлюється й іншими актами ЄС. Так, стаття 28 Закону про цифрові послуги[1], яка має назву «Онлайн захист неповнолітніх», передбачає, що постачальники онлайн-платформ не повинні розміщувати рекламу на основі профілювання з використанням особистих даних одержувача послуги, якщо вони з достатньою впевненістю знають, що одержувач послуги є неповнолітнім.

15 вересня 2022 року Європейська Комісія представила пропозицію щодо Закон про захист від кібернетичної активності (Cyber

[1] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065.

Resilience Act)[1]. Ця пропозиція підвищить прозорість та інформацію для користувачів, у тому числі для тих, хто може бути менш оснащений навичками кібербезпеки. Користувачі також будуть краще поінформовані про ризики, можливості та обмеження продуктів із цифровими елементами, що дасть їм змогу вжити необхідних профілактичних заходів і заходів для зменшення залишкових ризиків. Серед основних вимог щодо кібербезпеки інтерес представляють вимоги, що стосуються властивостей продуктів із цифровими елементами, зокрема забезпечення того, щоб такі продукти: захищали конфіденційність отриманих даних (персональних чи інших), наприклад, шляхом шифрування у стані спокою або під час передачі за допомогою найсучасніших механізмів; захищали цілісність збережених, переданих або іншим чином опрацьованих даних, особистих чи інших, команд, програм і конфігурації від будь-яких маніпуляцій або модифікацій, не дозволених користувачем, а також повідомляли про пошкодження; опрацьовували лише дані (персональні чи інші), які є адекватними, релевантними та обмеженими згідно того, що є необхідним для запланованого використання продукту (принцип «мінімізації даних»).

19 вересня 2022 року презентовано Надзвичайний інструмент єдиного ринку (SMEI)[2]. Ці рамки кризового управління мають на меті зберегти належне функціонування внутрішнього ринку ЄС навіть за кризових умов, як COVID-19 чи вторгнення Росії в Україну. Серед засобів, що пропонуються SMEI та стосуються вільного руху даних, можна виокремити: створення архітектури кризового управління для

[1] State of the Union: New EU cybersecurity rules ensure more secure hardware and software products. Press release, 15 September 2022. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5374.

[2] Crisis-proofing the Single Market: equipping Europe with a robust toolbox to preserve free movement and availability of relevant goods and services. Press release, 19 September 2022. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5443; Proposal for a Regulation of the European Parliament and of the Council Establishing a Single Market Emergency Instrument and Repealing Council Regulation No (EC) 2679/98. URL: https://single-market-economy.ec.europa.eu/system/files/2022-09/COM_2022_459_1_EN_ACT_part1_v12.pdf.

єдиного ринку (зокрема моніторинг та обмін даними); пропонування нових засобів для усунення загроз для єдиного ринку (зокрема моніторинг ланцюгів постачання визначених стратегічно важливих товарів і послуг); а також крайні заходи в надзвичайних ситуаціях (зокрема надсилання обов'язкових адресних інформаційних запитів суб'єктам господарювання). Як елемент архітектури кризового управління була також утворена Консультативна група (Advisory Group), що має статус «центрального органу» та відповідно до частини 5 статті 4 SMEI допомагає Європейської Комісії із забезпеченням стабільності єдиного ринку у наступних завданнях: встановлення факту загрози та її обсягу, якщо вона може призвести до порушення постачання товарів і послуг стратегічного значення та перерости у надзвичайну ситуацію на єдиному ринку протягом шести місяців; збір прогнозування, аналіз даних та аналітика ринку; консультації з представниками економічних операторів, включаючи МСП та промисловості для аналітики ринку; сприяння обміну інформацією, у тому числі з іншими відповідними органами та іншими органами, що мають відношення до кризи, на рівні Союзу, а також третіми країнами, у відповідних випадках, приділяючи особливу увагу країнам, що розвиваються, та міжнародним організаціям.

1 листопада 2022 року набрав чинності Закон про цифрові ринки (Digital Markets Act або DMA)[1]. DMA встановлює набір вузько визначених об'єктивних критеріїв для кваліфікації великої онлайн-платформи як так званого «привратника» або «гейткіпера» (gatekeeper). Основною метою цього акту є забезпечення чесної конкурентної поведінки цих діючих осіб в Інтернеті, оскільки вони можуть створювати значні перешкоди для нових гравців ринку та гальмувати інновації й економічний розвиток – зокрема й через контролювання великих наборів даних. Відповідно до загальних вимог, описаних у частині 1 статті 3 DMA, підприємство кваліфікується як гейткіпер, якщо воно: 1) має значний вплив на внутрішній ринок; 2) надає «осно-

[1] The Digital Markets Act: ensuring fair and open digital markets. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

вну послугу платформи», яка виступає в якості важливого шлюзу (вузьке місце) для бізнес-користувачів, щоб досягти кінцевих користувачів; 3) займає міцне становище у своїй діяльності, або можна передбачити, що воно матиме таке становище у найближчому майбутньому.

Очевидно, що гейткіпери отримують вигоду від доступу до великої кількості даних, які вони збирають, надаючи основні послуги платформи, а також інші цифрові послуги. Щоб гарантувати, що гейткіпери не підривають конкурентоспроможність основних платформних послуг або інноваційний потенціал динамічного цифрового сектору, користувачам слід надати ефективний і негайний доступ до даних, які вони надали або які було згенеровано в результаті їх діяльності на відповідних основних службах платформи гейткіпера. Гейткіпери також повинні забезпечити, за допомогою відповідних та високоякісних технічних заходів, таких як інтерфейси прикладного програмування, щоб кінцеві користувачі або треті сторони, авторизовані кінцевими користувачами, могли вільно переносити дані безперервно та в режимі реального часу. Крім того, гейткіпер не повинен використовувати будь-які договірні чи інші обмеження, щоб перешкодити користувачам отримати доступ до відповідних даних.

10 листопада 2022 року Європейська Комісія та Високий представник презентували Спільне повідомлення про політику ЄС у сфері кіберзахисту[1] та План дій щодо військової мобільності 2.0 для вирішення проблеми безпеки, що погіршилася після агресії Росії проти України. Загалом зазначене Повідомлення приділило мало уваги питанню захисту та опрацювання даних. Втім була відмічена важливість спільного запобігання та виявлення атак на ранніх стадіях за допомогою обміну даними. Зазначається, що «дані виявлення» («detection data») мають бути перетворені на ефективний інструмент розвідки, який може служити як кібербезпеці, так і кіберзахисту. Така співпраця між оборонними та цивільними кіберспільнотами має

[1] Cyber Defence: EU boosts action against cyber threats. Press release, 10 November 2022. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6642.

стати основою для покращеної загальної обізнаності про ситуацію у кіберпросторі, і вона однаково важлива для скоординованого реагування на кризу як на технічному, так і на оперативному рівні. В якості інфраструктури для покращення колективної взаємодії було утворено систему з національних і транскордонних операційних центрів безпеки (Security Operations Centres або SOC). Передбачається, що ці SOCs, серед іншого, будуть використовувати останні досягнення технологій штучного інтелекту для проведення аналітики даних, що охоплюють цивільні комунікаційні мережі.

16 листопада 2022 року набув чинності Закон про цифрові послуги[1] (Digital Service Act або DSA). DSA, розроблений як єдиний уніфікований набір правил ЄС для надання цифрових послуг, має за мету надати користувачам підвищений захист, а підприємствам – юридичну визначеність на всьому єдиному ринку. Даний акт має застосовуватися до всіх цифрових послуг, які підключають споживачів до товарів, послуг або контенту. Він створює принципово нові зобов'язання для онлайн-платформ щодо зменшення шкоди та протидії ризикам онлайн та розміщує цифрові платформи під новою системою прозорості та підзвітності. А одним з найбільш характерних ознак DSA стало виведення понять «дуже великих онлайн-платформ» та «дуже великих онлайн-пошукових систем».

Так, відповідно до пункту «е» частини 2 статті 34 DSA «Оцінка ризику», постачальники «дуже великих онлайн-платформ» і «дуже великих онлайн-пошукових систем» повинні враховувати, зокрема, чи впливають практики постачальника, пов'язані з даними, на системні ризики. Оцінки також підлягає, чи впливають на ризики навмисні маніпуляції з їхніми послугами, включно з неавтентичним використанням або автоматизованим використанням послуг, а також потенційно швидке та широке розповсюдження незаконного контенту та інформації, несумісних з їхніми умовами. Відповідно до частини 3 статті 40 DSA, постачальники дуже великих онлайн-платформ

[1] Digital Services Act: EU's landmark rules for online platforms enter into force. Press release, 16 November 2022. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6906.

або дуже великих онлайн-пошукових систем повинні на запит Координатора цифрових послуг установи або Європейської Комісії, пояснити дизайн, логіку, функціонування та тестування їхніх алгоритмічних систем, включаючи системи рекомендацій. Така вимога може включати, наприклад, дані, необхідні для оцінки ризиків і можливої шкоди, заподіяної системою, дані про точність, функціонування та тестування алгоритмічних систем для модерування вмісту, системи рекомендацій або рекламні системи, включаючи, якщо це доцільно, навчальні дані та алгоритми, або дані про процеси та результати модерації вмісту або внутрішніх систем опрацювання скарг.

Серед іншого, пункт 98 Преамбули DSA роз'яснює, що в тому разі, коли дані є загальнодоступними (наприклад про сукупну взаємодію з вмістом загальнодоступних сторінок, публічних груп або публічних діячів, включаючи дані про враження та залучення, такі як кількість реакцій, поширень, коментарів), постачальники не повинні перешкоджати дослідникам використовувати ці дані для дослідницьких цілей, які сприяють виявленню, ідентифікації та розумінню системних ризиків. Так, пункт 8 статті 40 DSA закріплює, що за належним чином обґрунтованим зверненням дослідників, координатор цифрових послуг установи надає таким дослідникам статус «перевірених дослідників» для конкретного дослідження, зазначеного в заяві, і надсилає вмотивований запит на доступ до даних постачальнику дуже великих онлайн-платформи або дуже великої онлайн-пошукової системи.

23 лютого 2023 року Європейська Комісія представляє нові ініціативи, закладаючи основу для трансформації сектору підключення в ЄС[1]. Серед іншого, було запропоновано Закону про гігабітну інфраструктуру, що має замінити Директиву про скорочення витрат на широкосмуговий доступ та враховує такі сучасні технології, як: штучний інтелект, хмарні послуги, простори даних, віртуальна реальність і метавсесвіт, в яких європейські громадяни користуються своїми цифровими правами.

[1] Commission presents new initiatives, laying the ground for the transformation of the connectivity sector in the EU. Press release, 23 February 2023. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_985.

29 березня 2023 року Європейська Комісія опублікувала Пропозицію щодо «Директиви про подальше розширення та вдосконалення використання цифрових інструментів і процесів у праві компаній»1. Дана пропозиція має на меті підвищити прозорість та зменшити бюрократичні процедур для компаній, щоб покращити бізнес-середовище в ЄС. Варто відзначити, що дана Директива стосується переважно врегулювання відносин навколо фізичної інфраструктури передачі даних, а не щодо відносин з їх опрацювання чи захисту. Було відзначено, що для швидкого розвитку цифрових технологій, таких як метавсесвіт, штучний інтелект (ШІ), квантові обчислення, доповнена та віртуальна реальність, необхідні значні інвестиції у мережу (зокрема гігабітні мережі, включаючи розгортання оптоволокна та 5G), щоб не відставати від зростаючих потреб у пропускній здатності. Хоча питання фізичних інфраструктур дещо виходить за межі даної роботи, може виявитися доречним проаналізувати спрощення бюрократичних процедур у подальших дослідженнях: наприклад, заходи, що полегшать операторам повторне використання громадської інфраструктури, такої як канали або щогли, і простору, наприклад даху, для встановлення мережевої інфраструктури.

18 квітня 2023 року Європейська Комісія пропонує Акт про кіберсолідарність ЄС для зміцнення потенціалу кібербезпеки в ЄС[1]. На національному рівні моніторинг, виявлення та аналіз кіберзагроз зазвичай забезпечують Security Operations Centres (SOC) державних і приватних організацій у поєднанні з комп'ютерними групами реагування на надзвичайні ситуації (CSIRT). Крім того, CSIRT обмінюються інформацією в контексті мережі CSIRT відповідно до Директиви (ЄС) 2022/2555. Транскордонні SOC спрямовані на розширення можливостей та доповнення мережі CSIRT шляхом об'єднання та обміну даними про загрози кібербезпеці від державних і приватних організацій, підвищення цінності таких даних за допомогою експерт-

[1] Cyber: towards stronger EU capabilities for effective operational cooperation, solidarity and resilience. Press release, 18 April 2023. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2243.

ного аналізу, а також спільного використання інфраструктур і сучасного рівня техніки. Суб'єкти, які беруть участь у Європейському «кіберщиті», повинні забезпечувати високий рівень взаємодії між собою, включаючи, за необхідності, уніфікації форматів даних, таксономії, інструментів опрацювання та аналізу даних, безпечних каналів зв'язку тощо. Шляхом збору, спільного використання та обміну даними Європейський «кіберщит» має посилити технологічний суверенітет Союзу, а об'єднання високоякісних підібраних даних також має сприяти розвитку передових технологій штучного інтелекту та аналізу даних. Додатково цьому має сприяти з'єднання Європейського кіберщита з пан'європейською інфраструктурою високопродуктивних обчислень.

25 квітня 2023 року Європейська Комісія визначає перший набір дуже великих онлайн-платформ та пошукових систем відповідно до Закону про цифрові послуги. До першої категорії були віднесені: Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, Zalando. До другої – Google та Bing[1].

Весна 2023-го року відзначилася також прийняттям ряду документів, що спрямовані на покращення регулювання сфери інтелектуальної власності. Так, 27 квітня 2023 року Європейська Комісія запропонувала узгоджені патентні правила ЄС для стимулювання інновацій, інвестицій і конкурентоспроможності[2]. А 4 травня 2023 року Європейською Комісією було прийнято Рекомендацію щодо того, як боротися з комерційним онлайн-піратством спортивних та інших подій у прямому ефірі[3], й у той же день – Рекомендацію щодо

[1] Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines. Press release, 25 April 2023. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413.

[2] Intellectual property: harmonised EU patent rules boost innovation, investment and competitiveness in the Single Market. Press release, 27 April 2023. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2454.

[3] Commission recommends actions to combat online piracy of sports and other live events. Press release, 4 May 2023. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2508.

боротьби з онлайн-піратством спортивних та інших подій у прямому ефірі[1].

13 вересня 2023 року було прийнято Регламент (ЄС) 2023/1781 «Про встановлення основних заходів для зміцнення європейської напівпровідникової екосистеми», яким встановлено основу для зміцнення напівпровідникової екосистеми на рівні ЄС, зокрема за допомогою таких заходів: заснування Ініціативи «Чіпи для Європи» («Ініціатива»); встановлення критеріїв для визнання та підтримки інтегрованих виробничих потужностей і відкритих ливарних підприємств ЄС, які є першими у своєму роді потужностями та сприяють безпеці постачання та стійкості напівпровідникової екосистеми ЄС; створення координаційного механізму між державами-членами та Європейською Комісією для картографування та моніторингу напівпровідникового сектору ЄС, а також для запобігання кризовим ситуаціям і реагування на дефіцит напівпровідників і, у відповідних випадках, консультування зацікавлених сторін із напівпровідникового сектору. Першою загальною метою цього Регламенту є забезпечення умов, необхідних для конкурентоспроможності та інноваційної спроможності ЄС та забезпечення пристосування галузі до структурних змін. Другою загальною метою, окремою від першої загальної мети, викладеної в параграфі 2, і такою, що доповнює її, є покращення функціонування внутрішнього ринку шляхом встановлення єдиної правової бази ЄС для підвищення стійкості ЄС та безпеки постачання в області напівпровідникових технологій[2].

[1] Commission recommends actions to combat online piracy of sports and other live events. Press release, 4 May 2023. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2508.

[2] Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe's semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act). URL: http://data.europa.eu/eli/reg/2023/1781/oj.

## 4.7. Переваги Єдиного цифрового ринку в контексті опрацювання та вільного руху даних

Підприємства в Європейському Союзі сьогодні базують значну частину своєї діяльності на «потоках даних», які, завдяки швидкому технологічному прогресу та оцифровці, є незамінними для виявлення нових економічних можливостей. Втім національні спроможності окремих держав не є достатніми, щоб скористатися усіма перевагами стрімких змін та впоратися з їх викликами. Намагання впровадити внутрішнє регулювання без будь-якого узгодження з іншими державами призводить лише до фрагментації цифрових ринків та створення зайвих регуляторних перешкод. Враховуючи, що цифрові ринки мають транскордонний характер, національні законодавці повинні враховувати, що належне функціонування таких ринків неможливе без вільного руху даних між державами. Отже, найбільший потенціал матимуть ті суб'єкти, що вчасно змогли акумулювати власні потужності для співпраці.

Успішним прикладом такої співпраці на рівні ЄС став процес інтеграції до Єдиного цифрового ринку. Він, серед іншого, передбачає побудову таких умов, де всі компанії, що пропонують свої товари чи послуги в Європейському Союзі, підпадають під однакові правила щодо захисту даних і споживачів, незалежно від того, де базується їхній сервер.

Стратегія єдиного цифрового єдиного ринку для Європи від 6 травня 2015 р.[1], що й запровадила дане поняття, проголосила ціль зламати національні розбіжності у регулюванні телекомунікацій, в управлінні радіохвилями, у застосуванні законодавства про конкуренцію та у законодавстві про авторське право та захист даних. Й, хоча за своєю сутністю ця стратегія є політичним документом, її зна-

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions a Digital Single Market Strategy for Europe. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192.

чення не може бути применшене через подальшу нормативно-правову роботу з інтеграції цифрових ринків країн-членів ЄС.

Хоча регулювання захисту даних є лише одним з напрямів інтеграції, термін «дані» («data») вживається у ньому близько 70 разів, що може свідчити про значення належного регулювання даних для діяльності Єдиного цифрового ринку. Структурно даний документ складається з шести розділів: 1. Вступ; 2. Шляхи покращення онлайн-доступу для споживачів та компаній; 3. Створення належних умов і рівних умов для передових цифрових мереж та інноваційних послуг; 4. Максимальне використання потенціалу зростання цифрової економіки; 5. Створення єдиного цифрового ринку; 6. Висновок. Так чи інакше, реалізація більшості з пунктів окреслених розділів буде вимагати відповідного врегулювання опрацювання та захисту даних (як, наприклад, у випадку з пунктом 2.3 щодо запобігання необґрунтованому геоблокуванню, яке стає унеможливленим у разі впровадження транскордонних принципів вільного руху даних). Втім особливо відмітити варто пункти 3.4 та 4.1, про які мова піде далі.

Пункт 3.4 Стратегії єдиного цифрового єдиного ринку для Європи прямо передбачає зміцнення довіри та безпеки до цифрових послуг і опрацювання персональних даних. Зазначається, що кіберзагрози за своєю природою є проблемами без кордонів та негативно впливають на економіку, фундаментальні права громадян і суспільство в цілому. У зв'язку з цим регулювання кібербезпеки має відбуватися не лише на національному рівні, а й на рівні ЄС. Документом, що стосується цього питання, є Директива (ЄС) 2016/1148 Європейського Парламенту та Ради від 6 липня 2016 року про заходи щодо високого спільного рівня безпеки мережевих та інформаційних систем у всьому Союзі[1].

Так, Директива 2016/1148 визнає, що мережні та інформаційні системи та послуги відіграють життєво важливу роль у суспільстві.

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016L1148.

Їх надійність і безпека є важливими для економічної та суспільної діяльності, і зокрема для функціонування внутрішнього ринку. Такі системи, і в першу чергу Інтернет, відіграють важливу роль у полегшенні транскордонного руху товарів, послуг і людей. Їх транснаціональна природа також означає, що збої та ризики в межах одної системи можуть вплинути на безліч суб'єктів з різних держав.

З метою подолання існуючих проблем, зокрема недостатньої та фрагментарної урегульованості, частина 2 статті 1 Директиви 2016/1148 передбачає перелік конкретних дій. Так, пункт «a» встановлює зобов'язання для всіх держав-членів прийняти національну стратегію щодо безпеки мережевих та інформаційних систем; пункт «b» передбачає створення «Групи Кооперації» з метою сприяння стратегічній співпраці та обміну інформацією; пункт «c» створює мережу груп реагування на інциденти комп'ютерної безпеки («мережа CSIRTs»); пункт «d» встановлює вимоги щодо безпеки та сповіщення для операторів основних послуг і для постачальників цифрових послуг; а пункт «e» встановлює зобов'язання держав-членів призначати національні компетентні органи, єдині контактні пункти та CSIRTs із завданнями, пов'язаними з безпекою мережевих та інформаційних систем.

Роль Національної стратегії щодо безпеки мережевих та інформаційних систем в Україні виконує Стратегія кібербезпеки України[1]. В тексті документу відзначається, що нова Стратегія кібербезпеки України враховує попередній досвід і проблеми, стан кібербезпекового середовища на національному та міжнародному рівні, а також положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегій кібербезпеки окремих держав-членів ЄС та держав-членів НАТО.

Щодо вимоги утворення «CSIRTs network», то Україна не може приєднатися до цієї мережі, оскільки до неї входять виключно країни-

[1] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n7.

члени ЄС[1]. Однак наша держава має національні групи реагування на інциденти комп'ютерної безпеки, що у майбутньому й мають інтегруватися до європейської мережі. Більш того, пункт 8 частини 3 статті 8 Закону України «Про основні засади забезпечення кібербезпеки України» прямо передбачає, що функціонування національної системи кібербезпеки забезпечується шляхом розвитку мережі команд реагування на комп'ютерні надзвичайні події[2]. Один з таких CSIRTs утворено в якості позаштатної структурної одиниці ДержНДІ технологій кібербезпеки[3], а ще один функціонує у складі Центру кіберзахисту Національного банку під назвою CSIRT-NBU[4].

Варто відзначити, що такі команди є необхідними для забезпечення інформаційного захисту, але разом з тим можуть наділятися занадто широкими повноваженнями, що навпаки ставить безпеку даних (перш за все, їх конфіденційність) під загрозу. Так, наприклад, Розпорядження НЦУ від 30.01.2023 р. № 67/850 «Про впровадження системи фільтрації фішингових доменів» отримало численні зауваження з боку інтернет-спільноти та юристів, що зрештою призвело до перегляду редакції та залучення пропозицій з боку Інтернет Асоціації України (ІнАУ) до РНБО.

Створення цієї системи було ініційовано НБУ, а 30 січня 2023 року Національним центром оперативно-технічного управління мережами телекомунікацій Державної служби спеціального зв'язку та захисту інформації України було ухвалено відповідне розпорядження[5]. У зв'язку з цим станом на 2 березня 2023 року всі українські провай-

[1] CSIRTs Network Members. URL: https://csirtsnetwork.eu/.

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

[3] Про CSIRT (Computer Security and Incident Response Team) Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації. URL: https://csirt.csi.cip.gov.ua/uk/pages/about-csirt.

[4] Центр кіберзахисту Національного банку України. URL: https://csirt.bank.gov.ua/.

[5] Розпорядження НЦУ від 30.01.2023 № 67/850 про впровадження системи фільтрації фішингових доменів. URL: https://nkrzi.gov.ua/index.php?r=site%2Findex&pg=99&id=2580&language=uk&fbclid=IwAR2UvAuj-EqS3jbUlDkQxQ8HQvM1Ow2tJrKk6KcwJK_H-sLTtqYcy9z_-mw.

дери були зобов'язані підключитися до системи, через яку CSIRT-NBU мала керувати боротьбою з фішингом. І, хоча система декларувалася для протидії фішингу, вона мала технічну можливість бути використаною для автоматичного блокування необмеженої кількості інтернет-ресурсів без судового рішення. Критиці було піддано цілий ряд недоліків: від сумнівності причин для збору персональних даних громадян на серверах РНБО до відсутності у вітчизняному законодавстві визначення поняття «фішинг», що взагалі нівелює критерії блокування сайтів. При чому, якщо раніше блокування сайту вимагало рішення суду, яке можна було оскаржити, то за нової системи воно мало відбуватися миттєво та без залучення судової влади[1].

Початкова концепція системи передбачала, що кожні 15 хвилин на сервер провайдера зі вказаного в Розпорядженні ресурсу автоматично завантажується перелік інтернет-адрес для автоматичного блокування (стоп-лист). У той же час інформація про користувача, який намагався зайти на «заборонені» ресурси, мала автоматично фіксуватися і передаватися до відповідних державних органів. У зверненні ІнАУ наголосила, що це є фактичним створенням централізованого механізму автоматичного блокування доступу користувачів до необмеженого переліку інтернет-ресурсів, а негативні наслідки для України в разі отримання ворогом доступу до цього механізму важно переоцінити[2]. Звісно, що в майбутньому такі ініціативи повинні піддаватися поміркованому аналізу та контролю з боку юристів, провайдерів, ІТ-експертів та інших зацікавлених сторін, включно з громадськістю.

Пункт 4.1 Стратегія єдиного цифрового єдиного ринку для Європи присвячено «Побудові економіки даних». Визнається, що дані все

[1] Яковлева М. Матриця по-українськи: Нацбанк прагне контролювати вітчизняний інтернет-простір. Веб-сайт Mind. 16.05.2023. URL: https://mind.ua/publications/20254832-matricya-po-ukrayinski-nacbank-pragne-kontrolyuvati-vitchiznyanij-internet-prostir.

[2] В Україні створюється «троянський кінь» - централізована система автоматичного блокування інтернет-ресурсів. Веб-сайт Інтернет Асоціації України. 28.02.2023. URL: https://inau.ua/news/novyny-inau/v-ukrayini-stvoryuyetsya-troyanskyy-kin-tsentralizovana-systema-avtomatychnoho.

частіше розглядаються як каталізатор економічного зростання, інновацій та оцифрування в усіх секторах економіки, особливо для МСП (і стартапів) та для суспільства в цілому. Особливий вплив справляють й «великі дані» та високопродуктивні обчислення, що змінюють спосіб проведення досліджень і обміну знаннями в рамках переходу до більш ефективної та чутливої«Відкритої науки». Окрім того, знов наголошується, що фрагментований ринок не забезпечує достатнього масштабу для того, щоб хмарні обчислення, великі дані, наука, що керується даними, та Інтернет речей повністю розкрили свій потенціал у Європі.

Існує цілий перелік перешкод, вирішення яких ставиться за мету в контексті пункту 4.1 Стратегії цифрового єдиного ринку для Європи. По-перше, обмеження щодо локалізації даних, тобто вимоги держав-членів зберігати дані на своїй території, змушують постачальників послуг будувати дорогу місцеву інфраструктуру (таку як центри опрацювання даних) у кожному регіоні чи країні.

По-друге, фрагментована імплементація правил авторського права та відсутність ясності щодо прав на використання даних ще більше перешкоджають розвитку транскордонного використання даних і нових технологій (наприклад, інтелектуальний аналіз тексту та даних);

По-третє, відсутність відкритих і сумісних систем і послуг, а також переносимості даних між службами є ще одним бар'єром для транскордонного потоку даних і розвитку нових послуг (наприклад, мультимодальних інформаційних систем подорожей або наукових досліджень, що керуються даними).

По-четверте, подолання юридичної невизначеності щодо розподілу відповідальності є важливою для розгортання Інтернету речей.

По-п'яте, прийняття пакету реформ щодо захисту даних у хмарі має забезпечити підвищення довіри споживачів до хмарних послуг. Проте контракти часто виключають або суворо обмежують договірну відповідальність постачальника хмарних послуг, якщо дані більше не доступні або непридатні для використання, або вони ускладнюють розірвання контракту.

По-шосте, має бути вирішено питання мобільності даних, та усунуті будь-які непотрібні обмеження щодо розміщення даних у межах ЄС.

## 4.8. Нормативно-правова база України щодо даних та ступінь її адаптації до вимог ЄС

Нормативно-правову базу України з питань регулювання захисту та вільного руху даних складають такі Закони: «Про інформацію», «Про електронні довірчі послуг», «Про електронні документи та електронний документообіг», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про стандартизацію», «Про технічні регламенти та оцінку відповідності», «Про наукову і науково-технічну експертизу», «Про захист персональних даних», «Про авторське право і суміжні права», «Про основні засади забезпечення кібербезпеки України».

Стратегією здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року[1] була проголошена Стратегічна ціль 1 «Централізація управління ІТ шляхом впровадження єдиних ІТ-стандартів, розбудова Єдиної інформаційно-телекомунікаційної системи системи управління державними фінансами». Серед завдань, передбачених для реалізації цієї стратегічної цілі визначено: «створення єдиного сховища даних Мінфіну […] шляхом інтеграції інформаційних ресурсів митної, податкової сфер та сфери казначейського обслуговування бюджетних коштів з подальшою інтеграцією з іншими державними інформаційними ресурсами, зокрема державними реєстрами»; а також «забезпечення надійного захисту інформації, в тому числі

[1] Стратегія здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року: схвалено розпорядженням Кабінету Міністрів України від 17 листопада 2021 р. № 1467 р. URL: https://zakon.rada.gov.ua/laws/show/1467-2021-%D1%80#n15.

персональних даних». Даний акт представляє цінність й через впровадження комплексної системи принципів, що розподілені на умовні групи: принципи у сфері бізнес-логіки інформаційних систем; у сфері архітектури інформаційних систем; у сфері IT-управління; у сфері технічної інфраструктури; у сфері кіберзахисту.

Можна констатувати, що Україна здійснила ряд кроків для інтеграції до Єдиного цифрового ринку ЄС. Так, зокрема, було прийнято Закон України «Про електронні довірчі послуги», а відповідними постановами Кабінету Міністрів України було затверджено вимоги у сфері електронних довірчих послуг[1] та Порядок взаємного визнання українських та іноземних сертифікатів відкритих ключів, електронних підписів[2].

Одна з минулих робіт автора[3], написана у 2021-му році, відзначала ряд проблем, які Україні ще належало подолати для подальшої інтеграції до Єдиного цифрового ринку ЄС (зокрема й в контексті регулювання даних). Незважаючи на складні умови воєнного часу, частина цих проблем була розв'язана у останні роки. Наприклад, в згаданих тезах була відмічена уповільненість укладення двосторонньої угоди про взаємне визнання електронних довірчих послуг між Україною та ЄС. Втім наразі Україна та ЄС взаємно визнають електро-

[1] Про затвердження вимог у сфері електронних довірчих послуг та порядку перевірки дотримання вимог законодавства у сфері електронних довірчих послуг: Постанова КМУ від 07.11.2018 р. № 992. URL: https://zakon.rada.gov.ua/laws/show/992-2018-%D0%BF#Text.

[2] Про затвердження Порядку взаємного визнання українських та іноземних сертифікатів відкритих ключів, електронних підписів, а також використання інформаційно-телекомунікаційної системи центрального засвідчувального органу для забезпечення визнання в Україні електронних довірчих послуг, іноземних сертифікатів відкритих ключів, що використовуються під час надання юридично значущих електронних послуг у процесі взаємодії між суб'єктами різних держав: Постанова КМУ від 23.01.2019 р. № 60. URL: https://zakon.rada.gov.ua/laws/show/60-2019-%D0%BF#Text.

[3] Мамаєв І. О. Аналіз готовності України та українського суспільства до інтеграції у єдиний цифровий ринок ЄС. *Збірник наукових праць НДІ ПЗІР НАПрН України. Вип. 5: Цифрові трансформації України 2021*: виклики та реалії: за матеріалами II круглого столу (м. Харків, 20 вересня 2021 року). Харків: НДІ ПЗІР НАПрН України, 2021. С. 136–147. URL: https://ndipzir.org.ua/wp-content/uploads/2021/Conf_20.09.21/23.pdf.

нні довірчі послуги у зв'язку із набранням чинності постанови Кабінету Міністрів України «Про реалізацію експериментального проекту щодо взаємного визнання електронних довірчих послуг між Україною та Європейським Союзом» від 22 листопада 2022 р.[1]. Тим самим взаємного визнання отримали: 1) іноземні кваліфіковані електронні довірчі послуги, а також результати надання таких послуг, зокрема кваліфіковані електронні підписи, що надаються кваліфікованими надавачами електронних довірчих послуг у державах-членах ЄС та інших державах-членах Європейської економічної зони, що включені в Список довірчих списків Європейського Союзу; 2) засоби для створення кваліфікованого електронного підпису, сертифіковані відповідними державними або приватними органами, що призначені державами – членами ЄС та включені до відповідного переліку сертифікованих засобів; 3) електронні підписи, створені в державах, що забезпечують належний захист персональних даних, перелік яких наведений у додатку до постанови Кабінету Міністрів України від 16 серпня 2022 р. № 910 «Деякі питання передачі персональних даних за межі України засобами Єдиного державного вебпорталу електронних послуг»[2].

Окрім того, гострою проблемою було названо порушення прав інтелектуальної власності. Так, щорічна доповідь Єврокомісії 2021-го року щодо захисту та забезпечення прав інтелектуальної власності у третіх країнах віднесла нашу державу до «другого пріоритету» за масштабами порушень та їх наслідками (при цьому «перший пріоритет» отримав лише Китай). Патентне законодавство України було визнано таким, що не відповідає міжнародним нормам. Критиці було піддане регулювання у сфері товарних знаків, авторських та суміжних

[1] Про реалізацію експериментального проекту щодо взаємного визнання електронних довірчих послуг між Україною та Європейським Союзом: Постанова КМУ від 22.11.2022 р. № 1311. URL: https://zakon.rada.gov.ua/laws/show/1311-2022-%D0%BF#Text.

[2] Деякі питання передачі персональних даних за межі України засобами Єдиного державного вебпорталу електронних послуг: Постанова Кабінету Міністрів України від 16.08.2022 р. № 910. URL: https://zakon.rada.gov.ua/laws/show/910-2022-%D0%BF#Text.

прав, сортів рослин. Проблемними сферами залишаються також онлайн-піратство та фальсифікація лікарських засобів. У той же час у щорічній доповіді Європейської Комісії за 2023-й рік[1], Україна не була віднесена до жодного з трьох пріоритетів. Для виправлення ситуації, зокрема, в Україні з 01.12.2022 році набрав чинності Закон України № 2811-IX «Про авторське право і суміжні права»[2], що скасував аналогічний застарілий Закон від 23.12.1993 р. № 3792-XII.

Відповідно до останніх публікацій прес-служби Апарату Верховної Ради України[3], інтеграція до Єдиного цифрового ринку ЄС лишається незмінним пріоритетом для України. Відзначається, що для досягнення цієї мети вже було прийнято Закон України «Про електронні комунікації», розроблений згідно з Кодексом електронних комунікацій ЄС та «Про електронну ідентифікацію та електронні довірчі послуги», спрямований на імплементацію норм Регламенту (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року. Також здійснюється розробка підзаконних нормативно-правових актів на виконання цих Законів. Крім того, в серпні 2023-го року було прийнято й Закон України «Про цифровий контент та цифрові послуги»[4], що спрямований на імплементацію європейських підходів до регулювання цифрових ринків та забезпечить безпечне і надійне онлайн-середовище, конкурентні і справедливі умови діяльності для всіх учасників ринків цифрових послуг, захист прав і законних інтересів користувачів.

Для демонстрації прикладу перенесення європейських норм у вітчизняне законодавство автором укладена Порівняльна таблиця

[1] Commission releases its Report on Intellectual Property Rights in Third Countries. 17 May 2023. URL: https://policy.trade.ec.europa.eu/news/commission-releases-its-report-intellectual-property-rights-third-countries-2023-05-17_en.

[2] Про авторське право і суміжні права: Закон України від 01.12.2022 р. № 2811-IX. URL: https://zakon.rada.gov.ua/laws/show/2811-20.

[3] Єдиний цифровий ринок та інші програми цифрового співробітництва з ЄС - Комітет з питань цифрової трансформації. Прес-служба Апарату Верховної Ради України. 18 липня 2023. URL: https://www.rada.gov.ua/news/news_kom/239177.html.

[4] Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text.

Директиви (ЄС) 2019/770 та Закону України «Про цифровий контент та цифрові послуги», що наводиться наприкінці.

Важливим актом стало прийняття Закон України «Про електрону комерцію». Комплексні зміни отримала сфера телекомунікацій: початково був ухвалений Закон України щодо внесення змін до Закону України «Про електронні телекомунікації» у частині посилення незалежності та адміністративної спроможності національного регулятора. Згодом був розроблений, затверджений та зареєстрований в Мін'юсті Порядок та методика здійснення моніторингу ринку телекомунікаційних послуг[1]. Потім – Кабінет Міністрів України ухвалив постанову щодо внесення змін до Правил надання та отримання телекомунікаційних послуг.

Було розроблено Стратегію інтеграції України до Єдиного цифрового ринку Європейського Союзу: виклики, можливості та бар'єри[2] та План заходів щодо її імплементації («Дорожня карта»). Стратегією, зокрема, були передбачені Рекомендації щодо інтеграції України до Єдиного цифрового ринку Європейського Союзу; Рекомендації щодо створення в Україні належних умов розвитку цифрових мереж та послуг; та Рекомендації щодо розвитку цифрової економіки.

Окрім того, Україна приєдналася до додаткового протоколу до конвенції про договір міжнародного автомобільного перевезення вантажів про електронну накладну[3], що має спрощувати експортні процедури.

На додаток до нормативно-правової роботи, варто відзначити й неправові заходи, що проводилися в межах виконання зобов'язань

[1] Про затвердження Порядку здійснення моніторингу якості електронних комунікаційних послуг: зареєстровано ареєстровано в Міністерстві юстиції України від 19 жовтня 2023 р. № 1830/40886. URL: https://ips.ligazakon.net/document/RE40886?an=1.

[2] Стратегія Інтеграції України до ЄЦР: https://eu-ua-csp.org.ua/media/uploads/Integration%20to%20EU%20DSM_Ukr%20side_UA.pdf.

[3] Про приєднання україни до додаткового протоколу до конвенції про договір міжнародного автомобільного перевезення вантажів (кдпв) про електронну накладну: Закон України від 03.06.2020 р. № 660-IX. URL: https://zakon.rada.gov.ua/laws/show/660-20#Text.

за євроінтеграційними процесами. Серед них соціологічне дослідження цифрових навичок громадян, ініційоване Міністерством цифрової трансформації України. В основі визначення рівня володіння цифровими навичками була покладена методологія Індексу цифрової економіки та суспільства (DESI), що підсумовує цифрові показники Європи та відстежує розвиток країн у сфері цифрової конкурентоспроможності.

# 5. ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ВПРОВАДЖЕННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ

## 5.1. Цифрова трансформація фінансових послуг

Цифрова трансформація фінансових послуг принесла значні зміни у фінансову галузь. Щоб забезпечити безпеку та надійність фінансових систем, уряди та регулюючі органи по всьому світу зробили кроки щодо створення правової бази для регулювання фінтех-діяльності.

Інформаційні технології справили значний вплив на фінансовий сектор, що призвело до розробки нових продуктів та послуг, підвищення ефективності та покращення якості обслуговування клієнтів. Серед найпоширеніших прикладів використання інформаційних технологій у фінансовій сфері можна виділити такі[1]:

1. Онлайн-банкінг. З його появою клієнти можуть отримувати доступ до своїх рахунків та проводити транзакції з будь-якого місця та у будь-який час. Вони можуть перевіряти баланс свого рахунку, переказувати кошти, сплачувати рахунки та подавати заявки на кредити онлайн.

2. Мобільний банкінг дозволяє клієнтам отримувати доступ до своїх рахунків за допомогою смартфонів або планшетів. Вони можуть

[1] Єфремова К. В., Новіков Є. А. Цифрова трансформація фінансових послуг. *Інноваційний процес: перспективи євроінтеграції*: матеріали круглого столу (м. Харків, 24 березня 2023 року). Харків: НДІ ПЗІР НАПрН України, 2023. С. 35-41.

здійснювати транзакції, сплачувати рахунки та навіть депонувати чеки за допомогою своїх мобільних пристроїв.

3. Електронні платежі стають все більш популярними, оскільки споживачі використовують дебетові та кредитні картки, мобільні платежі та цифрові гаманці для здійснення покупок.

4. Автоматизована торгівля: фінансові установи використовують алгоритми та штучний інтелект для автоматичної торгівлі акціями та іншими фінансовими інструментами. Це підвищує ефективність та знижує ризик помилок.

5. Технологія блокчейн використовується для створення безпечних, прозорих та захищених від несанкціонованого доступу цифрових реєстрів для фінансових транзакцій. Ця технологія може зробити революцію у способах проведення фінансових транзакцій.

6. Аналітика даних. Фінансові установи використовують аналітику даних для аналізу поведінки клієнтів та прийняття більш обґрунтованих рішень. Вони використовують дані для виявлення потенційного шахрайства, виявлення тенденцій та персоналізації продуктів та послуг для клієнтів.

7. Автоматизація обробки інформації змінила правила гри й у страховому секторі, надавши численні переваги страховим компаніям та їх клієнтам. Так, Автоматизація обробки претензій використовується для раціоналізації процесу претензій, скорочення часу, необхідного для обробки та підвищення точності оцінки претензій. Наприклад, страхові компанії можуть використовувати штучний інтелект для аналізу претензій та визначення їхньої обґрунтованості.

8. Андеррайтинг включає оцінку ризику страхування конкретної особи або організації. Автоматизація використовується для оптимізації цього процесу, що дозволяє страховим компаніям обробляти заявки швидше та точніше.

9. Автоматизація використовується й при обслуговуванні клієнтів. Наприклад, страхові компанії можуть використовувати чат-ботів або автоматизовані телефонні системи для надання клієнтам негайної підтримки та допомоги. Загалом автоматизація обробки інформації відкриває нові можливості страхового сектору, що призводить до

підвищення ефективності, точності та якості обслуговування клієнтів.

Масштаби використання штучного інтелекту (AI) в банківському секторі та в сфері FinTech розширюються, починаючи від послуг, орієнтованих на клієнта (таких, як чат-боти, персоналізований маркетинг), до внутрішніх процесів управління ризиками (наприклад, автоматизація операцій, аналіз контрактів, управління ризиками)[1]. Штучний інтелект добре структурований та підготовлений для зниження загроз шахрайства у сфері фінансів, кількість яких стрімко зростає, боротьби зі зростанням числа кіберзлочинів і розв'язання багатьох інших проблем безпеки банківських установ. Крім того, оцінка кредитних ризиків, що базується на штучному інтелекті (AI) і машинному навчанні (ML), є якіснішою та ефективною. Від регуляторних технологій до роботів-консультантів, системи AI/ML дозволяють компаніям краще контролювати поведінку клієнтів та виявляти можливості для розвитку й аномалії[2].

Проте, Глібком С. В. було проаналізовано інновації у банківській справі і він доходить висновку, що основною проблемою використання банками цифрових технологій є вирішення правових питань щодо співвідношення механізмів патентного захисту технологій та їх масового застосування, вирішення конфлікту публічних і приватних інтересів[3].

Правове регулювання FinTech залежить від кожної окремої держави, але зазвичай воно охоплює такі галузі, як конфіденційність даних, кібербезпека, захист прав споживачів та фінансова стабільність. Різні країни підходять до правового регулювання фінтеху по різному.

---

[1] Єфремова К. В. Особливості застосування штучного інтелекту у сфері фінансових послуг: досвід ЄС. *Право та інноваційне суспільство*. 2020, № 1 (14). С. 61-66. DOI: https://doi.org/10.37772/2309-9275-2020-1(14)-9.

[2] Худолій Ю. С., Свистун Л. А. Сучасні тенденції FinTech та їх вплив на безпеку банківських установ. *Економіка і регіон*. 2021, № 3 (82). С. 115-123. DOI: 10.26906/EiR.2021.3(82).2375.

[3] Glibko S. Problems of Legal Provision of Innovative Banking. *European Political and Law Discourse.* 2016, Vol. 3, Iss. 3. P. 168-173.

У США регулювання фінансових технологій розділене між федеральною владою та владою штатів. Федеральний уряд регулює такі галузі, як боротьба з відмиванням грошей, тоді як регулюючі органи штатів контролюють ліцензування та захист прав споживачів. Комісія з цінних паперів та бірж (SEC) регулює платформи краудфандингу та біржі цифрових активів, а Комісія з торгівлі товарними ф'ючерсами (CFTC) регулює торгівлю цифровими активами та деривативами.

Європейський Союз запровадив нормативну базу під назвою «Директива про платіжні послуги 2» (PSD2)[1], метою якої є підвищення конкуренції та безпеки у платіжній індустрії. Вона вимагає, щоб банки відкривали дані своїх клієнтів стороннім постачальникам через інтерфейси прикладного програмування (API), що дозволяє фінансовим компаніям отримувати доступ до інформації про облікові записи клієнтів та ініціювати платежі.

Китай запровадив спеціальну програму під назвою «План виправлення та розвитку інтернет-фінансів», метою якої є сприяння розвитку фінансових технологій у забезпеченні фінансової стабільності, вимагаючи від фінтех-компаній отримання ліцензій та дотримання суворих правил конфіденційності даних та кібербезпеки.

У Сінгапурі створено нормативну (регуляторну) пісочницю, яка дозволяє фінансовим компаніям, які впроваджують FinTech, тестувати свої продукти та послуги у контрольованому середовищі без необхідності дотримання всіх звичайних нормативних вимог. Це дозволяє їм швидше впроваджувати інновації, забезпечуючи захист споживачів.

Україна використала позитивний досвід різних країн та створила Стратегію розвитку фінтеху в Україні до 2025 року[2], та поступово впроваджує розроблений план дій щодо її реалізації. Так, в 2022 році

[1] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. OJ L 337, 23.12.2015, p. 35–127. URL: http://data.europa.eu/eli/dir/2015/2366/oj.

[2] Стратегія розвитку фінтеху в Україні до 2025 року, затверджена рішенням Правління НБУ від 09.07.2020 р. № 453-рш. URL: https://bank.gov.ua/admin_uploads/article/Strategy_finteh2025.pdf?v=4.

набув чинності Закон України «Про платіжні послуги»[1], який знаменує собою новий розділ у фінансовому середовищі України та його регулюванні. Закон встановлює рамки функціонування та регулювання сучасних фінансових технологій, у тому числі електронних грошей, платіжних мереж та цифрової валюти центрального банку (CBDC) на території України, а також передбачає можливість створення регуляторних пісочниць[2].

В цілому, правове регулювання фінтеху все ще розвивається, і цілком імовірно, що в міру того, як галузь зростатиме та розвиватиметься, ми побачимо більше нормативних рамок.

## 5.2. Економічна безпека України в умовах цифровізації

Стратегічно важливим в умовах цифрової трансформації економіки є забезпечення економічної безпеки кожної держави для збереження економічної стабільності та суверенітету.

Між економічною безпекою та цифровізацією існує сильний і зростаючий взаємозв'язок. Цифрові технології стали невід'ємною частиною сучасної економіки, впливаючи майже на всі галузі та аспекти економічної діяльності. Цифровізація змінила спосіб роботи бізнесу, створивши нові можливості для інновацій, зростання та конкурентоспроможності. Запровадження цифрових технологій дозволило підприємствам підвищити ефективність, зменшити витрати та підвищити продуктивність. Це, у свою чергу, призвело до створення робочих місць, підвищення економічної активності та посилення економічної безпеки[3].

[1] Про платіжні послуги: Закон України від 30 червня 2021 року № 1591-IX. URL: https://zakon.rada.gov.ua/laws/show/1591-20#top.

[2] Єфремова К. В., Новіков Є. А. Цифрова трансформація фінансових послуг. *Інноваційний процес: перспективи євроінтеграції*: матеріали круглого столу (м. Харків, 24 березня 2023 року). Харків: НДІ ПЗІР НАПрН України, 2023. С. 35-41.

[3] Єфремова К. В. Новітні вимоги до розрахунку рівня економічної безпеки України під впливом цифровізації. *Економічна безпека: міжнародний і національний*

Крім того, цифрова економіка уможливила створення нових галузей, таких як електронна комерція, онлайн-платформи та цифрові послуги, які стають все більш важливими рушійними силами економічного зростання. Ці галузі мають потенціал для отримання прибутку та сприяння загальному економічному розвитку країни.

Однак цифровізація також створює значні виклики економічній безпеці. Зростання використання цифрових технологій створило нові вразливості та ризики, такі як кібератаки, витоки даних і поширення дезінформації. Ці загрози можуть мати значні економічні наслідки, включаючи втрату прибутку, шкоду діловій репутації та падіння довіри споживачів.

Тому урядам важливо віддавати пріоритет кібербезпеці та цифровій стійкості для забезпечення економічної безпеки своєї країни. Це включає інвестування в інфраструктуру кібербезпеки, сприяння цифровій грамотності та сприяння міжнародній співпраці з питань кібербезпеки. Нездатність вирішити ці виклики може призвести до значних економічних зривів і підірвати економічну безпеку держави.

Окрім кібербезпеки, є й інші важливі шляхи взаємозв'язку цифровізації з економічною безпекою. Наприклад, можливість доступу та використання цифрових технологій стає все більш важливою для бізнесу, щоб конкурувати та досягати успіху в глобальній економіці.

Цифровізація також уможливлює нові форми економічної діяльності, такі як гіг-економіка та бізнес на основі платформ, які можуть створити нові можливості для працівників, але також викликають занепокоєння щодо гарантій зайнятості та прав працівників.

Крім того, цифровізація може посилити існуючу економічну нерівність, оскільки ті, у кого немає доступу до цифрових технологій або цифрових навичок, можуть залишитися позаду. Тому для урядів важливо сприяти цифровій інтеграції та гарантувати, що всі громадяни мають доступ до цифрових технологій і навичок їх ефективного використання[1].

*рівень*: матеріали ІІ наук.-практ. конференції (м. Харків, 27 трав. 2023 р.). Харків: НДІ ПЗІР НАПрН України, 2023. С. 25-30.

[1] Єфремова К. В. Новітні вимоги до розрахунку рівня економічної безпеки України під впливом цифровізації. *Економічна безпека: міжнародний і національний*

Нарешті, цифровізація також впливає на природу торгівлі та комерції, причому електронна комерція та цифрові послуги все більше стають значною частиною світової торгівлі. Це підкреслює важливість розробки політик і нормативних актів, які підтримують і дозволяють цифрову торгівлю, а також вирішують проблеми щодо захисту даних, прав інтелектуальної власності та чесної конкуренції.

Оцінка ризиків економічної безпеки держави є основою для прийняття рішень в економіці та політиці. Ризики виникають при перевищенні граничних рівнів показників економічної безпеки. Особливо актуальним є питання оцінки стану економічної безпеки з метою проведення ефективної державної політики щодо виявлення загроз та мінімізації їх впливу[1].

Оцінку рівня економічної безпеки Мінекономіки здійснює з використанням Методичних рекомендацій щодо розрахунку рівня економічної безпеки України, затверджених наказом Мінекономрозвитку від 29.10.2013 р. № 1277[2].

Відповідно до зазначених методичних рекомендацій Мінекономіки здійснює оцінку інтегрального рівня економічної безпеки України в цілому по економіці та за окремими сферами діяльності на підставі офіційних даних Держстату, Нацкомфінпослуг, ДПС, Держмитслужби, Мінекоенерго, Мінфіну і Національного банку та експертних оцінок, у тому числі рейтингових звітів міжнародних неурядових організацій[3].

Так, до Інтегрального індексу економічної безпеки включено 9 середньозважених субіндексів – складових економічної безпеки,

*рівень*: матеріали ІІ наук.-практ. конференції (м. Харків, 27 трав. 2023 р.). Харків: НДІ ПЗІР НАПрН України, 2023. С. 25-30.

[1] Kardash O. Theoretical and methodological principles of the country's economic security assessment. *International journal of new economics and social sciences*. 2017, № 6 (2). P. 108-119. DOI: 10.5604/01.3001.0010.7628.

[2] Методичні рекомендації щодо розрахунку рівня економічної безпеки України : затв. наказом Міністерства економічного розвитку і торгівлі України від 29.10.2013 р. № 1277. URL: https://zakon.rada.gov.ua/rada/show/v1277731-13#Text.

[3] Лист Міністерства економіки України від 03.10.2021 р. № 3032-05/48176-09. URL: https://dostup.pravda.com.ua/request/93135/response/341541/attach/3/0.pdf?cookie_passthrough=1.

а саме: 1) виробнича безпека; 2) демографічна безпека; 3) енергетична безпека; 4) зовнішньоекономічна безпека; 5) інвестиційно-інноваційна безпека; 6) макроекономічна безпека; 7) продовольча безпека; 8) соціальна безпека; 9) фінансова безпека. У свою чергу, фінансова безпека, містить такі складові: 1) банківська безпека; 2) безпека небанківського фінансового ринку; 3) боргова безпека; 4) бюджетна безпека; 5) валютна безпека; 6) грошово-кредитна безпека.

Указом Президента України від 11 серпня 2021 р. № 347/2021 уведено в дію рішення Ради національної безпеки і оборони України від 11 серпня 2021 р. «Про Стратегію економічної безпеки України на період до 2025року» та затверджено саму Стратегію економічної безпеки України на період до 2025 року[1], пунктом 30 якої передбачено розроблення методики щорічної оцінки стану економічної безпеки (наукове супроводження реалізації Стратегії забезпечують Національний інститут стратегічних досліджень та Національна академія наук України)[2].

Найважливішими індикаторами економічної діяльності, ефективності економічної політики є індикатори економічної безпеки. Слід виходити з того, що економіка держави є динамічною системою та має тисячі показників, що характеризують її стан, які використовуються на макро- та мезорівнях для оцінки та прогнозування загроз економічній безпеці. Проте, зазначена Методика використовує низку показників, які відображають лише найважливіші напрями економічної безпеки в реальному та фінансовому секторах економіки, соціальній сфері; застосовується застарілі індикатори, зокрема, в межах виробничої безпеки «різниця індексу промислового виробництва України та Росії» (Додаток 1 п. 1.3)[3] та не враховані нові виклики

[1] Стратегія економічної безпеки України на період до 2025 року : затв. Указом Президента України від 11 серп. 2021 р. № 347/2021. URL : https://zakon.rada.gov.ua/laws/show/347/2021#n2.

[2] Лист Міністерства економіки України від 03.10.2021 р. № 3032-05/48176-09. URL: https://dostup.pravda.com.ua/request/93135/response/341541/attach/3/0.pdf?cookie_passthrough=1.

[3] Методичні рекомендації щодо розрахунку рівня економічної безпеки України : затв. наказом Міністерства економічного розвитку і торгівлі України від 29.10.2013 р. № 1277. URL : https://zakon.rada.gov.ua/rada/show/v1277731-13#Text.

і загрози, що пов'язані із складною ситуацією через військову агресію росії та процесами цифрової трансформації економіки та суспільства.

В свою чергу, під загрозами розуміють прямі чи непрямі можливості заподіяння шкоди економічним інтересам держави, та розрізняють їх на зовнішні і внутрішні загрози. Так, Кардаш О. Л. зазначає, що внутрішні загрози виникають внаслідок порушення механізмів сталого розвитку економічних систем і зумовлені соціальними, політичними, виробничими та фінансовими факторами, а зовнішні загрози зумовлені тиском на економічний суверенітет, в тому числі й на цифровий, і захист економічних інтересів країни, її цілісність та зміцнення потенціалу, стабільність національної економіки[1].

Окремою групою ризиків економічної безпеки в умовах цифровізації економіки виступають ризики втрати оцифрованих фінансових даних, що виступають ключовими факторами фінансової безпеки та конкурентоспроможності[2]. Питання цифрового суверенітету, в умовах глобалізації економіки, формування єдиного цифрового простору, швидкого зростання світового цифрового ринку, розвитку цифрової інфраструктури й інформаційних технологій[3], зокрема FinTegh, та їх впливу на забезпечення національної та міжнародної економічної безпеки, виходить на перший план.

Як слушно наголошує Корват О. В., ризики втрати цих даних, несанкціоноване їх використання чи порушення роботи цифрової інфраструктури стають значущими для функціонування економіки взагалі та піднімають питання забезпечення економічної безпеки в сфері інформації, що, на думку автора, базується на захисті інформаційного та цифрового суверенітету держави, інформаційної при-

[1] Kardash O. Theoretical and methodological principles of the country's economic security assessment. *International journal of new economics and social sciences*. 2017, № 6 (2). P. 108-119. DOI: 10.5604/01.3001.0010.7628.

[2] Маковець О., Дрозд І. Кібербезпека як фактор фінансової безпеки підприємства. *Економіка. Фінанси. Право.* 2020. № 5/3. С. 31–35. DOI: https://doi.org/10.37634/efp.2020.5(3).8.

[3] Єфремова К. В., Шматков Д. І., Кохан В. П. та ін. Базові аспекти цифровізації та їх правове забезпечення : монографія / Харків : НДІ прав. забезп. інновац. розвитку НАПрН України, 2021. 180 с.

ватності, інформаційних ресурсів, цифрової інфраструктури та кіберпростору. На думку вченої, цифровізація може спровокувати мультиплікаційні ефекти не лише для переваг, але і для недоліків завдяки великій кількості цифрових взаємозв'язків між суб'єктами економічних відносин та між виробничими процесами[1].

Проте, до згаданої раніше Методики розрахунку рівня економічної безпеки України не включено показників інформаційної безпеки, кібербезпеки та безпеки цифрової інфраструктури ані в межах фінансової складової, ані якої іншої.

Саме тому, система показників (індикаторів) для оцінки рівня безпеки та сукупність факторів, що загрожують стабільності та розвитку економічної безпеки потребують істотного перегляду.

Підсумовуючи, взаємозв'язок між економічною безпекою та цифровізацією стає все більш важливим, оскільки цифрові технології формують сучасну економіку та створюють нові можливості та виклики як для окремих суб'єктів господарювання, так і для держави. Нові загрози потребують оцінки, аналізу та визначення вектору заходів щодо зменшення впливу загроз на економічну безпеку України. Важливо, щоб законодавець надавав пріоритет цифровій стійкості, цифровій інклюзії та відповідальній політиці цифрової торгівлі для забезпечення довгострокової економічної безпеки своєї держави.

## 5.3. Вплив цифровізації фінансової сфери на фінансову безпеку як складову економічної

У світі, що стає все більш цифровим, розвиток фінансових технологій, кардинально змінив спосіб проведення фінансових операцій і доступу до фінансових послуг. Оскільки FinTech відіграє дедалі зрос-

[1] Корват О. В. Економічна стійкість і безпека держави в умовах Індустрії 4.0. *Економічна безпека: міжнародний і національний рівень*: зб. наук. праць НДІ ПЗІР НАПрН України за матеріалами ІІ-ї науково-практичної конференції (м. Харків, 21 квітня 2023 року). Харків: НДІ ПЗІР НАПрН України, 2023. С. 37-43.

таючу роль у світовій економіці, розуміння його наслідків для фінансової безпеки є надзвичайно важливим. Традиційні фінансові системи стикаються як з новими викликами, так і можливостями через особливу природу фінансових технологій.

Трансформація української економічної системи та фінансового сектору пов'язана з новими потребами держави, глобалізацією світового фінансового простору, а отже і з новими загрозами. Чітке бачення передумов і наслідків цієї трансформації може стати основою для формування обґрунтованого вибору правових механізмів мінімізації або усунення негативних факторів, що впливають на фінансову безпеку держави. Необхідність створення сприятливих правових та інституційних умов для функціонування та розвитку фінансової системи держави ставить першочергове завдання зміцнення всіх підвидів фінансової безпеки через FinTech[1].

Протягом останніх років вітчизняні та іноземні автори підготували чимало публікацій щодо розвитку фінансових технологій, серед яких Шевченко О., Рудич Л., Сіренко Н., Полторак А., Атаманюк І., Волосюк Ю., Мельник О., Фененко П., Худолій Ю., Свистун Л. Питаннями нарощення обсягів діджиталізації, цифровізації фінансових продуктів та специфікою впливу фінтех компаній на фінансовий сектор у своїх роботах займалися Андрушків І., Надієвець Л., Гаряга Л., Стойко О. та інші. Питання безпеки фінансових установ вивчали такі вчені як: Барановський О., Варналій З., Єгоричева С. та інші. Разом з тим, проблемам правового регулювання використання FinTech та його впливу на державну економічну політику і безпеку не приділено належної уваги, що обумовлює актуальність проведення аналізу зв'язку цифрових фінансових технологій та фінансової безпеки держави, вивчення позитивного і негативного впливу FinTech на державну економічну політику і фінансову безпеку, та підкреслення необхідності адаптації регуляторних підходів для підтримки безпечної фінансової системи.

[1] Єфремова К. В. Технології цифрової економіки та фінансова безпека. *Право та інновації*. 2023. № 2 (42). С. 7-11. DOI: https://doi.org/10.37772/2518-1718-2023-2(42)-1.

Фінансова безпека є складовою частиною економічної безпеки держави та відображає стан фінансової системи країни, за якого створюються необхідні фінансові умови для стабільного соціально-економічного розвитку країни, забезпечується її стійкість до фінансових шоків та дисбалансів, створюються умови для збереження цілісності та єдності фінансової системи країни[1]. Фінансова безпека, у свою чергу, має такі складові:

1) банківська безпека як рівень фінансової стійкості банківських установ країни, що дає змогу забезпечити ефективність функціонування банківської системи країни та захист від зовнішніх і внутрішніх дестабілізуючих чинників незалежно від умов її функціонування;

2) безпека небанківського фінансового сектору – це рівень розвитку фондового та страхового ринків, що дає змогу повною мірою задовольняти потреби суспільства в зазначених фінансових інструментах та послугах;

3) боргова безпека - відповідний рівень внутрішньої та зовнішньої заборгованості з урахуванням вартості її обслуговування та ефективності використання внутрішніх і зовнішніх запозичень та оптимального співвідношення між ними, достатній для задоволення нагальних соціально-економічних потреб, що не загрожує суверенітету держави та її фінансовій системі;

4) бюджетна безпека відображає стан забезпечення платоспроможності та фінансової стійкості державних фінансів, що надає можливість органам державної влади максимально ефективно виконувати покладені на них функції;

5) валютна безпека – це стан курсоутворення, який характеризується високою довірою суспільства до національної грошової одиниці, її стійкістю, створює оптимальні умови для поступального розвитку вітчизняної економіки, залучення в країну іноземних інвестицій, інтеграції України до світової економічної системи, а також максимально захищає від потрясінь на міжнародних валютних ринках;

[1] Методичні рекомендації щодо розрахунку рівня економічної безпеки України: Наказ Міністерства економічного розвитку і торгівлі України від 29.10.2013 р. № 1277. URL: https://zakon.rada.gov.ua/rada/show/v1277731-13#Text.

6) грошово-кредитна безпека відображає стан грошово-кредитної системи, що забезпечує всіх суб'єктів національної економіки якісними та доступними кредитними ресурсами в обсягах та на умовах, сприятливих для досягнення економічного зростання національної економіки.

Комплексний розвиток інноваційного потенціалу держави шляхом створення масових інноваційних продуктів, розвитку високотехнологічного виробництва, досягнення науково-дослідних переваг та стрімкого розвитку FinTech може стати основою зміцнення фінансової безпеки України.

FinTech трактують як інноваційні технології та бізнес-моделі, технології індустрії послуги. Проте, в кожному з наведених визначень простежується їх головна особливість, яка полягає в тому, що FinTech дійсно не може працювати без цифрових технологій.

Сьогодні саме цифрові технології є потужним рушієм принципів прозорості фінансових відносин, що особливо помітно на рівні державних фінансів. Враховуючи те, що ключову роль у формуванні фінансової безпеки держави відіграє забезпечення індикаторів бюджетної безпеки, необхідно приділити значну увагу розгляду особливостей індексу відкритості бюджету, який формується шляхом розрахунку показників, які комплексно характеризують прозорість бюджетного процесу[1].

Підвищення рівня бюджетної прозорості сприяє реалізації наступних цілей: покращення виконання державою бюджетних зобов'язань та послуг, а також підвищення рівня задоволеності якістю публічних послуг; залучення громадськості до бюджетного процесу; здійснення більш широкого громадського контролю за цільовим витрачанням бюджетних коштів; підвищення рівня відповідальності виконавчої влади за виконання бюджету; підвищення ефективності використання бюджетних коштів та інші.

Саме прозорість дозволяє зменшити зловживання у фінансовій сфері, знизити рівень корупції та тіньовості економіки, що дозволяє

[1] Єфремова К. В. Технології цифрової економіки та фінансова безпека. *Право та інновації*. 2023. № 2 (42). С. 7-11. DOI: https://doi.org/10.37772/2518-1718-2023-2(42)-1.

підвищити рівень фінансової безпеки держави. В Україні у сфері державних фінансів цифровізація набула найбільшого поширення в бюджетному процесі, де завдяки запровадженню системи «Прозорий бюджет» веб-портали «spending.gov» та «openbudget.gov.ua» вдалося суттєво підвищити прозорість публічного та місцевого рівнів. Завдяки реалізації принципів інформаційної відкритості через сайт Міністерства фінансів України суттєво підвищилася прозорість державної боргової політики[1]. Важливою складовою забезпечення фінансової безпеки держави є банківська безпека, де головним інститутом публічності та прозорості є Національний банк України. Саме на сайті НБУ можна ознайомитися з актуальною інформацією про стан валютного ринку, монетарну політику тощо.

Для забезпечення заходів щодо підвищення прозорості валютного регулювання, які спрямовані на припинення вивезення капіталу, незаконного відмивання коштів під виглядом іноземних інвестицій, функціонування тіньового сектору зовнішньої торгівлі та фінансового ринку, особливе місце займають SupTech і RegTech.

Термін RegTech в сучасному розумінні було застосовано в 2017 році Радою з фінансової стабільності (FSB), яка створена для координації на міжнародному рівні роботи національних фінансових органів і міжнародних органів, що встановлюють стандарти, з метою розробки та сприяння реалізації ефективної регуляторної, наглядової та іншої політики у фінансовому секторі. Вони визначають RegTech як управління регуляторними процесами у фінансовій галузі за допомогою технологій. В свою чергу, Базельський Комітет з питань банківського нагляду[2] визначає SupTech, що здійснює контроль і моніторинг, як використання технології для полегшення та вдосконалення наглядових процесів з точки зору наглядових органів.

[1] Hrytsenko L., Zakharkina L., Zakharkin O., Novikov V., Chukhno R. The impact of digital transformations on the transparency of financial-economic relations and financial security of Ukraine. Financial and credit activity: problems of theory and practice. 2022. No. 3 (44), P. 167. DOI: 10.55643/fcaptp.3.44.2022.3767.

[2] Basel Committee on Banking Supervision (BCBS). Instructions for Basel III monitoring. 19 October 2018. URL: https://www.bis.org/bcbs/qis/biiiimplmoninstr_oct18.pdf.

Проте, Сіренко Н., Полторак А., Атаманюк І., Волосюк Ю., Мельник О. та Фененко П., виділяють інші фінансові технології, що формують можливості зміцнення фінансової безпеки держави[1]:

1) технології блокчейн, що впливають на централізовані бізнес-моделі;

2) хмарні технології, що сприяють адаптивності, економічності та зниженню кіберризиків;

3) платформи, які формують нові можливості;

4) Інтернет речей, що надає доступ до цінностей користувача;

5) технології BigData, що допомагають поглибити аналіз поведінки користувачів у поведінковому підході до моніторингу фінансової безпеки;

6) штучний інтелект і автоматизація, що зменшує кількість людської праці, створює нові можливості для аналізу;

7) цифрова платформа Banking API (сприяє інтеграції партнерів і ринку) тощо.

Так, найрозповсюдженіші платіжні інновації на базі FinTech включають ряд елементів, серед яких мобільні платежі, мобільні (електронні) гаманці, безконтактні платежі, технології перевірки особистості, а також штучний інтелект і машинне навчання спрямовані для забезпечення безпеки[2].

В свою чергу, хоч FinTech і означає використання інноваційних технологій для надання фінансових послуг і підвищення ефективності фінансових систем, коли мова заходить про фінансову безпеку, розвиток фінансових технологій може мати як позитивні, так і негативні наслідки.

Можна виділити такі позитивні ефекти впливу FinTech на фінансову безпеку: по-перше, це покращена безпека транзакцій. Рішення

[1] Sirenko N., Atamanyuk I., Volosyuk Yu. et al. Paradigm Changes that Strengthen the Financial Security of the State through FINTECH Development. The 11th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2020, Kyiv, Ukraine, 2020. DOI: 10.1109/DESSERT50317.2020.9125026.

[2] Худолій Ю., Свистун Л. Сучасні тенденції FINTECH та їх вплив на безпеку банківських установ. *Економіка і регіон*. 2021. № 3 (82). С. 115–123. DOI 10.26906/EiR.2021.3(82).2375.

FinTech використовують передові технології для зміцнення безпеки транзакцій, включаючи надійне шифрування, багатофакторну автентифікацію та системи виявлення шахрайства. Ці заходи зміцнюють захист фінансових даних, зменшують ризик шахрайства та покращують фінансову безпеку.

По-друге, покращений доступ до фінансових послуг: доступність Fintech розширює можливості незабезпеченого населення, пропонуючи раніше недоступні фінансові послуги. Мобільні банківські програми та онлайн-платформи забезпечують більшу фінансову доступність, дозволяючи окремим особам і компаніям ефективніше керувати своїми фінансами. Зменшуючи бар'єри для входу, FinTech сприяє загальній фінансовій безпеці.

По-третє, ефективне дотримання нормативних вимог: інновації фінансових технологій, такі як блокчейн, сприяють прозорому та перевіреному веденню записів, посилюючи регулятивний нагляд. Незмінність і відстежуваність транзакцій блокчейну допомагають боротися з відмиванням грошей, фінансуванням тероризму та іншою незаконною діяльністю, зміцнюючи фінансову безпеку та дотримання нормативних вимог.

Fintech може допомогти у зміцненні фінансової безпеки шляхом покращення дотримання нормативних актів і зменшення потенціалу для відмивання грошей, фінансування тероризму та іншої незаконної діяльності. Такі технології, як блокчейн, який лежить в основі криптовалют, забезпечують прозоре та незмінне ведення записів, сприяючи регуляторному контролю та забезпечуючи більшу фінансову безпеку. Розглядаючи негативні наслідки, найчастіше виділяють такі:

1. Ризики кібербезпеки[1]: залежність FinTech від цифрової інфраструктури створює вразливі місця для кіберзагроз. Досвідчені хакери можуть використовувати слабкі місця в системах фінансових технологій, потенційно скомпрометувавши конфіденційну фінансову інформацію або зриваючи критичні фінансові операції. Для усунення

[1] Zadvornykh S. Fintech and financial security – perspectives and dangers. *Proceedings of III International Scientific and Practical Conference.* Osaka, Japan, 2019. P. 392–401.

цих ризиків і підтримки фінансової безпеки необхідні надійні заходи кібербезпеки.

2. Занепокоєння щодо конфіденційності даних[1].

3. Розповсюдження фінансових технологій тягне за собою збір і обробку значної кількості персональних і фінансових даних, що викликає занепокоєння щодо конфіденційності. Неналежний захист даних або їх порушення можуть призвести до крадіжки особистих даних, фінансового шахрайства та порушення конфіденційності. Захист персональних даних і впровадження ефективних правил захисту даних є обов'язковими для забезпечення фінансової безпеки в епоху фінансових технологій.

4. Нерівний доступ і залучення: хоча FinTech розширив доступ до фінансових послуг для багатьох, цифровий розрив залишається. Обмежений доступ до технологій і недостатня цифрова грамотність перешкоджають фінансовій доступності, загострюючи економічну нерівність і підриваючи фінансову безпеку. Усунення цих прогалин має вирішальне значення для розвитку справедливих і безпечних фінансових систем.

Цифрові трансформації, які відбулися в Україні за останні роки, значно підвищили прозорість фінансових відносин, особливо вплинули на суспільний рівень. Загалом, розвиток фінансових технологій має потенціал для підвищення фінансової безпеки за рахунок покращення безпеки транзакцій, ефективного дотримання нормативних вимог і розширення доступу до фінансових послуг, зменшення потенціалу для відмивання грошей, фінансування тероризму та іншої незаконної діяльності. Однак це також створює проблеми, пов'язані з кібербезпекою, конфіденційністю даних і справедливим доступом, які необхідно вирішити, щоб забезпечити загальну фінансову безпеку держави. Трансформуючий вплив Fintech на фінансовий ландшафт вимагає всебічного розуміння його зв'язку з фінансовою безпекою.

[1] Musabegovic I., Özer M., Djukovic S, Jovanovic S. Influence of financial technology (fintech) on financial industry. *Economics of Agriculture, Year 66*. 2019. No. 4. P. 1003–1021. DOI:10.5937/ekoPolj1904003M.

Швидкі темпи розвитку цифрових фінансових технологій вимагають проактивної та адаптивної правової політики щодо трансформації нормативної бази. Традиційним регуляторним підходам може бути важко йти в ногу з інноваціями фінансових технологій і пов'язаними з ними ризиками. Законодавець повинен співпрацювати з галузевими зацікавленими сторонами, щоб знайти баланс між сприянням інноваціям і захистом фінансової безпеки. Динамічні нормативно-правові рамки повинні наголошувати на підходах, що ґрунтуються на оцінці ризиків, сприяючи кібербезпеці, конфіденційності даних і захисту споживачів, одночасно сприяючи розвитку фінансових технологій[1].

В епоху фінансових ринків, що швидко розвиваються, ефективний нагляд і регулювання фінансових систем є найважливішими для підтримки фінансової безпеки держави. Ризики кібербезпеки, проблеми конфіденційності даних і цифровий розрив повинні бути розглянуті для ефективної підтримки фінансової безпеки.

Для зменшення ризиків кібербезпеки співпраця між урядами, регуляторними органами та приватним сектором є надзвичайно важливою. Для захисту фінансових систем необхідні регулярні оцінки безпеки, надійні протоколи шифрування та освітні ініціативи з кібербезпеки. Ретельний контроль за дотриманням положень щодо конфіденційності даних, таких як Загальний регламент захисту даних (GDPR) у Європі, допомагає захистити особисту інформацію та зберегти довіру до послуг FinTech.

Європа була в авангарді інновацій FinTech, і численні країни впроваджували технологічні досягнення для покращення фінансових послуг. Інституції ЄС та національні регулятори визнають важливість FinTech для підвищення фінансової безпеки. Так, Європейська комісія за допомогою таких ініціатив, як Європейський порядок денний для спільної економіки та Стратегія цифрового фінансування, прагне сприяти інноваціям, одночасно забезпечуючи жорсткі правила для захисту споживачів і підтримки фінансової стабільності.

[1] Єфремова К. В. Технології цифрової економіки та фінансова безпека. *Право та інновації.* 2023. № 2 (42). С. 7-11. DOI: https://doi.org/10.37772/2518-1718-2023-2(42)-1.

Стратегія цифрових фінансів[1] визначає загальні напрямки того, як Європа може підтримати цифрову трансформацію фінансового сектору у найближчі роки, одночасно регулюючи ризики. Стратегія встановлює чотири основні пріоритети:

1) усунення фрагментації єдиного цифрового ринку;

2) адаптація нормативно-правової бази ЄС для сприяння цифровим інноваціям;

3) сприяння фінансуванню, керованому даними;

4) вирішення проблем і ризиків, пов'язаних з цифровою трансформацією, включаючи підвищення цифрової операційної стійкості фінансової системи.

За даними Європейського банківського управління (ЕВА)[2], фінансові технології можуть позитивно сприяти фінансовій безпеці взагалі шляхом підвищення безпеки платежів, покращення управління ризиками та сприяння фінансовій доступності. Використання вдосконаленого шифрування, надійної автентифікації клієнтів і систем виявлення шахрайства підвищило безпеку транзакцій, зменшивши ризик кіберзагроз і шахрайства.

Попри всі виклики останніх років, Україна теж швидко стає центром фінансових технологій із зростаючою екосистемою інноваційних стартапів і сприятливим регуляторним середовищем. Національний банк України визнає трансформаційний потенціал FinTech, наголошуючи на важливості фінансової безпеки. Упровадження SupTech та розвиток RegTech також є однією із цілей Національного банку, визначених Стратегією розвитку фінансового сектору до 2025 року[3], Стратегією розвитку фінтеху в Україні до 2025 року[4].

[1] European Commission (2020). Digital finance strategy. URL: https://finance.ec.europa.eu/publications/digital-finance-package_en.

[2] The European Banking Authority (2023). Annual Report 2022. URL: https://www.eba.europa.eu.

[3] Стратегія розвитку фінансового сектору до 2025 року (оновлена у березні 2021 року). Національний банк України. URL: https://bank.gov.ua/ua/news/all/strategiya-rozvitku-finansovogo-sektoru-ukrayini-do-2025-roku-7686.

[4] Стратегія розвитку фінтеху в Україні до 2025 року. Національний банк України. URL: https://bank.gov.ua/ua/about/develop-strategy/fintech2025.

Поява нових фінансових послуг, збільшення складності та швидкості операцій піднаглядних суб'єктів та їх клієнтів, зростання обсягу даних, посилення нормативних вимог регуляторів зумовили виникнення таких напрямів фінансових технологій, як RegTech і SupTech.

RegTech означає використання технології для сприяння дотриманню нормативних вимог, охоплює широкий спектр програм, включаючи аналітику даних, штучний інтелект і автоматизацію, які спрощують регулятивні процеси та підвищують ефективність. SupTech зосереджується на використанні технологій для посилення наглядових функцій, які виконують регуляторні органи.

Сьогодні забезпечення інформаційної безпеки в фінансовому секторі є основним напрямом застосування RegTech-рішень учасниками фінансового ринку. Інновації у наглядових та регуляторних технологіях – запорука сталого розвитку фінансового ринку, вони дозволяють фінансовим установам і регуляторам постійно удосконалювати чинні процеси, розширювати коло клієнтів/піднаглядних суб'єктів, виявляти та попереджувати потенційні ризики в діяльності фінансового сектору.

Світовий досвід свідчить, що використовуючи RegTech, фінансові установи можуть оптимізувати процес дотримання регуляторних вимог, а регулятори, зі свого боку, використовуючи SupTech, мають змогу автоматизувати та спростити власні процеси нагляду. Використання зазначених інструментів допомагає покращити аналітичні можливості, відслідковувати ризики в реальному часі, робити точніші прогнози та формувати виважену наглядову політику як для регуляторів, так і для піднаглядних суб'єктів[1].

Система зовнішнього аудиту інформаційної безпеки піднаглядових організацій дозволить підвищити стійкість учасників фінансового ринку до ризиків інформаційної безпеки та своєчасно їх виявляти.

[1] Концепція розвитку інноваційних наглядових та регуляторних технологій. Національний банк України. URL: https://bank.gov.ua/admin_uploads/article/Concept_development_Suptech_Regtech.pdf?v=4.

Складність фінансових систем, зростаючий обсяг фінансових даних і поява нових ризиків вимагають більш гнучкого та ефективного підходу до дотримання нормативних вимог і нагляду. RegTech і SupTech пропонують вирішення цих проблем, забезпечуючи моніторинг у реальному часі, прогнозну аналітику та інструменти оцінки ризиків.

Рішення RegTech дозволяють фінансовим установам автоматизувати процеси збору даних, звітності та аналізу, зменшуючи тягар дотримання вимог. Передові технології, такі як обробка природної мови та алгоритми машинного навчання, допомагають отримувати відповідну інформацію з неструктурованих джерел даних, забезпечуючи точні та своєчасні звіти[1].

Інструменти RegTech допомагають фінансовим установам ефективніше визначати й оцінювати потенційні ризики. Використовуючи аналітику великих даних і алгоритми машинного навчання, ці технології можуть аналізувати величезні обсяги даних, щоб виявляти шаблони, аномалії та потенційні порушення відповідності. Такий проактивний підхід до управління ризиками підвищує загальну фінансову безпеку держави.

В свою чергу, рішення SupTech дозволяють контролюючим органам контролювати діяльність фінансових установ у режимі реального часу, надаючи можливість завчасно виявляти потенційні ризики або порушення. Автоматизовані системи спостереження можуть аналізувати дані про транзакції, виявляти підозрілі дії та ініціювати попередження, забезпечуючи оперативні дії наглядачів[2].

Розглядаючи проблеми конфіденційності даних і кібербезпеки у фінансовому секторі, завжди RegTech і SupTech викликають занепокоєння. щодо конфіденційності даних і кібербезпеки. Проте, щоб

[1] Концепція розвитку інноваційних наглядових та регуляторних технологій. Національний банк України. URL: https://bank.gov.ua/admin_uploads/article/Concept_development_Suptech_Regtech.pdf?v=4.

[2] Єфремова К. В. FinTech та фінансова безпека. *Актуальні проблеми господарської діяльності в умовах розбудови економіки Індустрії 4.0* : зб. наук. пр. НДІ ПЗІР НАПрН України за матеріалами ІІІ круглого столу (м. Харків, 25 травня 2023 року). Харків: НДІ ПЗІР НАПрН України, 2023. С. 12-18.

повністю реалізувати потенціал RegTech і SupTech, нормативні рамки повинні розвиватися відповідно до технологічних досягнень. Співпраця між регулюючими органами, зацікавленими сторонами галузі та міжнародними органами має вирішальне значення для встановлення спільних стандартів і найкращих практик.

Фінансові технології пропонують значний потенціал для зміцнення опіки над фінансовою безпекою шляхом посилення відповідності нормативним вимогам і можливостей нагляду. Ефективне впровадження цих технологій може оптимізувати процеси, покращити управління ризиками та забезпечити оперативне втручання у фінансові системи.

Вплив FinTech на фінансову безпеку держави є значним і багатогранним. Як європейська, так і українська точки зору підкреслюють необхідність розробки сучасної нормативно-правової бази, підтримки технологічних інновацій і спільних зусиль для використання потенціалу фінансових технологій, одночасно пом'якшуючи пов'язані з цим ризики. Використовуючи досягнення FinTech, захищаючи інтереси споживачів і сприяючи фінансовій доступності та прозорості, країни можуть орієнтуватися в фінансовому ландшафті, що розвивається, забезпечуючи безпечну та стійку фінансову систему в майбутньому.

Усунення цифрового розриву є життєво важливим для забезпечення рівноправного доступу до послуг FinTech. Уряди та зацікавлені сторони галузі можуть співпрацювати, щоб подолати розрив, забезпечуючи програми цифрової грамотності, покращуючи інфраструктуру та просуваючи інклюзивні фінтех-рішення, адаптовані до потреб незахищених верств населення[1].

В Україні FinTech має потенціал для посилення фінансової безпеки шляхом підвищення фінансової доступності, сприяння безпечним транзакціям і підвищення ефективності дотримання нормативних вимог. Запровадження цифрових платіжних систем, мобільних

[1] Єфремова К. В. FinTech та фінансова безпека. *Актуальні проблеми господарської діяльності в умовах розбудови економіки Індустрії 4.0* : зб. наук. пр. НДІ ПЗІР НАПрН України за матеріалами III круглого столу (м. Харків, 25 травня 2023 року). Харків: НДІ ПЗІР НАПрН України, 2023. С. 12-18.

банківських програм і технології блокчейн сприяло більшій доступності, зменшивши залежність від готівки та мінімізувавши ризик шахрайства. Однак НБУ також визнає необхідність постійного моніторингу та адаптації нормативно-правових актів для усунення нових ризиків, пов'язаних з FinTech.

## 5.4. Посилення цифрової трансформації у напрямі зеленого курсу

Шкода завдана довкіллю воєнною агресії рф проти України є безпрецедентною. За Індексом екологічної ефективності в 2022 році Україна посідає 52 місце зі 180 країн. Найгірші показники мають такі категорії: екосистемні послуги (103), якість повітря (88), управління відходами (88), біорізноманіття (76)[1]. Саме тому цифрова трансформація економіки і суспільства має стати частиною Зеленого курсу. Його виконання важливе для євроінтеграції, залучення коштів на відновлення країни та розвитку економіки.

На думку О. Дороганя, виконавчого директора Офісу ефективного регулювання BRDO (англ. Better Regulation Delivery Office), цифрові рішення уможливлюють і полегшують у різних секторах підтримку декарбонізації, зменшення до 15-20% викидів парникових газів, забезпечення економічного зростання, застосування розумної інфраструктури для моніторингу екосистем, оптимізацію транспортних потоків, використання енергії і створюють багато інших можливостей[2]. Проте, це потребує заохочення інвестування і прискореного розвитку цифрової інфраструктури й технологій, цифрових послуг і ринків, а також розвитку цифрових навичок населення.

[1] Зелений курс і цифрова трансформація України – як використати потенціал ІКТ-сектору в післявоєнному відновленні. BRDO. 2022. URL: https://brdo.com.ua/news/zelenyj-kurs-i-tsyfrova-transformatsiya-ukrayiny-yak-vykorystaty-potentsial-ikt-sektoru-v-pislyavoyennomu-vidnovlenni/.

[2] Там само.

Необхідно звернути увагу, що динаміка цифрової трансформації соціально-економічних та екологічних систем залежить від якості управління такою трансформацією. Результати управління цифровим перетворенням економіки відображаються на конкурентоспроможності країни.

У світі застосовують різні методи оцінювання динаміки цифрової трансформації, які здебільшого базуються на оцінюванні структурних складових цифровізації економіки та суспільства. Існує багато способів оцінювання цих складових на макрорівні, на основі яких складають рейтинги інноваційного розвитку країн. Системи показників переважно містять валові показники продукту чи інвестицій у цифрову трансформацію. До таких систем належить Global Innovation Index, що є дуже потужним інструментом оцінювання цифрового розвитку країн. Окрім Global Innovation Index, є значна кількість інших методів оцінювання цифрової трансформації країн, серед яких можна виділити Technology Achievement Index і The European Digital Social Innovation Index[1].

На їх основі можна оцінювати цифрову трансформацію соціально-економічних та екологічних систем і, враховуючи те, що ці системи змінюються з часом, можна оцінювати динаміку цифрової трансформації. Це також дозволяє розробити рекомендації для управління цифровою трансформацією.

Так, результати DESI-2022 показують, що в той час як більшість держав-членів ЄС досягають прогресу в цифровій трансформації, впровадження ключових цифрових технологій бізнесом, таких як штучний інтелект і великі дані, залишається низьким, навіть серед лідерів ЄС[2]. Недостатній рівень цифрових навичок перешкоджає

[1] Єфремова К. В. Динаміка цифрової трансформації та зелений перехід. Збірник наукових праць НДІ ПЗІР НАПрН України : Цифрові трансформації України 2023: виклики та реалії : за матеріалами IV Круглого столу (м. Харків, 29 вересня 2023 року). Харків: НДІ ПЗІР НАПрН України, 2023. С. 42-48. URL: https://ndipzir.org.ua/wp-content/uploads/2023/09/conf_29.09.23.pdf.

[2] Digital Economy and Society Index (DESI) 2022. European Commission. 2023. URL: https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022/.

перспективам майбутнього зростання, поглиблює цифровий розрив і збільшує ризик цифрового відторгнення, оскільки все більше послуг, у тому числі найважливіших, переміщуються в Інтернет. Необхідно активізувати зусилля, щоб забезпечити повне розгортання повсюдної інфраструктури зв'язку (зокрема 5G), яка потрібна для високоінноваційних послуг і програм.

Фінляндія, Данія, Нідерланди та Швеція продовжують залишатися лідерами ЄС. Однак цикл Європейського семестру 2022 року визначив, що цифрові проблеми залишаються також для більшості лідерів. Це означає, що ЄС в цілому продовжує покращувати свій рівень цифровізації, впроваджуючи спеціальні програми підтримки та ініціативи, і зокрема ті країни-члени, які почали з нижчих рівнів, поступово наздоганяють, розвиваючись швидшими темпами. Наприклад, серед держав-членів, які відстають, Італія, Польща та Греція суттєво покращили свої показники DESI за останні п'ять років і здійснили стійкі інвестиції з посиленим політичним фокусом на цифрових технологій за підтримки загальноєвропейського фінансування.

Усвідомлюючи можливості цифрових технологій, уряди в усьому світі все частіше ставлять цифрову трансформацію на передній план і в центр своїх політичних планів для стимулювання соціального розвитку та економічного процвітання, реалізуючи цифрові стратегії, що охоплюють численні економічні сектори.

Дослідивши показники цифрової трансформації, можна виділити чотири окремі групи країн, кожна з яких перебуває на різному етапі цифрового розвитку та з різними рівнями зрілості своїх національних стратегій цифрової трансформації: а) країни з обмеженою готовністю, б) країни з перехідною економікою, в) передові країни та г) країни-лідери.

Говорячи про динаміку цифрової трансформації України, необхідно звернути увагу не лише на темпи цифровізації економіки і суспільства та віднесення до якоїсь з визначених категорій, а на якість цифрової трансформації, використовуючи всі можливості ІКТ для відновлення країни[1].

[1] Єфремова К. В. Динаміка цифрової трансформації та зелений перехід. Збірник наукових праць НДІ ПЗІР НАПрН України : Цифрові трансформації України 2023:

Існують певні показники того, що цифровізація може посприяти декарбонізації та зеленій трансформації як у масштабах всієї країни, так і для відновлення окремих міст. Застосування цифрових технологій, таких як штучний інтелект, 5G, хмарні та периферійні обчислення, а також Інтернет речей мають величезний потенціал, здатний прискорити і максимізувати вплив політики екологізації та створення нових екологічно чистих робочих місць. Так, цифровізація відіграє ключову роль у «перезапуску» вугледобувних міст України згідно з зеленими європейськими стандартами.

Сьогодні це є актуальним напрямком сучасної цифрової економіки. На думку радника Єврокомісії з цифрових аспектів зеленої трансформації Іліаса Яковідіса, «Побудова циркулярної економіки має бути головним пріоритетом, де цифрові технології дійсно можуть показати силу відокремлення нашої економіки від постійно зростаючого використання природних ресурсів»[1].

Реалізація Україною Зеленого курсу ЄС є важливою складовою євроінтеграції. Єврокомісія визначає, що відбудова України має відповідати зеленому та цифровому порядку денному[2]. Аналіз положень Європейського зеленого курсу показує необхідність впровадження в Україні таких напрямів посилення цифрової трансформації:

1) розвиток сектору інформаційно-комунікаційних технологій (ІКТ) щодо доступності, розвитку цифрових навичок населення та інше;

2) зелений перехід в ІКТ-секторі: енергоефективність, циркулярність;

---

виклики та реалії : за матеріалами IV Круглого столу (м. Харків, 29 вересня 2023 року). Харків: НДІ ПЗІР НАПрН України, 2023. С. 42-48. URL: https://ndipzir.org.ua/wp-content/uploads/2023/09/conf_29.09.23.pdf.

[1] Цифрова революція може спричинити екологічну катастрофу, – євродепутат. Екополітика. 2022. URL: https://ecopolitic.com.ua/ua/news/cifrova-revoljuciya-mozhe-sprichiniti-ekologichnu-katastrofu-ievrodeputat/.

[2] Communication from the Commission to the European Parliament, the European Council, the Council, the European economic and social committee and the committee of the regions. Ukraine relief and reconstruction. European Commission. Brussels, 18.5.2022 COM(2022) 233 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022DC0233.

3) цифрова трансформація секторів: енергетика, будівництво, сільське господарство й інших;

4) міжсекторальні «зелені зміни»: закупівлі, бюджетування, оподаткування та інше.

При цьому ІКТ-сектор потребує власної зеленої трансформації. Його вуглецевий слід в ЄС оцінюється біля 4 %, із тенденцією зростання до 8-10 %. Досягнення кліматичної нейтральності та циркулярності ІКТ передбачає, зокрема, більш енергоефективні центри обробки даних і електронні комунікаційні мережі, повністю циклічний екодизайн обладнання ІКТ, посилення екологічних заходів під час розгортання мереж, прозорість впливу сектору на довкілля[1].

Донедавна більшість учасників фінансового ринку вважали фінансові ризики, пов'язані з кліматом та екологічними проблемами, абстрактними. Особи, які приймають фінансові рішення, та інвестори стають більш обізнаними щодо клімату: інституційні інвестори та банки, які несуть відповідальність перед кінцевими інвесторами та акціонерами, перебувають під зростаючим тиском, щоб представити свої інвестиційні та кредитні рішення такими, що відповідають новим екологічним, соціальним стандартам і стандартам управління (ESG – абревіатура від environmental, social, governance – навколишнє середовище, суспільство, управління. Це підхід, при якому під час прийняття рішень до уваги береться структура корпоративного управління компаній з оцінкою впливу її діяльності на екологію та суспільство. Відповідно, дотримання бізнесом ESG-принципів і розкриття інформації щодо ESG-показників стає вагомим чинником інвестиційної привабливості бізнесу, майбутньої вартості інвестицій у нього, тобто безпосередньо впливає на прийняття інвесторами фінансових рішень)[2].

[1] Цифрова трансформація як основа Європейського зеленого курсу і відновлення. Міністерство економіки Україні. Платформа ефективного регулювання. URL: https://regulation.gov.ua/dialogue/it-i-telekom/81-cifrova-transformacia-ak-osnova-evropejskogo-zelenogo-kursu-i-vidnovlenna.

[2] Єфремова К. В. Динаміка цифрової трансформації та зелений перехід. Збірник наукових праць НДІ ПЗІР НАПрН України : Цифрові трансформації України 2023: виклики та реалії : за матеріалами IV Круглого столу (м. Харків, 29 вересня 2023

В результаті цього тиску фінансові ринки адаптуються та змінюються. У багатьох випадках облігації та інші інструменти, які не відповідають відповідним критеріям ESG, продаються з дисконтом порівняно з тими, які відповідають – цей розрив, імовірно, збільшиться в майбутньому. Дедалі частіше інвестори виділяють ресурси на фінансові інструменти, сертифіковані як такі, що відповідають певним принципам ESG, як-от «зелені» облігації та інші так звані марковані активи (активи, які отримали певний тип сертифікації або позначки, пов'язані з характеристиками ESG)[1].

Оскільки відбуваються ці зміни, ринок «зелених» облігацій і «зелених» активів швидко зростає. Інвестори купують нові випуски, а спеціалізовані міжнародні кліматичні фонди та банки розвитку прагнуть підтримати потік капіталу в екологічні проєкти, включаючи розвиток ринків екологічних облігацій, використовуючи пільгове фінансування, інструменти покращення кредитування та власні баланси.

Зелені активи – це фінансові інструменти, які збирають кошти, які будуть використовуватися для фінансування екологічно корисних або «зелених» проєктів або бізнес-діяльності. Зелені проєкти можуть включати будівництво потужностей з відновлюваних джерел енергії, чистої транспортної інфраструктури або енергоефективних будівель тощо.

Фінансування зелених проєктів в Україні можливе в декілька способів: а) кредитування в українських банках та міжнародних фінансових інститутах (IFC, EBRD, EIB, World Bank), б) участь у міжнародних донорських програмах та грантах, в) випуск «зелених» облігацій (Green bonds)[2].

При цьому, більшість фінансових інструментів не використовуються в Україні. Основною перепоною для ефективного розвитку цієї

року). Харків: НДІ ПЗІР НАПрН України, 2023. С. 42-48. URL: https://ndipzir.org.ua/wp-content/uploads/2023/09/conf_29.09.23.pdf.

[1] Тотєва Е. Звіт 2022. Зелена таксономія в Україні. URL: https://www.undp.org/sites/g/files/zskgke326/files/2022-08/UNDP-UA-green-taxonomy-report-UKR.pdf.

[2] Перелигіна-Ковальчук Г. Перспективи розвитку ринку «зелених» облігацій в Україні. URL: https://jurliga.ligazakon.net/analitycs/186379_perspektivi-rozvitku-rinku-zelenikh-oblgatsy-v-ukran.

галузі в Україні є висока вартість проектів та їх низька інвестиційна привабливість з огляду на ряд негативних чинників: низький суверенний рейтинг, недосконале законодавче урегулювання галузі, недостатня кількість фінансових інструментів інвестування.

В останні роки у відповідь на значне зростання потреб глобальної економіки у переході на модель сталого розвитку потужного імпульсу розвитку отримала сек'юритизація активів зелених банків. Ця глобальна тенденція розвитку світового ринку зелених кредитів полягає в об'єднанні різного роду активів, емісії під них цінних паперів з подальшим їх продажом інвесторам.

До категорії зеленої сек'юритизації відносяться три види паперів: 1) забезпечені зеленими активами; 2) забезпечені пулом зелених кредитів; 3) розміщені для фінансування зелених проєктів.

Сек'юритизація, забезпечена зеленими активами, є класичною ABS (asset-backed security – це інструменти, що підтримуються фондами стійких активів), активами для якої виступають екологічні засоби виробництва: вітряні та сонячні генератори енергії, електромобілі тощо.

Сек'юритизація, забезпечена пулом зелених кредитів, може бути як ABS, так і MBS (mortgage-backed security – іпотечні цінні папери є інвестиційними продуктами, подібними до облігацій), оскільки до цієї групи кредитів відносяться будь-які цільові позики, видані на розвиток зелених ініціатив. Серед таких кредитів можна виділити, наприклад, іпотечні кредити на будівництво енергозберігаючих будинків та кредити, видані підприємствам на реалізацію екологічних проектів[1].

Сек'юритизація, розміщена з метою залучення коштів на зелені проєкти, по суті не відрізняється від звичайних зелених облігацій, оскільки визначальним критерієм виступають цілі розміщення: якщо вони задовольняють принципам ESG, сек'юритизація є зеленою.

Щодо можливості використання цих фінансових інструментів в Україні та їх правового забезпечення, то необхідно наголосити, що

[1] Єфремова К. В. Зелені фінансові інструменти у економіки України. *Інновації для відродження: національний, регіональний, міжнародний контекст*: Тези доповідей міжнародної науково-практичної конференції (м. Запоріжжя, 12-13 жовтня 2023 р.). Запоріжжя: НУ «Запорізька політехніка», 2023. С. 211-214.

в цьому році Національна комісія з цінних паперів та фондового ринку затвердила Концепцію запровадження законодавчої бази щодо облігацій з покриттям та сек'юритизації в Україні, в якій описані найпоширеніші альтернативні форми сек'юритизації та облігацій з покриттям, а саме: синтетична сек'юритизація (передача ризику за активами без залучення фінансування) та сек'юритизація майбутніх надходжень (використання активів, права за якими ще не виникли)[1].

На думку багатьох вчених, механізм сек'юритизації активів має позитивний вплив на економіку країни загалом, що виявляється в стимулюванні економічного зростання та розвитку фондового ринку, більш ефективному розподілі ризиків у фінансовому секторі, здешевленні та збільшенні тривалості кредитів для споживачів, зниженні інфляції, зростанні капіталізації та покращенні ліквідності банківської системи, нарощенню внутрішніх і зовнішніх інвестицій. А щодо саме зеленої сек'юритизації, то вона може бути економічно ефективним рішенням для корпорацій і фінансових установ для фінансування екологічних ініціатив.

Таким чином, механізм сек'юритизації активів має позитивний вплив на економіку країни загалом, що виявляється в стимулюванні економічного зростання та розвитку фондового ринку, більш ефективному розподілі ризиків у фінансовому секторі, здешевленні та збільшенні тривалості кредитів для споживачів, зниженні інфляції, зростанні капіталізації та покращенні ліквідності банківської системи, нарощенню внутрішніх і зовнішніх інвестицій. А щодо саме зеленої сек'юритизації, то вона може бути економічно ефективним рішенням для корпорацій і фінансових установ для фінансування екологічних ініціатив – це особливо актуально для повоєнного відновлення економіки України[2].

[1] Концепція запровадження законодавчої бази щодо облігацій з покриттям та сек'юритизації в Україні: Рішення Національної комісії з цінних паперів та фондового ринку від 14 лютого 2023 року № 139. URL: https://zakon.rada.gov.ua/rada/show/v0139863-23#Text.

[2] Єфремова К. В. Зелені фінансові інструменти у економіки України. *Інновації для відродження: національний, регіональний, міжнародний контекст*: Тези доповідей міжнародної науково-практичної конференції (м. Запоріжжя, 12-13 жовтня 2023 р.). Запоріжжя: НУ «Запорізька політехніка», 2023. С. 211-214.

Цифрова трансформація може позитивно вплинути на екологічну стійкість завдяки розумнішому управлінню поводженню з відходами, запобіганню та контролю забруднення, а також сталому управлінню ресурсами в реальному часі. З точки зору управління, цифрова трансформація має потенціал для підвищення прозорості та підзвітності, обмеження бюрократії і корупції, ухилення від сплати податків і полегшення взаємодії громадян з урядами[1].

## 5.5. Запровадження індексу цифрової економіки та суспільства

Поточний геополітичний контекст із вторгненням росії в Україну робить впровадження інноваційних цифрових рішень, технологій та розвиток цифрових інфраструктур, заснованих на цінностях і принципах ЄС, а також зміцнення кібербезпеки ще більш актуальним. Наприклад, значні небезпеки та ризики, які становить дезінформація в Інтернеті для безпеки життєдіяльності та оборони, для повноцінного функціонування суспільно необхідних інституцій і економіки, були продемонстровані як найяскравіше.

У результаті інституції ЄС та національні органи влади активізували співпрацю та обмін інформацією щодо кібербезпеки. Крім того, перегляд Кодексу практики ЄС щодо дезінформації та Закону про цифрові послуги забезпечить ефективні засоби для того, щоб онлайн-платформи вживали рішучих заходів для протидії дезінформації, особливо щодо протидії незаконному контенту в Інтернеті.

Варто зазначити, що ЄС проводить комплексну політику у сфері цифрової економіки та цифрової трансформації, створюючи цілу

[1] Єфремова К. В. Динаміка цифрової трансформації та зелений перехід. Збірник наукових праць НДІ ПЗІР НАПрН України : Цифрові трансформації України 2023: виклики та реалії : за матеріалами IV Круглого столу (м. Харків, 29 вересня 2023 року). Харків: НДІ ПЗІР НАПрН України, 2023. С. 42-48. URL: https://ndipzir.org.ua/wp-content/uploads/2023/09/conf_29.09.23.pdf.

екосистему. Тому, для України важливо та необхідно формувати координовані з ЄС політики, беручи до уваги стратегічні документи ЄС в комплексі[1]. Такий підхід дозволяє здійснювати коригування відповідних політичних дій впродовж виконання показників, які потребують додаткової уваги, зокрема, фінансування.

Важливими є саме незалежні інструменти моніторингу реалізації програм цифрової трансформації та конкурентоспроможності економіки, наприклад Індекс Цифрової Економіки та Суспільства (DESI), що дозволяє інвесторам та міжнародним партнерам відстежувати прогрес кожної держави-члена ЄС у розбудові цифрової економіки та суспільства. Індекс цифрової економіки та суспільства (DESI) – це зведений індекс, який узагальнює відповідні показники з ефективності цифрових технологій в Європі і відстежує еволюцію держав-членів ЄС в сфері цифрової конкурентоспроможності[2].

Індекс DESI охоплює п'ять основних областей: зв'язок, людський капітал, використання Інтернету, інтеграція цифрових технологій і цифрові державні послуги. DESI вимірює показники цифрової економіки 27 держав- членів ЄС та ЄС загалом у порівнянні з 19 іншими країнами світу (Австралія, Албанія, Боснія та Герцеговина, Бразилія, Канада, Чилі, Ісландія, Ізраїль, Японія, Мексика, Чорногорія, Північна Македонія, Норвегія, Сербія, Південна Корея, Швейцарія, Туреччина, Великобританія та Сполучені Штати). I-DESI має на меті відобразити та розширити результати Індексу цифрової економіки та суспільства (DESI) Європейської комісії шляхом пошуку показників, які вимірюють подібні змінні для країн, що не входять до ЄС[3].

[1] На шляху до Єдиного цифрового ринку ЄС: електронна комерція, телекомунікації, довірчі послуги. Український центр європейської політики. 2021. URL: https://ucep.org.ua/doslidzhennya/na-shlyahu-do-yedynogo-czyfrovogo-rynku-yes-elektronna-komercziya-telekomunikacziyi-dovirchi-poslugy.html.

[2] The Digital Economy and Society Index (DESI). European Commission. 2022. URL: https://digital-strategy.ec.europa.eu/en/policies/desi.

[3] Шляхи імплементації європейської політики впровадження цифрових технологій: монографія /за ред. К. В. Єфремової. Харків: НДІ прав. забезп. інновац. розвитку НАПрН України, 2022. С. 21.

Таким чином, необхідно замислитися щодо побудови екосистеми DESI в Україні. Цифровізація державних сервісів, бізнесу та доступ до технологій відкривають безліч можливостей. Важливо зрозуміти прогрес держави у цій сфері та покращувати цифровий досвід громадян шляхом запровадження DESI в Україні[1].

16 листопада 2022 р. проєкт EU4DigitalUA разом із місією технічної допомоги та обміну інформацією (TAIEX) Європейської Комісії провів воркшоп щодо створення передумов впровадження DESI в Україні. У ньому взяли участь Мінцифри, Державна служба статистики, Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації НКРЗІ та Міністерство економіки України, а також іноземні експерти із різних відомств країн ЄС.

Так, експерти з Фінляндії та Естонії надали консультації щодо законодавчої та інституційної бази, включаючи координацію між державними органами, і поділилися своїм досвідом щодо практичних питань, що виникли під час впровадження індексу.

Проєкт EU4DigitalUA підтримує впровадження DESI в Україні, а запрошені експерти аналізують нормативно-правову та політичну базу збору цифрових даних та допомагають створити передумови для застосування DESI в Україні. Саме тому вітчизняним науковим інституціям, фундаментальні дослідження яких спрямовані на супутні теми, необхідно долучитися до такого аналізу та підготовити власні пропозиції щодо такого впровадження.

Запровадження індексу DESI в Україні є необхідною передумовою інтеграції до ЄС в цифровій сфері. Відповідно до Угоди про асоціацію між Україною та ЄС, підписаною ще у 2014 році, уряд України зобов'язався привести своє законодавство у відповідність до стандартів ЄС. У правовому полі прийнято Концепцію та План дій з розвитку цифрової економіки та суспільства України, однак потрібна

[1] Єфремова К. В. Індекс цифрової економіки та суспільства в Україні як необхідна передумова інтеграції до ЄС. Зб. наук. праць НДІ ПЗІР НАПрН України: «Актуальні питання розбудови науково-дослідницької інфраструктури у воєнний та повоєнний періоди» за матеріалами Інтернет-конференції (м. Харків, 28 лютого 2023 року). Харків: НДІ ПЗІР НАПрН України, 2023. С. 49-57.

більш сучасна цифрова стратегія, узгоджена з останніми стратегіями ЄС.

Встановивши цілісну юридичну, політичну, інституційну, координаційну та методологічну структуру DESI, український уряд зможе не лише вимірювати та відстежувати, а й формувати політику цифрової трансформації на основі даних.

У 2022 році була створена робоча група, в яку увійшли представники ключових державних органів, що працюють над включенням України до DESI. В рамках дій робочої групи за підтримки експертів EU4DigitalUA було підготовлено звіт та інші аналітичні матеріали, які оцінюють поточний стан та визначають необхідні кроки для включення України в DESI. Національна рада з відновлення України від наслідків війни відповідно до Указу Президента від 21 квітня 2022 року No 266/2022 в рамках плану заходів з післявоєнного відновлення та розвитку України розробила План робочої групи з питань діджиталізації, який включає в себе такі етапи:

1) етап економіка та інститути воєнного часу – «Все для перемоги!» – на період до кінця до 2022 року;

2) етап відновлення – «Відновлення, перезапуск економіки та інститутів» – показники досягнення цілей та середньострокові завдання на період 2023-2025 роки;

3) етап модернізації «Структурна модернізація та повноцінна інтеграція до ЄС» – на період 2026-2032 роки[1].

В межах другого етапу запланований до розроблення проєкт постанови Кабінету Міністрів «Про запровадження національної системи показників цифрової економіки та суспільства», завданням якої є надати поштовх для створення екосистеми DESI в Україні.

Відповідальними за виконання створення умов для включення України до європейського індексу цифрової економіки та суспільства (DESI): впровадження європейських підходів до вимірювання та запровадження національної економіки та моніторингу прогресу циф-

[1] Проект плану робочої групи з питань діджиталізації. Урядовий портал. 2022. URL: https://uploads- ssl.webflow.com/625d81ec8313622a52e2f031/62c1aff95a97c394e066f05d_Діджи талізація.pdf.

рового розвитку держави, визначені Міністерство цифрової трансформації України, Державна служба статистики України, Національна комісія, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв`язку, Міністерство економіки України[1].

Впровадження DESI в Україні дасть змогу визначити динаміку та прогрес цифрового розвитку, порівнюючи з цифровими економіками ЄС, і таким чином сприятиме інтеграції до Єдиного цифрового ринку ЄС. Розглядаючи досвід ЄС на напрямки європейської політики в цифровій сфері, необхідно звернути увагу на програму «Шлях до цифрового десятиліття», що підтримує оновлений акцент на цінностях ЄС, стійкості та безпеці, пов'язуючи конкретні цифрові цілі з ціннісними цілями та цифровими принципами. Лише під час реалізації цифрового суверенітету ЄС може сформувати свою цифрову трансформацію відповідно до європейських цінностей.

Кожна держава-член ЄС робитиме свій внесок у досягнення загальної мети з різної початкової точки, виходячи з наявних ресурсів, порівняльних економічних переваг і суспільних потреб. Після того, як Програма набуде чинності, показники кожної держави-члена DESI розглядатимуться з точки зору їх майбутнього внеску в Європейське цифрове десятиліття.

Інструмент технічної підтримки забезпечує держави-члени у плануванні, розробці та впровадженні реформ цифрової сфери. Підтримка надається за запитом і охоплює широкий спектр сфер, включаючи реформи та інвестиції, пов'язані з цифровою трансформацією в рамках Планів відновлення та стійкості.

Так, 21 із 25 схвалених планів, за винятком Болгарії, Данії, Мальти та Швеції, беруть на себе зобов'язання щодо ключових багатонаціональних цифрових проектів, представлених у комунікації «Цифровий компас» і в політичній програмі «Шлях до цифрового десятиліття». Загалом понад 60 заходів стосуються багатонаціональ-

[1] Робочі групи. Національна рада з відновлення України від наслідків війни. Урядовий портал. 2022. URL: https://www.kmu.gov.ua/diyalnist/nacionalna-rada-z-vidnovlennya-ukrayini-vid- naslidkiv-vijni/robochi-grupi.

них цифрових проєктів на загальну суму близько 5 мільярдів євро. Два потенційних важливих проекти спільного європейського інтересу (IPCEI) з мікроелектроніки (12 планів) і хмарних технологій (7 планів) є одними з багатонаціональних проектів із найбільшим охопленням. Кілька Планів відновлення та стійкості (RRP) також включають інвестиції в багатонаціональні проекти, пов'язані з Європейськими центрами цифрових інновацій, коридорами 5G і квантовим зв'язком. Основними пріоритетами щодо впровадження та фінансування можна визначити такі напрями:

а) Європейські центри цифрових інновацій;

б) 5G коридори;

в) хмара (хмарні обчислення);

г) Євро квант;

ґ) обчислювальна техніка євровисокою продуктивністю;

д) електронне врядування (державне управління);

е) Геном Європи (багатонаціональний проект, розроблений і координований за підтримки B1MG; об'єднує європейські країни для створення високоякісної європейської мережі національних геномних еталонних когорт, що репрезентують європейське населення);

є) підводні кабелі;

ж) блокчейн (EBSI);

з) операційні центри безпеки;

і) цифрові навички та освіта.

Європейська комісія запропонувала Рішення про створення політичної програми до 2030 року «Шлях до цифрового десятиліття», щоб надати державам-членам можливість досягти спільного прогресу у формуванні цифрової трансформації. Цю пропозицію було прийнято 15 вересня 2021 року у відповідь на заклик Ради Європейського Союзу після повідомлення «Цифровий компас 2030: європейський шлях до цифрового десятиліття». Зокрема, у ньому встановлюються спільні цифрові цілі, яких ЄС загалом має досягти до 2030 року. Декларація про цифрові права та принципи, запропонована Комісією 26 січня 2022 року, доповнює цілі зі спільною довідковою структурою, яка спрямована на те, щоб керувати політиками

та приватними учасниками у формуванні Цифрового десятиліття відповідно до європейських цінностей, а також прав і свобод, закріплених у правовій базі ЄС[1].

У свою чергу, Україна використовуючи досвід ЄС, у серпні 2022 р. в межах проєкту EU4DigitalUA розпочала розробку державної інформаційної системи e-Permit. Розробка фінансується Європейським Союзом, бенефіціар проєкту – Міністерство цифрової трансформації, реципієнт – Міністерство економіки[2].

Завдяки e-Permit отримання ліцензій та дозвільних документів стане зручнішим. E-Permit цифровізує та спростить процедури ліцензування та надання дозволів, подання документів здобувачів ліцензії та ліцензіатів за допомогою електронних кабінетів. Структура, процес розробки і використання електронної системи дозволятимуть легке оновлення бізнес- процесів електронних сервісів, а також подальшу модернізацію системи е-Дозвіл.

Таким чином, України демонструє готовність до співпраці щодо цифрової трансформації та гармонізації з Єдиним цифровим ринком ЄС, включаючи посилену кібербезпеку та захист даних, імплементацію Угоди про асоціацію між Україною та ЄС.

[1] Єфремова К. В. Індекс цифрової економіки та суспільства в Україні як необхідна передумова інтеграції до ЄС. Зб. наук. праць НДІ ПЗІР НАПрН України: «Актуальні питання розбудови науково-дослідницької інфраструктури у воєнний та повоєнний періоди» за матеріалами Інтернет-конференції (м. Харків, 28 лютого 2023 року). Харків: НДІ ПЗІР НАПрН України, 2023. С. 49-57.

[2] EU4DigitalUA завершив розробку технічного завдання для системи e-Permit. EU4DigitalUA. 2022. URL: https://eu4digitalua.eu/news/eu4digitalua-zavershyv-rozrobku-tehnichnogo- zavdannya-dlya-systemy-e-permit/.

# 6. МЕРЕЖІ ТРАНСФЕРУ ТЕХНОЛОГІЙ: СУТНІСТЬ, ПРИНЦИПИ ТА АСПЕКТИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Процес трансферу технологій забезпечує розвиток галузей промисловості, є основою якісних змін в економіці в цілому, на 75–80% визначають приріст ВВП розвинутих країн. Серед основних видів трансферу технологій можна виділити наступні: передача патентів на винаходи, передача «ноу-хау», інжиніринг, інформаційний обмін через персональні контакти, наукові дослідження та розробки під час програм обміну вченими та спеціалістами, а також організування спільного виробництва. Розрив між створенням новітньої технології та її впровадженням в промисловість розвинені країни постійно скорочують. Завдяки цьому використання та впровадження технологій відбувається все швидше та ефективно їх використовувати.

У наслідок активного пошуку нових напрямів промислового розвитку, сформувалася підвищена увага науковців та виробників до процесу створення та впровадження інноваційних продуктів, серед яких найбільш цікавими для дослідження є інтелектуальні технологічні розробки. У цьому ланцюгу особливу актуальність має процес передачі технології від наукової сфери до промислового сегмента, від розробників до виробників, тобто трансферу технологій (далі ТТ).

Незважаючи на значну кількість теоретичних наукових досліджень та набутого за останні роки практичного досвіду низький рівень правового регулювання ТТ в Україні вимагає прийняття важливих рішень, які б забезпечили ефективні підходи до законодавчого забезпечення цього процесу від ідеї до практичного результату. Зо-

крема, необхідне вироблення спільної думки щодо визначення змісту дефініції «трансфер технології» та відмінності цього терміна від близьких за змістом та наповненням дефініцій «трансфер інформації», «комерціалізація технології».

Теоретичні та методичні положення ТТ були досить актуальною проблемою в наукових розробках багатьох вчених. Поняття трансферу технологій (англ. Transfer – передача, від лат. Transferre – передавати; від грец. τεχνολογια, що походить від грец. τεχνολογος; грец. τεχνη – майстерність, техніка; грец. λογος — передавати) використовується в світовій практиці досить широко.

З наукової точки зору і сьогодні не маємо єдиного визначення поняття «трансфер технологій», оскільки науковці різних галузей трактують його через особливості своєї сфери діяльності. Швидкість виникнення нових форм передачі технологій заважає надати усталене визначення цього поняття. Так, серед наукових підходів до розглядуваного поняття можна згадати Л. І. Федулову, яка визначає ТТ як передачу систематичного знання про виробництво продукції, застосування процесу чи надання послуг[1]. У свою чергу, О. Б. Бутнік-Сіверський розуміє ТТ як термін, що поєднує у собі наукові дослідження технології, її масштабування та оптимізацію, маркетинг, організацію збутової мережі. Із ним погоджуються О. П. Орлюк, С. Ф. Ревуцький, В. І. Нежиборець, Л. Ю. Федченко[2].

Є. І. Ходаківський вважає, що ТТ – це поширення науково-технологічних знань прикладного характеру відносно процесів, методів виробництва та інноваційних продуктів усередині галузі, між галузями та між країнами, яке включає комерціалізацію наукових розробок, тобто передачу нової технології (інновації) в комерційне використання, а також поширення вже існуючих технологій.

[1] Федулова Л. І. Економічна природа технологій та технологічного розвитку. *Економічна теорія.* 2006. № 6. С. 3-16.

[2] Омельяненко В. А. Методичні основи оцінки потенціалу трансферу технологій : монографія. Становлення економіки України у післякризовий період: ризики та проблеми розвитку ; під ред. д.е.н., проф. О. О. Непочатенко (Ч. 1). Умань. Видавець «Сочінський», 2012. С. 350–353.

Вагомим внеском у правове забезпечення ТТ став проект Міжнародного кодексу поведінки у сфері передачі технологій, який пропонує таке визначення ТТ: передача систематизованих знань для випуску відповідної продукції, застосування відповідного процесу або для надання відповідних послуг, яка не поширюється на правочини, пов'язані з продажем або орендою товарів[1].

Наведені визначення ТТ підкреслюють знаннєвий характер цього явища: йдеться не про передачу прав власності на речі, а про розповсюдження інформації про результати інтелектуальної діяльності, інтелектуальні продукти та умови їх реалізації/застосування при виробництві продукції, наданні послуг, виконанні робіт.

Саме тому ТТ відіграє визначальну роль у поширенні об'єктів права інтелектуальної власності. У широкому розумінні він означає взаємодію між двома або більше партнерами, де хоча б один із них передає інформацію про свою технологію та надає (передає) права інтелектуальної власності на неї через ноу-хау, патенти і технічне сприяння іншому партнерові, який бажає впровадити й використовувати цю технологію для конкретної мети. Такий підхід підтримують В. Омельяненко[2].

Слід звернути увагу, що цим визначенням вони не трактують ТТ як комерційне явище, оскільки він може слугувати збільшенню суми знань однієї зі сторін без будь-якої фінансової угоди. Проте основне значення ТТ полягає у тому, що користь від нього на взаємовигідній основі повинні одержати обидві сторони. Як зазначають згадані науковці, одержувач технології, наприклад, може придбати ноу-хау

[1] Draft International Code of Conduct on the Transfer of Technology. U.N. Doc. TD/CODE TOT/47 (1985) 2 Лукша О., Пильнов Г., Тарасова О., Яновский А. Как работать с сетями трансфера технологий: практическое пособие; проект EuropeAid «Наука и коммерциализация технологий». 2006. 140 с. 3 Омельяненко В. А. Методичні основи оцінки потенціалу трансферу технологій : монографія. Становлення економіки України у післякризовий період: ризики та проблеми розвитку ; під ред. д.е.н., проф. О. О. Непочатенко (Ч. 1). Умань. Видавець «Сочінський», 2012. С. 350–353.

[2] Омельяненко В. А. Методичні основи оцінки потенціалу трансферу технологій : монографія. Становлення економіки України у післякризовий період: ризики та проблеми розвитку ; під ред. д.е.н., проф. О. О. Непочатенко (Ч. 1). Умань. Видавець «Сочінський», 2012. С. 350–353.

і отримати технологічну перевагу над конкурентами, а власник технології – певну фінансову перевагу від співробітництва і розробити інші технологічні рішення для підвищення конкурентоспроможності, зниження собівартості, збільшення прибутку.

У вузькому розумінні, на думку В. К. Хаустова, ТТ – це процес передачі технологій, в основі яких завжди лежить об'єкт інтелектуальної власності, зі сфери їхнього розроблення до сфери практичного використання[1].

ТТ обов'язково передбачає отримання інформації про зміст технології та право її використовувати реципієнтом, який і здійснює її промислове освоєння, практичне застосування, впровадження, що не обов'язково має бути спрямоване на отримання прибутку. Крім того, ТТ включає в себе процес комерціалізації результатів фундаментальних і прикладних наукових досліджень, науково-технологічних розробок, тобто фактично надання доступу, розповсюдження нових спеціалізованих знань, необхідних для використання технології та її інтелектуальних складових частин.

В офіційних документах Конференція ООН з питань торгівлі та розвитку (UNCTAD) 2001 р. визначає ТТ як процес поширення комерційної технології у формі передачі технології, який може бути захищений юридичним договором, а може і не бути, але включає взаємозв'язок (комунікацію) між особою, яка передає відповідні знання, і особою, яка їх набуває.

У методологічних і прикладних документах, розроблених Організацією економічного співробітництва та розвитку (ОЕСР), у поняття «трансфер технологій» включається широке коло комерційних угод: з передачі технічних засобів за допомогою патентів і ліцензій, передачі ноу-хау; з трансферу проектів, торгових марок і зразків; з надання послуг технічного характеру, включаючи технічне та інжинірингове навчання, а також технічну допомогу; з передачі результатів НДДКР.

[1] Хаустов В. К. Трансфер технологій в інноваційних процесах України та Білорусі. *Економіка і прогнозування.* 2012. № 2. С. 24–34. 2 United Nations Conference on Trade and Development: Transfer of technology. New York; Geneva, 2001. URL: http://www.unctad.org/en/ docs//psiteiitd28.en.pdf.

Рада з наукових та промислових досліджень (CSIR) – це організація досліджень та розробок, яка створена на підставі акту парламенту Індії в 1945 р.[1]. Вона проводить цілеспрямовані міждисциплінарні дослідження і технологічні інновації, які сприяють підвищенню якості життя південноафриканців. Організація відіграє ключову роль у підтримці урядових програм за допомогою спрямованих досліджень, які відповідають пріоритетам країни, статуту організації та її науково-технічним і технологічним компетенціям. На своєму офіційному сайті CSIR визначає ТТ як процес, при якому інтелектуальна власність перетворюється на фізичний продукт або процес, який генерує комерційну вигоду або може бути використаний на благо суспільства.

Нормативне визначення поняття «трансферу технологій» закріплено у Законі України «Про державне регулювання діяльності у сфері трансферу технологій»: під ним розуміється передача технології, що оформляється шляхом укладення між фізичними та/або юридичними особами двостороннього або багатостороннього договору, яким установлюються, змінюються або припиняються майнові права та обов'язки щодо технології та/або її складових[2]. На наш погляд, таке визначення є дещо вузьким і характеризує процес ТТ як певну ринкову угоду – правочин між продавцем та покупцем такого товару з приводу результату інтелектуальної діяльності.

У Методичних рекомендаціях щодо створення та діяльності центрів ТТ (затверджені Наказом Держінформнауки від 27.12.2010 р. № 150) визначено можливі шляхи створення та основні напрями діяльності центрів трансферу технологій із врахуванням світового досвіду у сфері розвитку центрів трансферу технологій і наведено таке визначення: «Трансфер технології – передача технології, що оформляється шляхом укладення двостороннього або багатосторон-

[1] The Council for Scientific and Industrial Research. URL: http://www.csir.co.za/index.html.

[2] Про державне регулювання діяльності у сфері трансферу технологій : Закон України від 14.09.2006 № 143-V. *Відомості Верховної РадиУкраїни*, 211 2006, № 45, ст. 434.

нього договору між фізичними та/або юридичними особами, яким установлюються, змінюються або припиняються майнові права і обов'язки щодо технології та/або її складових. Метою трансферу технологій може бути як комерційне використання технологій (у виробництві товарів та послуг, залучення додаткових ресурсів для подальших досліджень і розробок тощо), так і некомерційне їх використання»[1].

Цікавим у розглядуваному контексті є американський досвід: законодавство США не визначає поняття «трансфер технологій», проте існують кілька базових визначень, прийнятих відомими суб'єктами ТТ у США:

1) «процес використання технології, знань, ноу-хау або обладнання з метою, яка не була передбачена його розробниками. ТТ може привести до її комерціалізації або модифікації продукту або процесу» (визначення Національного центру трансферу технологій);

2) «процес, який дозволяє використовувати існуючі, розроблені в рамках бюджетного фінансування знання, обладнання або потужності з тим, щоб задовольнити певні суспільні або приватні потреби» (визначення Федерального консорціуму лабораторій);

3) «формальна передача нових знань або інновацій, отриманих у результаті науково-дослідних робіт в університетах і неприбуткових дослідних організаціях, у комерційний сектор для загальної вигоди» (визначення Асоціації університетських менеджерів технологій).

Хоча наведені визначення відрізняються між собою, проте погоджуємося з Федуловою Л. І., що закладена в них головна ідея однакова – це просування технології на шляху до її практичного використання з отриманням прибутку чи іншої користі[2].

Крім того, на нашу думку, у визначеннях Національного центру трансферу технологій США та Федерального консорціуму лабораторій США акцент зроблений не лише на факті передачі – вказується

[1] Федулова Л. І. Розбудова системи трансферу технологій – важлива умова впровадження кластерної моделі розвитку економіки України. *Актуальні проблеми розвитку економіки регіону*. 2011. Вип. 7(2). С. 275-284.

[2] Там само.

на процес використання технології. Вважаємо, що в разі такого підходу ТТ націлений не просто на дифузію нового знання, передання інформації про отримані нові інтелектуальні продукти, – його метою слід визнавати практичне використання іншими суб'єктами господарювання. У той же час ТТ є завершеним з моменту укладення відповідного договору, на підставі якого користувач технології отримує право на її використання та/або інформацію про зміст та умови її реалізації, впровадження. Сам же реальний факт її застосування у реальному секторі економіки не впливає на правову характеристику передачі технології, однак свідчить про її економічний ефект.

Трансфер і комерціалізація технологій відносно самостійні процеси і можуть існувати окремо один від одного, проте вони можуть бути і пов'язані у випадку, коли в результаті ТТ виникає можливість успішної комерціалізації.

Технологія як об'єкт трансферу, як вважають Є. І. Ходаківський, В. П. Якобчук, І. Л. Литвинчук, може бути в окремих випадках конкретним об'єктом предметного типу, що сам по собі технологією як такою не є. Однак із цим об'єктом обов'язково пов'язані ті або інші вміння й навички, та / або інша технологія (виробництва, застосування чи впровадження). Тому автори зазначають, що об'єктом трансферу є інформація у різних формах, в тому числі й про методи її практичного використання[1].

У свою чергу В. П. Соловйов стверджує, що ТТ завжди передує процесам їх комерціалізації і базований на сукупності специфічних явищ і процесів. Комерціалізація технологій означає перетворення технологій на джерело прибутку, тобто її визначають як будь-яку діяльність, спрямовану на отримання доходу від використання результатів наукових досліджень, вмінь і навичок набутих від володіння певною технологією[2]. Таке визначення, на наш погляд, більшою мірою

[1] Ходаківський Є. І., Якобчук В. П., Литвинчук І. Л. Інтелектуальна власність : економіко-правові аспекти. К. Центр учбової літератури. 2014. 276 с. URL: http://pidruchniki.com/1356061563567/pravo/tipi_formi_tehnologichnogo_transferu.

[2] Родіонова І. В. Основні форми та етапи здійснення трансфера технологій промислових підприємств. *Вісник Запорізького національного університету*. № 3 (15). 2012. С. 60–64.

притаманне неринковим формам господарювання, так як це було, наприклад, у системі соціалістичних відносин, де комерційному впровадженню досить часто передує некомерційна апробація інтелектуальної розробки. У ринкових умовах такого роду ситуації зустрічаються вкрай рідко (наприклад, у сфері унікального обладнання, оборонного комплексу тощо), у переважній кількості випадків такий двоетапний процес ТТ (некомерційний, а потім комерційний) практично не зустрічається, крім випадків, коли відповідні вимоги про проведення випробувань вимагаються чинним законодавством (наприклад, розроблення нових фармацевтичних препаратів).

Професор О. М. Ляшенко виділяє дві відмінності, які варто враховувати при визначенні трансферу та комерціалізації технологій.

Перша пов'язана з тим положенням, що «комерціалізація технології передбачає обов'язкове одержання прибутку від її використання у господарській діяльності і не обов'язково пов'язана із залученням у цей процес третіх осіб»; друга – це визначення ТТ як «обов'язкової передачі технології реципієнтові, котрий і здійснює її промислове освоєння, але це не обов'язково пов'язано з отриманням прибутку сторонами»[1]. У цьому визначенні проглядається певна незалежність термінів «комерціалізація» і «трансфер», відсутність їх поєднання та тісного взаємозв'язку.

Відокремлення в теоретико-методичному розумінні процесу комерціалізації технологій від їх трансферу підтримує і А. В. Косенко, який стверджує, що «комерціалізація об'єктів інтелектуальної власності – це самостійний процес перетворення результатів науковотехнічної та інноваційної діяльності в товар і їх ефективна реалізація в промислових масштабах. Комерціалізація є найважливішим елементом інноваційного процесу»[2]. Певна фетишизація терміна «комерціалізація» і приниження терміна «трансфер» в працях А. В. Косенка, на наш погляд, є надмірними. Є. І. Ходаківський, В. П. Якобчук,

[1] Ляшенко О. М. Методи та моделі комерціалізації трансферу технологій : дис. д-ра економ. наук. К., 2009. 504 с.

[2] Косенко А. В. Організаційно-економічний механізм комерціалізації об'єктів інтелектуальної власності підприємства : дис. канд. економ. наук. Харків. 2009. 215 с.

І. Л. Литвинчук виокремлюють: некомерційний трансфер, який найчастіше використовується в галузі наукових досліджень фундаментального та прикладного характеру, що супроводжується незначними витратами, може підтримуватися державою або проходити на основі особистих чи міжвідомчих контактів; трансфер комерційного характеру, що переважає у сфері виробництва та міжнародній економічній діяльності[1].

Базуючись на висновках В. П. Соловйова, О. М. Ляшенко, А. В. Косенка, І. В. Родіонова вважає, що «доцільним є сприйняття ТТ та комерціалізації технологій як двох автономних процесів інноваційної діяльності. Адже вони можуть відбуватись як послідовно, так і незалежно один від одного»[2]. Отже, зазначені науковці є прихильниками теорії самостійності процесів комерціалізації та ТТ, які реалізуються незалежно один від одного. Водночас така позиція не є однозначною та загальноприйнятою.

Дійсно, процес ринкового впровадження технологічного продукту частіше всього відбувається на комерційній основі, тобто його власник (правовласник) у результаті отримує дохід, передаючи свою розробку (права на неї) покупцю, тобто користувачу технологій. Такого роду трансферну операцію (технологічний трансфер) називають комерційним трансфером або комерціалізацією технології.

При цьому зазначимо, що практичне використання технологічного продукту може здійснюватися і без наявності комерційних відносин між розробником технології та її користувачем. Маємо численні приклади технологічного трансферу такого виду (некомерційного трансферу). Предметом некомерційного трансферу, наприклад, є наукові відкриття, оскільки на них не поширюються майнові права інтелектуальної власності, тому що, по суті, вони є відображенням

[1] Ходаківський Є. І., Якобчук В. П., Литвинчук І. Л. Інтелектуальна власність : економіко-правові аспекти. К. Центр учбової літератури. 2014. 276 с. URL: http://pidruchniki.com/1356061563567/pravo/tipi_formi_tehnologichnogo_transferu.

[2] Родіонова І. В. Основні форми та етапи здійснення трансфера технологій промислових підприємств. *Вісник Запорізького національного університету.* № 3 (15). 2012. С. 60–64.

об'єктивно існуючих закономірностей природи та соціуму, тобто досягненням всього людства; як правило, немає реальних передумов їхнього комерційного використання; і, нарешті, такі відкриття можуть бути здійснені відразу декількома дослідниками, як відомо з історії науки. Некомерційний трансфер по своїй суті притаманний екологічним, соціальним розробкам, тобто таким, практичне невикористання яких може завдати людству або глобальній економіці значної шкоди, а комерційне використання таких технологій або не має комерційного сенсу, або є занадто дорогим для окремого господарюючого суб'єкта.

Доповнює перелік певних відмінностей між термінами «трансфер» та «комерціалізація» В. В. Титов, який стверджує, що «на відміну від комерціалізації, ТТ передбачає не лише передачу інформації про інновацію, але і її освоєння за умов активної участі автора винаходу, реалізатору інформації та кінцевого споживача продукції, яка виготовляється за допомогою нової технології»[1]. Саме тому при передачі технології основна увага приділяється не стільки технології, скільки учасникам цього процесу.

О. С. Трофімчук твердить, що «сутність трансферу технологій полягає в передачі ноу-хау, нових технологій, технологічного знання та науково-технічних знань від власника до споживача (передачі технологій від науки до виробництва на рівні НДІ, дослідних лабораторій, ВНЗ, підприємств та інших організацій) та в здійсненні міжнародного обміну технологій»[2]. Таке визначення більш чітко визначає сутність дефініції, яка аналізується.

Всесвітня організація інтелектуальної власності (WIPO) на своєму офіційному сайти надає таке визначення: ТТ – це процес, в якому розробник технології робить свою технологію доступною для комерційного партнера, який буде її використовувати[3].

---

[1] Лихолет С. І. Трансфер технологій у системі інноваційної діяльності. *Економіка та держава.* 2009. № 6. С. 37–38.

[2] Трофімчук О. С. Сутність поняття трансферу технологій та його ролі для розвитку України. URL: http://nauka.kushnir.mk.ua/?p=64546.

[3] Онищенко В. О., Комеліна А. А. Сучасні засади комерціалізації інноваційних технологій. *Економіка і регіон.* №4 (53). 2015. С. 3-9.

На думку Е. П. Зараменских, процес можна вважати ТТ, коли передача технологій закріплена юридичною угодою. У разі коли процес передачі технології відбувається без укладання юридичної угоди, його можна визначити як трансфер інформації. Автор наголошує, що трансфер інформації перетворюється на ТТ у момент юридичного засвідчення передачі технологій від власника до реципієнта. ТТ – це не одномоментна дія, а є процесом, у свою чергу укладання та підписання угоди є тільки одним з етапів цього тривалого процесу.

Згідно з офіційними рекомендаціями Організації з економічного співробітництва та розвитку (далі – OECD) ТТ – це передача науковотехнічних знань і досвіду для надання науково-технічних послуг, застосування технологічних процесів, випуску продукції[1].

Т. О. Зінчук визначає ТТ як послідовності дій, в ході яких нові знання, отримані в результаті фундаментальних та прикладних досліджень в університетах та науково-дослідних інституціях, вільно розповсюджуються, передаються через надання науково-технічних послуг або купуються підприємствами для впровадження в якості продукції чи технології. Комерціалізація технологій – це вид комерційного ТТ, в результаті якого відбувається реалізація інноваційної продукції та готових інноваційних технологій на ринку через пошук партнерів та потенційних покупців. Комерціалізацією технологій мають займатися професіонали з інноваційного менеджменту (провайдери) – підприємці та інвестори інноваційного бізнесу[2].

Наведені підходи до розуміння трансферу та комерціалізації технологій можна охарактеризувати як теорію єдності зазначених процесів, які мають спільний зміст правовідносин, однак відмінні за цілями – з метою отримання прибутку чи без такої мети, – та співвідносяться як родове та видове поняття.

[1] The Measurement of Scientific and Technological Activities. Proposed Standart Practice for Surveys on Research and Experimental Development: Frascati Manual. Paris: OECD Publishing, 2002. 256 p.

[2] Зінчук Т. О., Кащук К. М. Трансфер інноваційних технологій: сутність та значення у розвитку вітчизняної економіки. *Збірник наукових праць Таврійського державного агротехнологічного ун-ту (економічні науки)*. 2012. № 2(18). Т. 4. С. 199-208.

ТТ слід розглядати як один з аспектів інноваційного процесу, під яким розуміють процес перетворення наукового знання на інновацію, який можна уявити як послідовний ланцюг подій, у ході яких інновація визріває від ідеї до конкретного продукту, технології або послуги і поширюється при практичному використанні.

Таким чином, проаналізувавши дефініції поняття «трансфер технологій», надані як вітчизняними вченими та нормативними актами, оцінку діяльнотсті так і міжнародною науковою спільнотою, можна твердити про наявність двох основних концепцій визначення ТТ у співвідношенні з процесом їх комерціалізації: теорію єдності та теорію самостійності. Юридичне значення встановлення термінологічних зв'язків понять «трансфер технології» та «комерціалізація технологій» полягає у сфері законодавчого регулювання та формування економічної правової політики. Залежно від обраних державою завдань на конкретному технологічному укладі: належати до країн розробників технологій або країн технологічного авангарду, поєднувати такі стратегії або не визначати подібних цілей, – держава нормативно закріплює той підхід до визначення ТТ, який дозволяє їх досягти.

Відповідно у правовій площині отримало закріплення визначення ТТ у широкому та вузькому значенні. У разі широкого правового підходу до розуміння ТТ до нього відносять всі форми розповсюдження та передачі нових знань, навичок, результатів інтелектуальної діяльності самостійно або разом із матеріальними об'єктами, в яких вони реалізовані, або шляхом надання науковотехнічних послуг. У такому разі ТТ означає взаємодію між двома або більше партнерами, де хоча б один із них є розробником, автором, володільцем прав інтелектуальної власності на результати інтелектуальної діяльності, а другий одержує або нову для нього інформацію про такі результати, або майнові права інтелектуальної власності на них з метою подальшого комерційного або некомерційного використання при виробництві товарів, виконанні робіт, наданні послуг.

При вузькому законодавчому закріпленні визначення ТТ припускається передача майнових прав на нові розробки, результати

інтелектуальної діяльності третім особам на підставі юридично оформленого правочину (договору).

Порівняння законодавчих підходів до визначення ТТ дозволяє встановити принципову відмінність між українським та європейським законодавством у цьому питанні. Поняття ТТ у Законі України «Про державне регулювання діяльності у сфері трансферу технологій» відсилає до правочину, яким установлюються, змінюються або припиняються майнові права та обов'язки щодо технології та/або її складових, що кореспондує вузькому підходу до розуміння ТТ.

На відміну від нього у рекомендаціях OECD встановлення факту ТТ вимагає не лише передачі науково-технічних знань і досвіду, а й практичного їх застосування для надання науково-технічних послуг, здійснення технологічних процесів, випуску продукції із реалізацією в ній нових розробок. На нашу думку, європейське законодавство слідує широкому підходу до розуміння ТТ та відповідно до нього будує систему центрів та мереж для його забезпечення.

Передача нових технічних досягнень, розробок від наукових установ, авторів до третіх осіб відбувається за допомогою різних організаційних заходів та правових форм. Економічною наукою виділяються такі основні організаційні форми ТТ:

1) видача ліцензій, якими найчастіше передаються не найновіші технології, а так звані «технології проміжного покоління»;

2) передача ноу-хау у формі надання безпатентної ліцензії. При цьому передача ноу-хау має незворотний характер, із невизначеним періодом збереження конфіденційності ноу-хау та високим ризиком його розкриття третім особам після укладення контракту до закінчення його дії;

3) інжиніринг, який припускає виконання користувачем сукупності проектних і практичних робіт (консультаційних, технологічних, будівельних та ін.), необхідних для реалізації нової технології;

4) промислова кооперація, за якої сторони, які об'єдналися для організації кооперованого виробництва, здійснюють інтенсивний технологічний обмін для досягнення загальної мети з реалізації проекту за наявності власних кореспондуючих інтересів;

5) франшиза, що припускає передачу або переуступку (на комерційни умовах) суб'єктом господарювання із рентабельним бізнесом або відомою діловою репутацією дозволу продавати аналогічні товари, виконувати роботи або надавати послуги в деяких сферах третім суб'єктам для започаткування ними нового виду ділової активності, що включає й передачу необхідних навичок;

6) лізинг (фінансова оренда), за умовами якого лізингова компанія викуповує у постачальника обладнання і технологію і здає його в оренду на певний обумовлений строк. Після закінчення строку оренди орендар зобов'язаний повернути обладнання, технологію лізинговій компанії або викупити їх у свою власність за залишковою вартістю;

7) технічна допомога, яка надається на підставі окремої угоди або в межах угоди про передачу технології або постачання обладнання і полягає у виконанні досліджень, навчанні та підготовці кадрів із поєднанням елементів інжинірингових послуг, підрядних робіт, контрактів на оренду приладів та інструментів;

8) створення спільних підприємств з метою об'єднання зусиль, знань і досвіду у виробництві нової для даного ринку продукції та поділу спільного ризику;

9) сприяння взаємозв'язкам науки і промисловості з боку держави, зокрема, у формі часткового фінансування робіт фахівців (науковців, викладачів вузів, аспірантів, магістрантів і студентів старших курсів) для вирішення технологічних проблем підприємств.

Вітчизняні науковці виокремлюють форми здійснення ТТ залежно від його типу, а саме комерційного або некомерційного ТТ. Так, некомерційний трансфер здійснюється через передачу науково-технічної інформації шляхом публікації науково-технічної та навчальної літератури такої як наукові статті, довідники, стандарти, описи патентів, каталоги проспектів, Інтернет – публікації, а також через відкриті бази даних, інформаційні сайти, пошукові сервери, форуми, зустрічі, конференції, сесії, симпозіуми, виставки, круглі столи, проведення курсів навчання та стажування вчених на безкоштовній основі або на умовах власного фінансування.

До форм здійснення комерційного технологічного трансферу Ходаківський Є. І., Якобчук В. П. та Литвинчук І. Л. відносять передачу патентів на винахід та/або свідоцтв на промислові зразки та корисні моделі; ліцензування; організацію спільного виробництва, створення державно-приватного партнерства; створення start-up компаній («новачків»); інжиніринг; передачу супутніх купівлі чи оренді обладнання технологічних відомостей; включення об'єктів інтелектуальної власності до статутного капіталу інноваційних структур; міжнародне науково-технічне співробітництво у рамках технологічних платформ, участь у рамкових програмах[1].

На практиці зазначені форми ТТ застосовуються паралельно у межах одного проекту, доповнюють одна одну, особливо в масштабних проектах, у міждержавних угодах про промислово-інвестиційне співробітництво, науково-технічну та виробничу кооперацію.

Трансфер та комерціалізація технологій можуть бути послідовними стадіями інноваційного процесу. У результаті ТТ з'являється можливість успішної комерціалізації розробки та отримання доходу її автором, організацією-розробником і, як наслідок, збільшення податкових надходжень до національного і місцевого (регіонального) бюджетів, організації виробництва інноваційної продукції. Отже, у сучасних глобальних відносинах з розповсюдження нової інформації, поширення нових технологій, нових знань та навичок ТТ охоплює широке коло відносин, предметом яких виступають не лише конкретні результати інтелектуальної діяльності, а й інформація, роботи та послуги, спільна діяльність, навчання та підготовка як спеціальний вид послуг.

Але на практиці розробники і власники нових технологій – наукові організації, малі інноваційні фірми, організації інноваційної інфраструктури – важко знаходять покупців своїх розробок або партнерів для створення виробництв. Крім того, вчені здебільшого не володіють навичками ведення господарської діяльності, що необхідні для

[1] Ходаківський Є. І., Якобчук В. П., Литвинчук І. Л. Інтелектуальна власність : економіко-правові аспекти. К. Центр учбової літератури. 2014. 276 с. URL: http://pidruchniki.com/1356061563567/pravo/tipi_formi_tehnologichnogo_transferu.

створення власної справи. Існує й інша сторона цієї проблеми. Якщо компанія планує досягти конкурентних переваг шляхом вдосконалення технології своєї роботи, то неминуче виникає питання про те, де знайти інформацію про такі технології, які можуть забезпечити підвищення ефективності бізнесу[1].

Чимало експертів зазначають наступні проблеми, що перешкоджають інтеграції процесу трансферу технологій на українських підприємствах в міжнародні інноваційну систему:

1) зовнішня та внутрішня міграція науковців; 2) недостатні обсяги фінансування інноваційної діяльності; 3) низька інноваційна діяльність активних підприємств, що зумовлює скорочення частки інноваційної продукції як у структурі виробництва, так і в експорті;

4) низький рівень державної підтримки інновацій і попиту на високотехнологічну продукцію; 5) відсутність стимулюючих механізмів трансферу технологій.

З огляду на вказані проблеми у розвитку системи трансферу технологій, що в свою чергу буде сприяти повноцінному функціонування технологічної безпеки, вважаємо що побудова та функціонування єдиної мережі трансферу технологій позитивно вплине на ці проблеми і допоможе їх розв'язати. Мережа трансферу технологій – це об'єднання осіб - професійних учасників ринку трансферу технологій (зі створенням або без створення юридичної особи) з метою консолідації інформаційних ресурсів у технологічній сфері шляхом об'єднання нематеріальних об'єктів та/або інформації про них на електронному майданчику, спільних дій учасників та їх мережевої організації співпраці, у результаті діяльності якого відбувається передача прав інтелектуальної власності від авторів (розробників) до суб'єктів господарської діяльності, які використовують такі об'єкти при виробництві товарів, виконанні робіт, наданні послуг[2].

[1] Касич А. О. Звіт про стійкий розвиток як аналітичний інструмент формування корпоративної соціальної відповідальності. *Ефективна економіка*. 2014. № 10. URL: http//www.economy.nauka.com.

[2] Новіков Є. А. Господарсько-правове регулювання діяльності мереж трансферу технологій. Дис. ... канд. юрид. наук: 12.00.04. м. Київ. 27 жовтня 2018 р. 200 с.

Розглянемо ці перспективи більш детально крізь призму оголошених проблем.

1. Міграція науковців. Однією з причин міграції науковців є занадто складний пошук потенційних інвесторів та підприємств які були б зацікавлені в їх технологіях. Не знаходячи підтримки та допомоги, вони шукають інші шляхи реалізації свої інновацій, най вірогіднішою є виїзд за кордон. Саме для вирішення такої проблеми у Європі і створювались перші мережі трансферу технологій. Зі своїм завдання в країнах ЄС вони впоралися, більш того вони були на стільки успішними, що давно вже перестали бути просто мережею трансферу технологій, а вже виконують набагато більш широкі функції і інноваційному європейській системі[1].

2. Недостатні обсяги фінансування інноваційної діяльності. Звичайно на пряму мережі трансферу технологій не фінансують інноваційні проєкти, однак вони опосередковано впливають на збільшення можливостей фінансування інновацій, шляхом пошуку інвесторів для науковців як у середині країни так і за її межами. Що на наш погляд є доволі суттєвим фактором збільшення фінансових інструментів.

3. Низька інноваційна діяльність активних підприємств, що зумовлює скорочення частки інноваційної продукції як у структурі виробництва, так і в експорті. Така тенденція є доволі типовим фактором для нашої країни враховуючи що більшість підприємств є або не зацікавлені у розвитку та удосконаленні свого виробництва або ж не можуть знайти необхідні технології. Вплинути на підприємства які не зацікавлені навряд чи вдасться, але допомогти тим які хочуть розширювати свій бізнес мережа технологій має стати ключовим гравцем.

Для вирішення цих проблем в усьому світі існує велика кількість організацій-посередників на ринку інновацій, до яких належать центри комерціалізації, інноваційні центри, агентства розвитку і центри трансферу технологій. Їх основна функція полягає в забезпеченні

[1] Yevgen Novikov, Sergiy Glibko, Legal Relations between Participants in a Technology Transfer Network. Mind the Gaps Economical Aspects in the Legal Thinking. 2018. pp. 141-150.

учасників інноваційних процесів всіма необхідними послугами для реалізації їх потенціалу і розвитку інноваційних можливостей.

Як зазначає С. В. Теребова, до структури більшості зарубіжних університетів входять відділи, відповідальні за зв'язок університету і бізнесу. ТТ у деяких країнах (США, Фінляндія) зведений законом у статус третьої місії університетів (крім освітньої та науково-дослідної діяльності), невиконання якої тягне за собою покарання у вигляді позбавлення університету прав на створену ним інтелектуальну власність.

Центри трансферу технологій являють собою організації зі середньою чисельністю працівників до 100 осіб, які часто працюють за принципом самофінансування та є структурними підрозділами науково-дослідних державних установ або ж здійснюють свою діяльність на комерційних засадах, незалежно від державних програм.

На думку В. Я. Козаченка основними напрямами діяльності центрів трансферу технологій є: здійснення заходів, спрямованих на передачу інноваційних технологій зі сфери їхнього розроблення в сферу практичного застосування у межах науково-виробничої кооперації й інвестиційного співробітництва (технологічне брокерство); дослідження кон'юнктури ринку технологій; управління інтелектуальною власністю та розроблення стратегій комерціалізації технологій (ліцензування, створення компаній на основі університетських технологій, підготовка бізнес-плану інвестиційного проекту); здійснення технологічного аудиту підприємств та надання консультаційних послуг; підготовка проектів міжнародних договорів про співробітництво з питань ТТ та інноваційної діяльності; моніторинг новітніх науково-технічних досягнень у різних країнах та створення банку запитів і пропозицій вже готових інноваційних розробок; підвищення кваліфікації фахівців з інноваційної діяльності та менеджерів з ТТ; забезпечення участі вітчизняних підприємств у міжнародних виставках і ярмарках високотехнологічної продукції[1].

[1] Козаченко В. Я. Сучасний стан мереж трансферу технологій за кордоном та проблеми їх розвитку в Україні. *Вісн. Нац. ун-ту «Львівська Політехніка»*. Л. 2010. № 694. С. 162–173.

Слід зазначити, що такі центри забезпечують ТТ у широкому розумінні: від організації передачі майнових прав на результати інтелектуальної діяльності із забезпеченням вчинення відповідних правочинів до проведення маркетингових заходів, навчання та консультування.

Як зауважують В. Лисенко та С. Єгоров, деякі з таких центрів трансферу технологій об'єднуються у цілі мережі, що, своєю чергою, дає змогу забезпечити концентрацію інформаційних ресурсів та підвищити комерційну ефективність посередницької діяльності у сфері трансферу (передачі) технологій[1].

Таким чином, можна визначити центр трансферу технологій як інфраструктурну організацію, яка виступає первинною ланкою мережі, а продукцією якої є цілий комплекс послуг учасникам інноваційного процесу. Такі центри трансферу технологій на різних засадах об'єднуються в мережі, наприклад, в Європейську мережу підтримки підприємництва EEN входять більше 500 центрів з різних країн світу.

Для виявлення характерних ознак та особливостей МТТ, які виокремлюють їх серед інших інноваційних та допоміжних структур, слід більш детально розглянути принципи побудови мережі. Термін «мережа» досить поширений у науковій літературі, хоча здебільшого згадується у контексті організації комп'ютерних мереж або ж торговельних об'єднань. Так, онлайн-енциклопедія Wikipedia містить таке визначення поняття «мережа» (англ. network) – об'єднання однорідних об'єктів, яке визначає правила поведінки всередині (між її членами) і ззовні мережі (до одиниці мережі або до сукупності), вимагає правил використання одиниць мережі та всієї мережі; однорідність членів мережі дає можливість оперувати кожним з них одноково; об'єднання – дає можливість оперувати мережею як одним цільним об'єктом. Мережі можуть бути членами загальнішої мережі, утворюючи таким чином ієрархію[2].

[1] Лысенко В., Егоров С. Предпосылки и методологические основы создания и развития на Украине сети трансфера технологий. *Математичні машини і системи.* №1. 2008. С. 46–51.

[2] Поняття «мережа». Вікіпедія. URL: https://uk.wikipedia.org/wiki/Мережа 3 Толковый словарь Дмитриева. URL: https://dic.academic.ru/dic.nsf/dmitriev/4845/%D1%81%D0%B5%D1%82%D1%8C.

Тлумачний словник Д. В. Дмитрієва мережею називає безліч однорідних чи взаємозалежних установ чи пристроїв[1]. Утім, значення цього терміна набагато ширше: він включає низку аспектів, насамперед пов'язаних з інноваційною діяльністю. Мережевий характер притаманний великій кількості явищ, процесів та об'єктів. Типова мережева структура є системою, взаємовідносини між структурними елементами якої знаходяться на одному рівні. Мережева структура є формою горизонтальної інтеграції. У правовому значенні це означає, що виникають правовідносини між рівними суб'єктами незалежно від їх фінансового стану та правового статусу, однак які мають спільні та/ або взаємопов'язані інтереси. Економічне значення таких об'єднань полягає в тому, що на цьому етапі вони є більш ефективними у деяких сферах економічної діяльності, а в першу чергу – в інноваційній.

Структури, що мали мережевий характер організації діяльності, виникли досить давно. Так, С. В. Теребова зазначає, що окремі риси мережевих об'єднань мали мореплавні торговельні компанії, які були засновані на принципах акціонерного капіталу і виконували функції посередників між багатьма комерційними агентами одночасно у декількох країнах. Виражений мережевий характер мали галузеві об'єднання (асоціації, синдикати), що сформувалися в найбільш розвинених країнах наприкінці XIX ст. у металургії, вугледобуванні, пізніше – у нафтодобуванні, суднобудуванні, паперовій та військовопромисловій індустрії. Їхньою особливістю була кооперація між багатьма партнерами, які формально залишалися незалежними учасниками ринку. Тобто саме торговельні об'єднання стали першими суб'єктами економічної діяльності, що спиралися на мережеві принципи організації. Пізніше такого характеру набули акціонерні промислові об'єднання і фінансові установи.

Для визначення правової природи таких мережевих організацій розглянемо існуючи мережі та їх визначення на нормативному рівні. Так, Наказ Держкомстату України «Про затвердження Інструкції щодо

[1] Січкаренко К. О. Мережева організація інноваційної діяльності : наукова доповідь. К. 2015. 48 с.

заповнення форм державних статистичних спостережень стосовно торгової мережі та мережі ресторанного господарства»[1] № 327 від 24.10.2005 р. містить визначення таких термінів:

Торгова мережа – сукупність об'єктів (закладів) роздрібної торгівлі, розміщених на визначеній території (місто, селище тощо). Мережа роздрібної торгівлі поділяється на стаціонарну, напівстаціонарну, торгівлю поза магазинами (включаючи пересувну).

Мережа роздрібної торгівлі стаціонарна – це сукупність об'єктів роздрібної торгівлі, що розміщені в капітальних будівлях, мають систему спеціальних приміщень, оснащених торгово-технологічним устатковуванням. Стаціонарна мережа функціонує у вигляді об'єктів роздрібної торгівлі –магазинів.

Мережа роздрібної торгівлі напівстаціонарна – сукупність об'єктів роздрібної торгівлі, які займають відокремлене приміщення, як правило, легкої конструкції без великих капітальних витрат і, як правило, не мають торгового залу для здійснення торгово-технологічних операцій з покупцями.

Наказ Державної комісії з цінних паперів та фондового ринку «Про затвердження Тимчасового положення про депозитарії та депозитарну діяльність»[2] від 21.05.1996 р. № 117 (втратив чинність) надавав визначення електронної торговельної та/або інформаційної мережа (ЕТІМ) як юридичної особи будь-якої організаційно-правової форми, створеної згідно із Законом України «Про господарські товариства» торговцями цінними паперами з метою укладення угод з цінними паперами, які існують у вигляді записів на рахунках ДЕПО на електронних носіях (технічному продукті, що застосовується для накопичення, обробки та видачі інформації) в облікових реєстрах локального депозитарію, який її обслуговує.

[1] Про затвердження Інструкції щодо заповнення форм державних статистичних спостережень стосовно торгової мережі та мережі ресторанного господарства : Наказ Державного комітету статистики України від 24.10.2005 № 327. URL: http://zakon2.rada.gov.ua/laws/show/z1350-05.

[2] Про затвердження Тимчасового положення про депозитарії та депозитарну діяльність : Наказ Державної комісії з цінних паперів та фондового ринку від 21.05.1996. № 117. URL: http://zakon.rada.gov.ua/laws/show/z0318-96.

Таким чином, поняття «мережа» належить до родових категорій економічного походження. Мережі складаються як системи, сформовані за певною ознакою, учасниками яких є рівноправні суб'єкти. Їх види та особливості залежать від галузей господарства та сегментів економіки, в яких вони утворюються.

За структурою та функціями виокремлюють декілька типів мережевих об'єднань. Так, К. О. Січкаренко виділяє суто комерційні мережі: їхніми компонентами виступають власне учасники мережі, до яких відносять підприємства та їх структурні підрозділи, що забезпечують функціонування самої мережі, а також зв'язки і відносини.

Відповідно до такого підходу мережевою організацією є структура, в яку входять підрозділи, що взаємодіють між собою у межах узгоджених стандартів діяльності з метою підвищення конкурентоспроможності один одного. «Відносинами» він вважає економічні функції на кшталт інформаційного обміну, укладання угод та трастові взаємовідносини, включення певних фірм у замкнений ланцюг транзакцій.

Самі ж зв'язки у мережі він розділяє на більш інтенсивні (сильні, тісні) та епізодичні (слабкі, м'які). До перших відносять участь у статутному капіталі один одного, інших варіантах договірних відносин, передачу ліцензій, підряд на виконання робіт, спільне виробництво, спільне підприємство, компенсаційні угоди і домовленості. Вважається, що інтенсивні зв'язки властиві організаційним ядрам мережевого утворення, тоді як епізодичні – його периферії. Особливе місце в рамках мережі посідає науково-технічна співпраця між її учасниками (обмін технічною інформацією і документацією, спільні науково-дослідні роботи, маркетингові дослідження). Як додаткову форму К. О. Січкаренко виділяє передачу виробничого досвіду, знань на рівні контактів співробітників[1].

Для інноваційних та науково-інноваційних мереж характерна скоординована діяльність її учасників щодо вибору напрямів до-

[1] Січкаренко К. О. Мережева організація інноваційної діяльності : наукова доповідь. Київ, 2015. 48 с.

сліджень, що забезпечує економію часу, а отже, конкурентну перевагу. До того ж організація науково-дослідні роботи на основі мережевого принципу зумовлює високий ступінь інтеграції інформаційних ресурсів, лабораторної бази та нову якість інформаційних потоків. Останнє є принциповим моментом, оскільки саме якісний стрибок у характеристиці інформаційних потоків, перетворення інформації на публічний ресурс зумовлює виникнення умов для генерації саме нового знання (як технічного, так і гуманітарного). Організація науково-технічної та інноваційної сфери на мережевій основі спричиняє принципові зміни в самому механізмі інноваційної діяльності, дозволяє учасникам (як національним і локальним, так і глобальним) провести якісні зміни у моделі інноваційної діяльності на своїх виробничих потужностях: повноцінно комерціалізувати свої розробки, сформувати довкола себе потужне експертне середовище.

Конкретні завдання та функції МТТ кожна з них визначає самостійно, закріплюючи їх у своїх внутрішніх документах, зокрема, у регламенті. «Зразковими» для усіх МТТ цілями можна вважати завдання EEN, що належить до найвідоміших з нині існуючих мереж.

В. Я. Козаченко як головні цілі EEN виокремлює такі: а) створити інтегровану мережу послуг підтримки бізнесу, засновану на досвіді двох мереж з 270 Euro Info Centres (далі – EIC) і 250 Innovation Relay Centres (далі – IRC); б) збільшити синергію між усіма партнерами мережі з метою забезпечення інтегрованих послуг; в) покращити доступ малого та середнього бізнесу до послуг мережі за концепцією «No wrong door»; г) полегшити адміністративні процедури для учасників мережі; ґ) забезпечити професіоналізм та якість послуг[1].

Відповідно до Концепції Національної мережі трансферу технологій України (далі – NTTN) метою створення NTTN є сприяння розвитку інноваційного бізнесу і комерціалізації наукоємних тех-

[1] Козаченко В. Я. Сучасний стан мереж трансферу технологій за кордоном та проблеми їх розвитку в Україні. *Вісн. Нац. ун-ту «Львівська Політехніка»*. Львів. 2010. № 694. С. 162–173.

нологій, залучення наукового потенціалу України до обігу на світовому ринку технологій, консолідація інформаційних ресурсів державних, громадських, приватних інноваційних структур України, підприємств, установ та організацій в єдину МТТ та подальша інтеграція NTTN до європейської мережі EEN. Функціями NTTN є: трансфер технологій, ноу-хау між науковими секторами та промисловістю; пошук партнерів та інвесторів для кооперації при розробці і впровадженні високотехнологічного наукового продукту як в Україні, так і за кордоном; організація взаємодії NTTN з міжнародними МТТ.

Таким чином, основною функцією МТТ є просування послуг щодо забезпечення ефективного доступу до технологічної інформації та її розповсюдження, а також передача прав інтелектуальної власності розробників суб'єктами інноваційної діяльності, на що спрямована діяльність всіх суб'єктів такої мережевої організації.

Функції та задачі МТТ здійснюються через діяльність її учасників, які надають широкий перелік послуг як щодо забезпечення ТТ у широкому розумінні, так й інші допоміжні (які іноді йменують інфраструктурними) розробникам та користувачам результатів науково-технічної діяльності, об'єктам інтелектуальної власності на підставі відповідних договорів про надання послуг, виконання робіт або змішаних договорів. Відносини, які виникають між ними, пов'язані із здійсненням господарської діяльності кожною із сторін та ґрунтуються на засадах рівності та свободи договору. Відповідно відносини, які виникають між учасниками та розробниками («продавцями») або користувачами технологій («покупцями»), належать до господарсько-виробничих відносин відповідно до ст. 3 ГК України та по суті становлять зміст діяльності МТТ[1].

Адміністратор визначає засади діяльності МТТ та скеровує її відповідно до поставлених цілей. Ним формуються необхідні внутрішньоструктурні підрозділи (органи) для здійснення загальної політи-

[1] Господарський кодекс України Закон України від 16.01.2003 № 436-IV. *Відомості Верховної Ради України.* 2003, № 18, № 19-20, № 21-22, ст. 144.

ки у мережі, для прийняття рішень з поточної діяльності та моніторингу результатів діяльності. Адміністратор також забезпечує формування матеріально-технічної, програмної та фінансової основи МТТ, підтримує та просуває сайт, здійснює пошук та розподіл фінансів та відповідає за їх використання. Він приймає рішення про приєднання до мережі інших учасників та укладає договори з учасниками про вступ (приєднання) або про членство із забезпеченням (якщо це передбачено внутрішніми документами) проходження навчання та сертифікації.

Отже, між учасниками та адміністратором, залежно від організаційно-правової форми діяльності, виникають господарські відносини, що складаються стосовно формування бази даних щодо технологічних, інвестиційних та дослідницьких запитів та пропозицій та їх перевірки, – з одного боку, та надання матеріально-технічного, програмного та фінансового забезпечення поширення таких даних серед широкого кола кінцевих суб'єктів ТТ (клієнтів) – з другого. Такі відносини спрямовані на управляння мережею як організацією, в якій саме учасники надають послуги клієнтам, виконуючи при цьому завдання самої мережі. У них саме адміністратор встановлює правила приєднання учасників, вимоги до їх кваліфікації та надання ними послуг. Адміністратор, керуючи діяльністю мережі, здійснює моніторинг та забезпечує обробку звітності діяльності всіх її учасників. Отже, адміністратор наділений певним колом організаційно-господарських повноважень щодо учасників, які ґрунтуються на підставі укладених між ними договорів про приєднання до мережі (або договорів участі).

Адміністратор МТТ вступає у договірні відносини також з партнерами, разом з якими здійснюються спільні дії щодо розвитку мережі та її взаємодії з іншими суб'єктами права (приватними та публічними, національними та міжнародними). Такі правовідносини, на наш погляд, належать до горизонтальних господарських відносин навіть у тих випадках, коли однією із сторін (партнером) виступає орган державної влади або місцевого самоврядування. У них останні, як правило, не виконують державні владні повноваження, а виступа-

ють рівним партнером адміністратора, який має з ним спільний інтерес щодо забезпечення активної діяльності у мережі.

Таким чином, на наш погляд, відносини, які виникають у зв'язку із функціонуванням мереж трансферу технологій, слід класифікувати на три кола: 1) між адміністратором та учасниками: технологічних посередників та сервісних організацій; 2) між адміністратором та партнерами; 3) між учасниками та клієнтами (розробниками та користувачами технологій). Їх особливістю слід визнати те, що частина з них належить до горизонтальних господарських (майново-господарських) відносин, в яких відбувається реалізація предмета діяльності мережі щодо надання відповідних послуг клієнтам, пов'язаних із трансфером технологій, а інші – організаційні господарські відносини, пов'язані із забезпеченням її функціонування. При цьому незалежно від виду зобов'язальних відносин у мережі всі вони мають своєю підставою договір. Наслідком такого характеру відносин між учасниками мережі трансферу технологій стає мобільність та гнучкість цієї організації, яка легко пристосовується до запитів та потреб національного та міжнародного ринків.

Від зазначених внутрішніх відносин усередині мережі між її учасниками слід відрізняти зовнішні відносини щодо мережевої організації, до яких належать, на наш погляд, зобов'язальні відносини між самими клієнтами щодо трансферу технологій у широкому значенні та між адміністратором, який діє в інтересах розвитку мережі, з іншими регіональними та міжнародними мережами трансферу технологій. Відносини між клієнтами мережі щодо трансферу технологій виникають на підставі відповідного договору, який може стосуватися надання/передання майнових прав інтелектуальної власності, виконання науково-дослідних, дослідно-конструкторських, технічних робіт, виконання послуг (сертифікаційних, інжинірингових, з авторського нагляду та ін.), договорів про спільну діяльність у реалізації проекту. Перелік таких договорів не є прямо встановленим або вичерпним. Зобов'язання, що виникають на їх підставі, стосуються прав та обов'язків розробників та користувачів технологій (клієнтів) і не пов'язані із виконанням будь-яких зобов'язань з боку мережевої

організації. Учасники мереж трансферу техногій, які сприяли трансферу технологій, вступають у відносини з кожним клієнтом. Отже, зобов'язальні відносини між самими клієнтами щодо трансферу технологій у широкому значенні, вважаємо, належать до зовнішніх відносин, які виникають у зв'язку із функціонуванням мереж трансферу технологій.

# 7. РЕАЛІЗАЦІЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ ТА ПРАВООХОРОННОЇ ФУНКЦІЙ ПУБЛІЧНИХ ЕЛЕКТРОННИХ РЕЄСТРІВ

## 7.1. Узагальнення результатів фундаментального дослідження проблем функціонування публічних електронних реєстрів

Держава Україна взяла на себе роль основного популяризатора цифрових перетворень. Вона запропонувала суспільству цифрові інноваційні послуги та стала дійсним лідером цифрових трансформацій в умовах, коли у значному колі суб'єктів господарювання панувала засторога перед можливими ризиками цифрової трансформації. У колі дослідників цієї проблеми росхожим став наголос щодо завдань нашої держави – стати замовником і першим покупцем інновацій та цифрових сервісів, що спонукало б до поштову щодо утворення нових ринків цифрових (як держаних так і недержавних) послуг.

Рівень усвідомленості сучасних фахівців галузі права дозволяє сприймати нові цифрові технології інтелектуальною базою для створення оновлених за суттю послуг, нетипових цінностей, властивостей, іншої продукції як матріального характеру так й з іншими якісними характристиками. Визнання цього факту державою і суспільством потребує збалансованості обсягу потенціалу цифрової зрілості, який

вже містить наша держава, із тим, якого досягло суспільство. Відсутність балансу (у тому числі з причини низького рівня цифрової грамотності суспільства) зашкоджає реалізації потенціалу держави.

В Україні практична вагомість Національного проекту цифрової держави булп підтверджена брендом «Дія». Цей інноваційний продукт створювався за кошти швейцарсько-української програми EGAP, проекту USAID, проекту EGOV4UKRAINE, що фінансується ЄС та його країнами-членами: Данією, Естонією, Німеччиною, Польщею і Швецією. За концепцією цифрової держави Україна були передбачені численні реальні зміни щодо стовідсоткової доступності онлайн всіх державних послуг Також для суспільства комфортно, коли 20% послуг надаються автоматизовано, без втручання посадової особи. Очікуваними є: єдина база ДНК українців, одна онлайн-форма для заповнення з метою отримання пакету послуг у будь-якій життєвій ситуації та інше. Відповідні завдання були поставлені державою перед Міністерством цифровий трансформації України.

У 2022 році відбулася низка позитивних подій щодо цифрової трансформації України. Внаслідок імплементації європейської політики впровадження цифрових технологій відбулося отримання нашою країною статусу учасниці програми Європейського Союзу «Цифрова Європа». Разом із ним з'явилися відовідні міжнародні зобов'язання України щодо наближення її сучасного праворозуміння шляхів імплементації до правового простору ЄС. Наближення до правового простору ЄС породжує нові актуальні завдання для втілення у цифровому просторі України. В цілому нашою державою створюються результативні передумови розвитку інформаційного суспільства та впровадження інформаційно-комунікаційних і цифрових технологій.

Стає зрозумілим, що досягнення цілі збалансування цифрової самодостатності держави та цифрової зрілості суспільства потребує відповідного теоретичного підґрунтя. Теоретичні засади опосередкованого правового впливу на досягнення балансу грунтуються на вже наявному досвіді та завданнях на поточний період. З огляду на доцільність прискорення даного процесу в умовах військового стану,

проблему досягнення балансу цифрової зрілості держави та цифрової зрілості суспільства слід актуалізувати у дослідженнях, спираючись на те, що Україна як цифрова держава мала значний прорив у довоєнний період[1].

Внаслідок того, що у зазначений період було розпочато активне формування та значне забезпечення реалізації державної політики у сферах цифровізації економіки, цифрового розвитку освіти, цифрових інновацій та технологій у бізнесі, електронного урядування та електронної демократії, інформатизації суспільства. На минулих досягненнях вдалося суттєво оновити законодавчу базу вже у період військової агресії Росії проти України. Йдеться про Закон України «Про Національну програму інформатизації» від 01.12.2022 за № 2807-IX, який набирає чинності з 01.12.2023 року. За Концепцією Національної програми інформатизації зазначена програма формується та виконується (поруч із іншими завданнями) для досягнення електронної демократії.

На законодавчому рівні електронною демократією визнається така форма суспільних відносин, за якої громадяни та організації залучаються до державотворення та державного управління, а також до місцевого самоврядування шляхом широкого застосування інформаційно-комунікаційних технологій у демократичних процесах. Це надає можливість посилити участь, ініціативність та залучення громадян до публічного життя на загальнодержавному, регіональному

[1] Див.: Про публічні електронні реєстри: Закон України від 18.11.2021 р. № 1907-IX. URL: https://zakon.rada.gov.ua/laws/show/1907-20#Text; Про віртуальні активи: Закон України від 17.02.2022 р. № 2074-IX. URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text; Про електронні комунікації: Закон України від 16.12.2020 р. № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text; Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text; Про стимулювання розвитку цифрової економіки в Україні: Закон України від 15.07.2021 р. № 1667-IX. URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text; Про Національну комісію, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку: Закон України від 16.12.2021 р. № 1971-IX. URL: https://zakon.rada.gov.ua/laws/show/1971-20#Text; Цифрова адженда України – 2020 (проект). URL: https://ucci.org.ua/uploads/files/58e78ee3c3922.pdf.

та місцевому рівнях. Також – підвищити прозорість процесу прийняття рішень та підзвітність демократичних інститутів. Значно поліпшується зворотний зв'язок суб'єктів владних повноважень на звернення громадян[1]. Електронна демократія зазвичай активізує публічні дискусії, привертає увагу громадян до процесу прийняття рішень, сприяє пожвавленню процесів саморозвитку громадян, в тому числі, - їх тяжіння до самосвіти та освіти.

Визначення поняття цифрової держави як певної сукупності реєстрів, баз даних, які між собою взаємодіють має суто практичне забарвлення. Воно широко розповсюджено у публіцистичних та інших ненаукових джерелах. Саме у такому значенні сприймали загрози її існуванню у перші дні російсько-української війни. Але «цифрова держава не похитнулась і продовжила розвиватись і працювати» довів М. Федоров, надаючи (як Віцепрем'єр-міністр, міністр цифрової трансформації України) звіт про технологічні досягнення України у 2022 році.

Попри повномасштабну війну Україна змогла не тільки захистити персональні дані своїх громадян та державні реєстри, але й продовжити свій рух до цифрового майбутнього. За 2022 рік в застосунку Дія з'явились нові цифрові документи та 16 послуг. Ще 25 – на порталі Дія. Усі вони полегшують життя українцям, економлять бюджетні кошти та допомагають протистояти російським окупантам. Також відбувається експорт технологій за кордон та популяризація їх внаслідок визнання Дії в інших країнах[2].

Чимало фахівців вважають, що Закон України "Про цифровий контент та цифрові послуги" значно сприятиме зміцненню цифрового бренду України за кордоном та демонструватиме наші цінності правового забезпечення розвитку технологій цифрової економіки та суспільства.

---

[1] Про Національну програму інформатизації: Закон України від 01.12.2022 р. № 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20?find=1&text=%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0.

[2] Яковлева О. Цифрова держава не похитнулась і продовжила розвиватись і працювати – Інтерв'ю з Михайлом Федоровим. Матеріали ЗМІ від 11 січня 2023 р.

Прийняття цього Закону було обумовлено необхідністю імплементації у національне законодавство України Директиви 2019/770 Європейського Парламенту і Ради Європи щодо деяких аспектів, що стосуються контрактів на постачання цифрового контенту та цифрових послуг як сучасного нетипового блага.

Дійсно, слід визнати цінність його потенціалу у внесенні важливих змін до Цивільного кодексу України. Йдеться про доповнення переліку об'єктів цивільних прав оновленим різновидом, а саме - цифровими речами. Так важливим законоположенням закріплюється визнання факту існування об'єктів цивільних прав у матеріальному світі та/або цифровому середовищі. Знаковим нюансом нововведення стає обумовлення самої сутності та форми цифрових речей як об'єктів цивільних прав. Також у законодавчому порядку регламентуються особливості набуття цивільних прав і обов'язків щодо них, нюанси їх здійснення та припинення.

Зокрема, текст змісту ЦК України доповнився новою статтею 179-1, норма якої надає визначення цифрової речі як блага, яке створюється та існує виключно у цифровому середовищі та має майнову цінність[1]. Із визначенням цифрової речі, яке співвідноситься, але не співпадає, з визначенням цифрового контенту, передбачаються далекоглядні наслідки. Коли законодавець подає цифровий контент наступним чином – «це дані, які створюються і надаються в цифровій формі», то така подача передбачає розрізнення понять «цифрового контенту» та «цифрових послуг». А відтак – «розведення» цих понять не лише в теорії, але й на практиці при введенні їх в обіг означає необхідність виокремлення правових наслідків обігу.

Але тут постає птання щодо необхідності прояснення низки певних продуктів та послуг, на які не поширюється дія Закону про цифровий контент. Згідно нього цифровою визнається така послуга, що надає можливість споживачу створювати, обробляти, зберігати та поширювати дані у цифровій формі або отримувати доступ до таких

[1] Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 р. № 3321-IX. URL: https://ips.ligazakon.net/document/T233321?utm_source=biz.ligazakon.net&utm_medium=news&utm_content=bizpress01.

даних, а також здійснювати будь-які інші дії з даними у цифровій формі, що були створені чи завантажені споживачем або іншими користувачами такої послуги. До цифрових послуг належать, зокрема такі, що дають змогу створювати, обробляти, отримувати доступ або зберігати дані в цифровій формі, включаючи хостинг файлів, обробку текстів або гри, які пропонуються в середовищі хмарних обчислень і соціальних мережах[1].

Практикуючи фахівці юридичної фірми Sayenko Kharenko (О. Климчук, А. Фінько та ін.) зробили огляд, у якому, спираючись на пункт 27 Преамбули Директиви 2019/770, коментують коло базових обмежень. Зокрема, Закон про цифровий контент та цифрові послуги, серед інших обмежень, не буде застосовуватися до: надання державних послуг, послуг державних реєстрів[2].

При цьому їх аргуметація – це посилання на пункт 27 Преамбули Директиви 2019/770. Втім, Директива лише вимагає уточнення окремих положень законодавства України українським законотворцем. Він (законодачий орган) відповідного чи тотожнього положення щодо публічних електронних реєстрів у ст.1 не закріплював. І хоча огляд вищезазначених фахівців призначенй виключно для загального інформаційного ознайомлення і не є юридичною чи іншою професійною консультацією, все ж спонукає до прояснення та уточнення, як мінімум, двох питань.

По-перше, чи слід посилатися на пункт 27 Преамбули Директиви 2019/770 за відсутності норми прямої дії у ч.4 ст.1 Закону України «Про цифровий контент та цифрові послуги», яка пойменована приписом: «Дія цього Закону не поширюється на регулювання відносин щодо: …»?

---

[1] Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 р. № 3321-IX. URL: https://ips.ligazakon.net/document/T233321?utm_source=biz.ligazakon.net&utm_medium=news&utm_content=bizpress01.

[2] Закон України «Про цифровий контент та цифрові послуги»: деталь регуляторного пазлу, якої бракувало? Огляд фахівців юридичної фірми Sayenko Kharenko. О. Климчук, А. Фінько та ін. 23 жовтня 2023. https://sk.ua/uk/zakon-ukraini-pro-cifrovij-kontent-i-cifrovi-poslugi-detal-u-reguljatornij-golovolomci-cifrovogo-sektoru-jakoi-brakuvalo/.

Закон спирається на Директиву (ЄС) 2019/770 в унормуванні деяких відносин та встановленні вимог й умов, але далеко не всіх, які того потребують. Зокрема, в аспекті виявлення спорідненої правової природи цифрових послуг із суттевими ознаками послуг, які надає публічний електронний реєстр як юридична особа. Тому рефлексія практичного характеру, (як підхід щодо відповіді на це запитання) – погодження з позицією Міністерства юстиції України стосовно «імплементації відповідних положень Директиви у національне законодавство, яку юридично коректніше проводити шляхом внесення необхідних для цього змін до законів……., що має, зокрема, дозволити чіткіше імплементувати відповідні положення Директиви у законодавство України та забезпечити системне регулювання відповідних суспільних відносин»[1].

З такої позиції маємо продовжити дослідження проблем функціонування публічних електронних реєстрів в умовах реалізації нового Закону. Отже потребує детального дослідження вплив ухваленого Закону «Про цифровий контент та цифрові послуги» на такий важливий закон як Закон України «Про публічні електронні реєстри».

По-друге, навність подвійного правового статусу низки публічних електронних реєстрів не враховано ані у новому Зконі ані у наданому огляді фахівців, ані в міжнародних документах. Проблемні аспекти розуміння правової природи публічних електронних реєстрів ще не стали популярними для науковців. У правовій науці відсутні відповідні комплесні фундаментальні дослідження. Натомість системне тлумачення співвідношення вищезгаданих двох законів не може здійснюватися у межах сприйняття публічних електронних реєстрів виключно інформаційно-комунікаційним ресурсом.

Рефлексія загально-аналітичного теоретичного характеру на це запитання є потребою сучасної правової науки. Аргументовані

[1] Верховна Рада готується ухвалити закон про цифровий контент та цифрові послуги, незважаючи на критику Мін'юсту. *Судово-юридична газета*. 7 Грудня, 2022. https://finap.com.ua/verhovna-rada-gotuyetsya-uhvalyty-zakon-pro-tsyfrovyj-kontent-ta-tsyfrovi-poslugy-nezvazhayuchy-na-krytyku-min-yustu/.

роз'яснення та аналітика щодо нового законодавчого акта «Про цифровий контент та цифрові послуги» були здійснені О. Загнітком.

Серед його оцінок та прогнозів слід звернути увагу на наступні безумовно негативні наслідки: «…висока імовірність, що положення нового Закону конкуруватимуть з нормами раніше ухвалених законодавчих актів, як-от, щодо «суб'єктивності» чи «цифрової речі»[1].

У вітчизняному правовому полі не виокремлюються різновиди цифрових послуг в інноваційній сфері. Виявлення їх за критерієм суб'єктивності залежно від правового статусу публічного реєстру, який їх формує на запит замовника та надає на договірних засадах, дозволить повно та об'єктивно оцінити їх правову природу, комплексно дослідити, а також виділити неоднорідність з метою належного договірного та законодавчого забезпечення.

Якщо гіпотетично сприймати особливі цифрові послуги різновидом послуг інноваційних, то слід звернутися до напрацювань А.Шапошник, яка обгрунтовує необхідність встановлення особливих умови їх надання, виокремлює низку критеріїв відповідності та пропонує пордок притягнення до відповідальності за порушення договірних зобов язань[2].

Вперше у законодавстві України термін «електронна послуга» визначено в Стратегії розвитку інформаційного суспільства в Україні у значенні «послуга, надана громадянам та організаціям в електронному вигляді за допомогою інформаційно-комунікаційних технологій»[3]. А вже менше ніж за десять років важливою новацією (згідно нового Закону) вважається запровадження суб'єктивних та

[1] Загнітко О. Огляд Закону України «Про цифровий контент та цифрові послуги». https://jurliga.ligazakon.net/analitycs/223718_oglyad-zakonu-ukrani-pro-tsifroviy-kontent-ta-tsifrov-poslugi.

[2] Шапошник А.О. Послуги в інноваційній сфері та їх договірно-правове забезпечення. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 «Право». – Національний юридичний університет імені Ярослава Мудрого, Міністерство освіти і науки України, Харків, 2021. 231 с.

[3] Про схвалення Стратегії розвитку інформаційного суспільства в Україні : Розпорядження, Стратегія України від 15.05.2013 р. No 386-р. URL: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text.

об'єктивних критеріїв, яким мають відповідати цифрова послуга. За умови недотримання яких договір не можна вважати укладеним.

Таким чином навіть в умовах воєнного стану нашої державою та науковцями забезпечується належне спрямування цифрової трансформації України до цивілізаційного простору. Це є, в нашій країні та за її межами, потужним поштовхом до розвитку обігу відповідної (безпосередньої та/або опосередкованої) інформації в умовах впровадження цифровізації діянь у сферу ідентифікації та контролю.

Отже результати наукових досліджень щодо правового забезпечення розвитку технологій цифрової економіки та суспільства, проведених НДІ ПЗІР НАПрН України, є вкрай затребуваними для актуалізації самого процесу економіко-правового запровадження новацій цифрового механізму державного контролю у сфері господарювання.

Даний підрозділ об'єднує положення авторських досліджень, підготовлених протягом 2021, 2022 та 2023 років за темою «Правове забезпечення розвитку технологій цифрової економіки та суспільства», результати яких доводять, що у ході дослідження даної проблематики було виправданим звернення уваги на сферу публічних електронних реєстрів (далі – ПЕР).

Узагальнення результатів фундаментального дослідження проблем функціонування електронних публічних реєстрів щодо авторського ставлення до зазначеного питання обумовлене потребою досягнення результативності контролю у сфері господарювання, який здійснюється з використанням ПЕР.

Нові знання про досягнення зазначеного завдання, а саме – утворення правового механізму забезпечення результативності контролю у зазначеній сфері з використанням ресурсів ПЕР, потребують обґрунтування методологічного забезпечения високого рівня. Йдеться про ситемний аналіз повних і достовірних знань про практичну результативність нині діючих правових приписів щодо ПЄР. Виявлення ступеню їх економіко-правової ефективності, а також наявних причин неефективності (рівно як й недостатньої ефективності) має перспективу все більшої актуалізції багатьох аспектів функціонуван-

ня Глобальних публічних реєстрів, Міждержавних публічних реєстрів та їх модифікацій.

На першому році дослідження в НДІ ПЗІР НАПрН України теми «Правове забезпечення розвитку технологій цифрової економіки та суспільства» було використано підхід обгрунтування закономірностей зміни напрямів економічної політики під впливом активізації процесів цифровізації у всіх галузях суспільного життя.

Методологічною основою дослідження було обрано за основний діалектичний метод пізнання. На початковому етапі вивчення стану розв'язання проблем зміни напрямів економічної політики під впливом інформаційно-комунікаційних технологій було обрано дослідницький підхід систематизації за часовим фактором. Він залишився актуальним, але відбулася вимушена пріорітезація змін, спричинених військовою агресією Росії проти України.

Також на початковому етапі було впорядковано дослідницький підхід щодо систематизації зміни напрямів економічної політики під впливом інформаційно-комунікаційних технологій за часовим фактором. Актуальність зазначеного підходу обумовлена тим, що за критерієм часового фактору зміни напрямів економічної політики, виокремлюють два основних різновиди змін (1) стратегічної та (2) ситуативної природи. Перший – зміни стратегічного характеру, які відбуваються (мають відбуватися) згідно із концепцією цифровізації економіки (у тому числі її правової інфраструктури). Другий – ситуативні зміни державної політики, спричинені діями (подіями), внаслідок яких вносяться суттеві корективи у стратегію та тактику державної політики в цілому.

До 24 лютого 2022 року в Україні вектором нової економічної політики були зміни стратегічного характеру, а не ситуативного. Після названої дати вібулися важливі зміни економічної політики ситуативного характеру.

За фактором змістовного наповнення змін ситуативного характеру стали затребуваними дослідження передусім наступних правових проблем: а) вдосконалення цифрового контролю та самоконтролю у сфері господарювання в умовах воєнного стану та післявоєнно-

го відновлення економіки; б) розширення функціоналу електронних публічних реєстрів як юридичної гарантії реалізації цифрових прав; в) збалансування обсягу цифрової грамотності сусільства з рівнем цифровізації державних інституцій, внаслідок запровадження дієвих механізмів популяризації сучасних онлайн-процесів та інше.

Перша із зазначених правових проблем у такому контексті, як вона сформульована вище, не висвітлювалася науковцями. Хоча більш широкий підхід до проблемних питань кількості та повноважень контролюючих органів, але з прєкцією на воєннийо стан, не був обділений увагою[1]. Натомість подія щодо прийняття Верховною Радою України за основу Проєкту Закону за № 10016-д від 16.10.2023 р. «Про внесення змін до Податкового кодексу України та інших законів України щодо скасування мораторію на проведення податкових перевірок»[2] зачно актуалізувала обговорення проблем адміністрвання податків.

Отже, оцінка стану дослідження наявних правових проблем за першим із зазначених напрямів буде продуктивною, якщо проаналізувати не лише природу саме цифрового контролю та самоконтролю у сфері господарювання, але й спрогнозувати особливості її прояву в умовах воєнного стану та післявоєнного відновлення економіки.

Наприклад, всупереч умов воєнного стану було отримано результативні судові рішення стовоно усунення практики блокування податковими органами податкових накладних без деталізації причин, критеріїв ризиковості та надання переліку документів, які необхідно подати платнику податків.

Це відбувлося всупереч того, що часто змінюється законодавче регулювання цього питання. Так, лише у 2023 році двічі (влітку та

[1] Див.: Козій Т. В., Почтарьов С. О. Діяльність органів контролю за якістю продукції в умовах надзвичайного стану. *Економічний вісник університету.* 2023. № 56. С. 15–19; Поліщук І. В. Особливості правового регулювання державного нагляду(контролю) за здійснення господарської діяльності в умовах воєнного стану / / *Юридичний вісник.* 2022. №2 (63). С. 175–182 та ін.

[2] Проєкт Закону про внесення змін до Податкового кодексу України та інших законів України щодо скасування мораторію на проведення податкових перевірок від 09.11.2023 р. № 3453-IX. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/42994.

в грудні) набували чинності зміни до відповідного законодавства. Зокрема, 9 грудня 2023 року вступили в силу суттеви зміни до Порядку зупинення реєстрації податкової накладної/розрахунку коригування в Єдиному реєстрі податкових накладних. Як наслідок змін, фахівці стверджують про існування сформованої сталої судової практики, щодо наступних основних положень:

- подання податковому органу договорів та інших документів, що підтверджують вчинення інших операцій, аніж зазначених в податковій накладній є підставою для відмови в реєстрації такої накладної;
- рішення про відмову в реєстрації податкових накладних повинне містити чіткі підстави для такої відмови;
- можливість надання платником податків вичерпного переліку документів на підтвердження правомірності формування та подання податкової накладної прямо залежить від зазначення у квитанції про зупинення реєстрації податкової накладної чіткого переліку документів;
- контролюючий орган в квитанції про зупинення реєстрації податкової накладної/розрахунку коригування повинен здійснювати не лише загальне посилання на пункт Критеріїв оцінки, а конкретно зазначати відповідний підпункт, в межах якого й закріплений конкретний критерій, на основі якого було зупинено реєстрацію податкової накладної[1].

Відомо, що вцілому контроль у сфері господарювання в умовах воєнного стану зазнає змін щодо його лібералізації. Водночас обсяги тіньової економіки під час лібералізації та відсутності економічної стабільності суттево зростають. І тоді спотворюється призначення господарської діяльності – бути джерелом досягнення економічних та соціальних результатів. Коли йдеться про такий комерційний різновид господарської діяльності як підприємництво, то контролюючим органам доводиться стикаться з проблемою фіктивного підприємництва.

[1] Беляєв С. Блокування податкових накладних: аналіз судової практики 2023 року. URL: https://zedsoft.com.ua/blog/index.php?blokuvannia-podatkovykh-nakladnykh-analiz-sudovoi-praktyky-2023-roku.

Попередження фіктивного підприємництва має досить важливе значення в умовах воєнного стану та післявоєнного відновлення економіки. Фіктивна господарська діяльність наносить значну шкоду економіці країни. Виходячи з того, що фіктивні діяння нерідко мають інтелектуальний характер, її попередження по'язують із запровдженням ресурсів цифрового контролю та самоконтролю.

Така вимушена обставина як припинення повноцінного функціонування (на протязі більше як двох місяців) двох основних державних реєстрів України знизила інформаційно-комунікативну значимість публічних реєстрів. Йдеться про Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань і про Державний реєстр речових прав на нерухоме майно.

Коли для реалізації функціоналу контролю залишилися можливими лише такі реєстраційні дії, як створення благодійних організацій та внесення змін до відомостей про них, зміна керівника юридичної особи, зміна місцезнаходження юридичної особи (адже відбувалася релокація бізнесу), створення нової юридичної особи, реєстрація ФОПів, то це сповільнило процес отримання результатів контролю. Цей фактор негативно вплинув на реалізацію можливостей контролю з використанням цифровх ресурсів.

Операції з нерухомістю, в тому числі тією, що входить до складу майнової основи господарюванн, були заборонені і блокувлися до прийняття постанови Кабінету Міністрів України №480 від 19 квітня 2022 р.[1] Вона має назву «Про внесення змін до деяких постанов Кабінету Міністрів України щодо діяльності нотаріусів та функціонування єдиних та державних реєстрів, держателем яких є Міністерство юстиції, в умовах воєнного стану».

Віновлення функціонування ПЕР та низка нововведень при реєстрації різних майнових прав в умовах воєнного стану слід сприйма-

[1] Про внесення змін до деяких постанов Кабінету Міністрів України щодо діяльності нотаріусів та функціонування єдиних та державних реєстрів, держателем яких є Міністерство юстиції, в умовах воєнного стану: Постанова Кабінету Міністрів України від 19.04.2022 р. № 480. URL: https://zakon.rada.gov.ua/laws/show/480-2022-%D0%BF#Text.

ти як позитивну подію, бо це надало можливість правоохоронним та контролюючим органам запроваджувати заходи протидії поширенню фіктивного підприємництва, іншим злочинам, пов'язаним з використанням можливостей фіктивних підприємств. Адже важливим елементом механізму стримування є сигнальна інформація, яка розміщується у реєстрах, використовується та за потреби адмініструється.

Довгий час досить критичною залишалася ситуація із контролем за відомостяи про бенефіціарних власників компаній, що не дозволяло протиставити механізм відповідальності маніпуляціям із приховування об'єктів власності. Дієвість такого запобіжника корупції як доступність інформації про реальних власників компаній обумовлена інформаційно-комунікаційною функцією низки цифрових ресурсів. Йдеться про локальні та глобальні Реєстри, як містить відомості про бенефіціарних власників компаній та структуру власності.

Приєднання України до ініціативи Transparency International щодо сприяння прозорості та запобігання корупції зобов'язує забезпечити доступність інформації у публічному просторі про реальних власників компаній. Глобальний реєстр бенефіціарних власників[1] об'єднує країни, що беруть на себе зобов'язання забезпечити передачу до зазначеного Реєстру відомості про бенефіціарних власників компаній, відомості про які містяться в їх державних реєстрах юридичних осіб, фізичних осіб-підприємців та тому подібні.

Утворення реєстру відбулося за результатами роботи Лондонського антикорупційного саміту (Anti-corruption Summit). Він був проведений 12 травня 2016 року у м. Лондоні та стрімко набуває популярності внаслідок того, що відомості про бенефіціарних власників компаній, розміщені у публічних реєстрах, є запорукою протистояння маніпуляціям із структурою власності та приховуванням об'єктів власності.

Отже Глобальний публічний електронний реєстр сприймається як глобальний стандарт досягнення результативності цифрової трансформації нашої країни. В Україні соціальні пастки встановлен-

[1] Who controls, influences, or benefits from a company? 2020. *Open Ownership Register*. https://register.openownership.org/.

ною глобальної стандартизації досягнення результативності усуваються разом з міжнародними партнерами. Зокрема, шляхом забезпечення відповідності даних, які містяться в українських реєстрах Стандарту даних про бенефіціарну власність (BODS). Вимоги Стандарту – відповідність ключовим критеріям якості, прозорості та здатності до машинного зчитування. Наприклад, за пілотною програмою «OpenOwnership» відбулося технічне супроводження підготовки низки концептуальних документів та розробки необхідної законодавчої бази для подальшої безпосередньої регулярної передачі якісно вивірених даних про реальних власників компаній з ЄДР до Глобального реєстру бенефіціарних власників.

Участь в Глобальному реєстрі має потенціал суттєвого поліпшення іміджу держави на міжнародній арені. Також приєднання України до ініціативи Transparency International щодо сприяння прозорості та запобігання корупції здатне сприяти підвищенню позицій нашої країни в рейтингу Світового Банку «Ведення Бізнесу» («Doing Business»).

Опікуючись забзпеченням встановлення достовірності відомостей про КБВ та структуру власності, які ними подаються, а також – ефективністю її використання нашим законодавцем внесено низку відповідних змін до важливих законів України.

Закон України «Про внесення змін до деяких законів України щодо вдосконалення регулювання кінцевої бенефіціарної власності та структури власності юридичних осіб» за № 2571-IX від 06.09.2022 набув чинності 29.12.2022.

Зокрема, Законом України «Про внесення змін до деяких законів України щодо вдосконалення регулювання кінцевої бенефіціарної власності та структури власності юридичних осіб» за № 2571-IX від 06.09.2022 (набув чинності 29.12.22) було внесено зіни до Закону України «Про державну реєстрацію юридичних осіб, фізичних осіб – підприємців та громадських формувань».

Із внесенням наступних змін розширюється коло суб'єктів впливу на функціональність ПЕР в частині їх придатності слугувати ресурсом контролю. Так, «Державний реєстратор під час проведення реєстраційних дій щодо юридичної особи (крім державної реєстрації

припинення) та у разі подання такою юридичною особою відомостей про особу, яка є кінцевим бенефіціарним власником юридичної особи, обов'язково здійснює перевірку (верифікацію) відомостей, зазначених стосовно такої особи, з використанням відомостей з Державного реєстру актів цивільного стану громадян, Єдиного державного демографічного реєстру, Державного реєстру фізичних осіб – платників податків, Єдиної інформаційної системи Міністерства внутрішніх справ України щодо розшуку осіб, зниклих безвісти, та викрадених (втрачених) документів за зверненнями громадян, крім відомостей, перевірка яких автоматично здійснюється засобами Єдиного державного вебпорталу.

У разі подання відомостей про особу, яка є кінцевим бенефіціарним власником юридичної особи, в електронній формі перевірка відомостей, зазначених стосовно такої особи, здійснюється державним реєстратором, а також автоматично засобами Єдиного державного вебпорталу електронних послуг з використанням відомостей з Державного реєстру актів цивільного стану громадян, Єдиного державного демографічного реєстру, Державного реєстру фізичних осіб – платників податків, Єдиної інформаційної системи Міністерства внутрішніх справ України щодо розшуку осіб, зниклих безвісти, та викрадених (втрачених) документів за зверненнями громадян.

Автоматична перевірка відомостей засобами Єдиного державного веб-порталу електронних послуг здійснюється з використанням відомостей з Єдиного державного демографічного реєстру, Державного реєстру фізичних осіб – платників податків у порядку, встановленому Кабінетом Міністрів України.

У разі встановлення за результатами проведеної автоматичної перевірки невідповідності відомостей про кінцевого бенефіціарного власника юридичної особи, зазначених у заяві про державну реєстрацію, відомостям, що містяться в інформаційних системах, формування заяви за допомогою програмних засобів Єдиного державного вебпорталу електронних послуг припиняється[1].

[1] Про внесення змін до деяких законів України щодо вдосконалення регулювання кінцевої бенефіціарної власності та структури власності юридичних осіб: Закон України від 06.09.2022 р. № 2571-IX. Ч. 1. Ст. 9.

У вищезазначених законоположеннях ще й було надано акцент на активізації самоконтролю суб'єктів господарювання та їх відповідальності у сфері фінансового моніторингу. Зокрема, щодо надання достовірних відомостей про КБВ та структуру власності, які ними подаються. Відповідальний самоконтроль суб'єктів господарювання опосередковується вимогою підтримувати відповідні відомості в актуальному стані та повідомляти державного реєстратора про зміни у встановлений термін із дня їх виникнення. Також суб' єкту господарювання належить подавати державному реєстратору документи, які підтверджують відповіді зміни.

Новацією є дві підставі для внесення до Єдиного державного реєстру відомостей про юридичну особу, громадське формування, що має статус юридичної особи та фізичну особу - підприємця. Зокрема, внаслідок доповнення частини першої статті 9 пунктами 4 і 5 відповідного змісту, нові підстви є наступними:

– повідомлення про виявлення розбіжностей між відомостями про кінцевих бенефіціарних власників та структуру власності клієнта, зокрема про виявлення неповноти, неточностей чи помилок в інформації про кінцевого бенефіціарного власника або структуру власності, що містяться в Єдиному державному реєстрі (п. 4);

– інформація від Національного банку України про визнання структури власності юридичної особи, державне регулювання та нагляд за діяльністю якої здійснює Національний банк України, непрозорою (прозорою)»[1].

Новим підходом слід визнати законоположення про суб'єкта відповідальності (винниу особу) у сфері внесення до установчих документів (та/або інших, які подаються для державної реєстрації), завідомо неправдивих відомостей, призначених для внесення до Єдиного державного реєстру. Також вважаються винними ті особи, які вчинили бездіяльність у вигляді неподання або несвоєчасного подання державному реєстратору передбаченої Законом інформації про кінцевого бенефіціарного власника юридичної особи або про його відсутність.

[1] Про державну реєстрацію юридичних осіб, фізичних осіб - підприємців та громадських формувань: Закон України від 15.05.2003 № 755-IV. URL: https://zakon.rada.gov.ua/laws/show/755-15#n160. П. 4, П. 5. Ст. 9.

Наразі частина четверта статті 35 Закону України «Про державну реєстрацію юридичних осіб, фізичних осіб - підприємців та громадських формувань» була викладена у редакції наступного змісту:

«4. Внесення особами, уповноваженими на вчинення дій, спрямованих на державну реєстрацію створення юридичної особи або зміну учасників юридичної особи, до документів, що подаються для такої державної реєстрації, завідомо неправдивих відомостей про кінцевого бенефіціарного власника юридичної особи або про його відсутність тягнуть за собою накладення штрафу на таку юридичну особу у розмірі від однієї тисячі до двадцяти тисяч неоподатковуваних мінімумів доходів громадян.

Неподання або несвоєчасне подання особами, уповноваженими діяти від імені юридичної особи, державному реєстратору інформації про кінцевого бенефіціарного власника юридичної особи або про його відсутність тягне за собою накладення штрафу на таку юридичну особу в розмірі від однієї тисячі до двадцяти тисяч неоподатковуваних мінімумів доходів громадян.

Ненадання юридичними особами - резидентами, які є засновниками (учасниками) юридичних осіб, та фізичними особами - резидентами, які є засновниками (учасниками) юридичних осіб та/або здійснюють вирішальний вплив на їхню діяльність, на запит юридичних осіб інформації, необхідної для подання юридичною особою для внесення або актуалізації в Єдиному державному реєстрі інформації про кінцевого бенефіціарного власника та структуру власності юридичної особи, тягнуть за собою накладення штрафу на таку юридичну або фізичну особу - резидента в розмірі від однієї тисячі до двадцяти тисяч неоподатковуваних мінімумів доходів громадян.

Притягнення осіб до відповідальності за порушення, передбачені цією частиною, здійснюється Міністерством юстиції України. Порядок притягнення юридичних осіб до відповідальності та порядок визначення розмірів штрафів за такі дії встановлюється Міністерством юстиції України»[1].

[1] Про державну реєстрацію юридичних осіб, фізичних осіб - підприємців та громадських формувань: Закон України від 15.05.2003 р. № 755-IV. URL: https://zakon.rada.gov.ua/laws/show/755-15#Text. Ч. 4. Ст. 35.

Вищезазначені новації були вкрай затребуваними як з огляду на внутршні завдання щодо викриття тіньових структур бізнесу так і на потребу правового забеспечення інвестицій під час війни та у найближчу перспективу відновлення економіки України

Реалізація зазначеної відповідальність у вигляді санкції - накладення штрафу вкрай важлива з огляду на пріоритетизацію проєктів піснявоєнної відбудови економіки нашої країни, пов'язанних із залученням інвесторів та інших міжнародних партнерів.

Розробка економіко-правових механізмів залучення інвесторів для фінансування бізнесу в Україні, створення робочих місць та відновлення інфраструктури нашої держави буде супроводжуватися зверненням також до реєстру індустріальних (промислових) парків України, міжнародного Реєстру збитків, завданих агресією Російської Федерації проти України та багатьох інших, запроваджних як в Україні так і за її межами.

Відомо, аби відбудувати зруйновані виробничі потужності підприємств, необхідні значні обсяги інвестицій. За даними спільної оцінки, оприлюдненої 23 березня 2023 року урядом України, Групою Світового банку, Європейською Комісією та ООН, потреби України на відновлення і відбудову зросли до 411 млрд. дол. США[1].

Вже складається практика надання міжнародними партнерами грантів, позик, кредитів, інших засобів фінансування процесу відновлюення інфраструктури та покращення якості життя громад, які постраждали від агресії. Наприклад, Європейський Союз виділив значний грант у розмірі 50 млн. євро для відновлення систем постачання електроенергії, води, опалення та управління відходами на деокупованих територіях Київщини.

Також деякі країни оголосили про намір сприяння деяким регіонам України у процесі відновлення. Попередньо 15 країн світу повідомили про допомогу в майбутній відбудові, зокрема, з частковою

[1] Собкевич О. Підтримка інвестицій у промисловості України в умовах війни та повоєнного відновлення. Національний інститут стратегічних досліджень 29.05.2023 року. URL: https://niss.gov.ua/news/komentari-ekspertiv/pidtrymka-investytsiy-u-promyslovist-ukrayiny-v-umovakh-viyny-ta.

фінансовою допомогою. Так, Італія буде інвестувати Рівне, відповідно Німеччина-Чернігів, Канада-буде відповідати за Суми, США та Туреччина за Харків, Чехія, Фінляндія, Швеція буде інвестувати у відбудову Луганська, Бельгія допоможе Миколаєву, Швеція та Нідерланди «має відповідати» за Херсон, Латвія надасть допомогу Запоріжжю[1].

І.Гужва надав аналітичний прогноз щодо страхування інвестицій в Україні від воєнних ризиків. Дозвіл здійснювати страхування інвестицій українських підприємств від ризиків, які можуть бути спричинені збройною агресією, бойовими діями та/або тероризмом – це логічний захід. Наявність механізму страхування інвестицій з боку Експортно-кредитного агентства (ЕКА) дозволить активізувати інвестиційну діяльність, зокрема це відкриє можливості для банківського фінансування, яке по суті на сьогодні фактично не використовується для фінансування проєктів у сфері виробництва[2].

Відповідний Закон «Про внесення змін до Закону України «Про фінансові механізми стимулювання експортної діяльності» щодо страхування інвестицій в Україні від воєнних ризиків» за № 3497-IX був прийнятий 22.11.2023 та набирає чинності з 1 січня 2024 року.

Згідно його положень на діяльність ЕКА із страхування та перестрахування не поширюються вимоги Закону України «Про страхування» щодо врегулювання переддоговірних відносин та розкриття інформації клієнтам до укладення договору страхування».

Уся система внутрішнього контролю представлена сукупністю заходів з внутрішнього аудиту, управління ризиками, комплаєнсу та інших елементів, визначених законадвтвом, а також політик, правил і заходів, які забезпечують функціонування, взаємозв'язок та підтримку таких заходів та елементів і спрямовані на досягнення визначених мети (місії), стратегічних та інших цілей, завдань, планів і вимог до діяльності надавача фінансових послуг.

---

[1] Провідні країни Європи відбудовуватимуть Україну. Веб-сайт LB.ua. URL: https://lb.ua/economics/2022/07/05/522198_providni_kraini_ievropi.html.

[2] Гужва І. Як убезпечити інвестиції під час війни. *Економічна правда.* 23 лютого 2023. URL: https://www.epravda.com.ua/columns/2023/02/23/697382/.

Згідно із законоположеннями щодо нового підходу передбачається «страхування та перестрахування експортних кредитів, а також страхування та перестрахування від воєнних та/або політичних ризиків кредитів українських суб'єктів господарювання, пов'язаних з інвестиціями у створення об'єктів та інфраструктури, необхідних для розвитку переробної промисловості та експорту товарів (робіт, послуг) українського походження», а також – «страхування та перестрахування прямих інвестицій з України, страхування та перестрахування прямих інвестицій в Україну від воєнних та/або політичних ризиків»[1].

ЕКА зможе покривати ризики, якщо використовуватиме власний статусний капітал, що на даний момент сягає близько 2 млрд. грн. Також є можливість залучити міжнародних перестрахувальників, що часто роблять в розвинутих країнах інші ЕКА. Наявність схем страхування інвестицій стимулюватиме інвестиційну активність. Це відкрило б можливості для банківського кредитування, яке зараз не використовується для фінансування виробничих проектів.

Перелік воєнних та політичних ризиків, а також умови та порядок страхування (перестрахування) таких ризиків при здійсненні ЕКА видів діяльності, доручено визначати Кабінетом Міністрів України за погодженням із Національним банком України[2]. Можна сподіватися, що реєстр індустріальних (промислових) парків України поповнюється новими об'єктами самн завдяки прийняттю вищезазначеного Закону.

Отже, відбувається процес доопрацювання законодавствачих механізмів залучення інвесторів. Тому науковцям необхідно донести важливість нових популярних знань про створення правових позицій щодо надання консультацій потенційним інвесторам. Здебільшого прозора підготовка інвестиційних пропозицій, обрання проектів з розвитку виробництва та експертна співпраця з потенційними ін-

[1] Про внесення змін до Закону України «Про фінансові механізми стимулювання експортної діяльності» щодо страхування інвестицій в Україні від воєнних ризиків: Закон України від 22.11.2023 р. № 3497-IX

[2] Там само.

весторами буде відбуватися, посилаючись на відомості міжнародного Реєстру збитків, завданих агресією Російської Федерації проти України.

Цей Реєстр створюється як платформа для міжурядового співробітництва, яка діє в інституційних рамках Ради Європи. На сьогодні в Реєстрі збитків для України беруть участь 43 країни та Євросоюз. Реєстр розташований у Гаазі (Королівство Нідерланди), він буде реєстром доказів і позовів про відшкодування, збитків або шкоди, завданих усім зацікавленим фізичним і юридичним особам, а також державі Україна міжнародно протиправними діями Росії в Україні або проти неї.

За Концепцією міжнародного компенсаційного механізму передбачено наступні категорії збитків: категорія (А) – збитки, завдані фізичним особам; категорія (В) – держава Україна, включаючи центральні та місцеві органи державної влади, державні чи підконтрольні установи; категорія (С) – юридичні особи, підприємства, в тому числі державні підприємства, підприємства критичної інфраструктури, фізичні особи - підприємці.

Функції Реєстру збитків грунтуються на цифровій платформі задля створення відповідного міжнародного інструментарію[1]. Реєстр має правовий статус юридичної особи згідно з національним законодавством Королівства Нідерландів та України і, таким чином, користується такою правоздатністю, яка необхідна для реалізації своїх функцій, виконання свого мандату і захисту своїх інтересів, зокрема здатністю укладати договори, набувати та відчужувати рухоме та нерухоме майно. Реєстр має здатність укладати договори з державами, міжнародними організаціями та органами в межах свого мандату[2].

Водночас наявність в Україні реєстрового публічного формату щодо актуалізації, збереження та використання відомостей про стан

[1] Про встановлення Розширеної часткової угоди про Реєстр збитків, завданих агресією Російської Федерації проти України: Резолюція CM/Res(2023)3 від 12.05.2023 р. URL: https://ips.ligazakon.net/document/view/mu23024?an=2&ed=2023_05_12. Ст. 2.

[2] Про приєднання України до Розширеної часткової угоди про Реєстр збитків, завданих агресією Російської Федерації проти України : Закон України від 08.11.2023 р. № 3432-IX. Ст. 3.

пошкодженого та зруйнованого житла, споруд, майна під час військової агресії сприяє реалізації низки цифрових прав українців та впливає на формування нормативно правових основ регулювання інвестиційної діяльності в Україні[1].

У Законі України «Про публічні електронні реєстри» закріплено систему реєстрів, яка включає базові реєстри; інші реєстри; визначені законом реєстри саморегулівних організацій. До базових реєстрів належать: державний земельний кадастр; Єдиний державний реєстр транспортних засобів; Реєстр будівель та споруд; Єдиний державний реєстр адрес; Державний реєстр речових прав на нерухоме майно та деякі інші.

До інших реєстрів належать реєстри, держателями яких є органи державної влади, органи місцевого самоврядування, юридичні особи публічного права, визначені законом, та які містять інформацію про окремі спеціальні статуси особи, про сертифікати, ліцензії, декларації, повідомлення, інші документи дозвільного характеру; про природні ресурси; про правові режими використання та забудови територій та окремих об'єктів; про рухоме майно, що відповідно до закону є об'єктом державного обліку; про майнові та немайнові права, їх обмеження та обтяження; про нормативно-правові акти, нормативні акти та документи технічного характеру, судові рішення, виконавчі документи, довіреності та про інші об'єкти, які відповідно до закону є об'єктами державного обліку, але не належать до об'єктів базових державних реєстрів, інші державні інформаційні ресурси.

Внаслідок руйнівної військової агресії Росії та тимчасової окупації частини нашої території актуалізувалося питання оцінки стану деурбанізації населених пунктів Харківської, Луганської, Донецької, Запорізької, Херсонської області та інших областей Центру, Сходу й Півдня нашої країни.

В Україні виправданим став правовий інтерес членів територіальних громад (у минулому їх мешканців, а нині - переселенців) щодо

[1] Андрущенко Л. В. Теоретичні аспекти формування нормативно правових основ регулювання інвестиційної діяльності в Україні. *Право і суспільство*. 2021. С. 38–42.

стану руйнації їх будівель, квартир, інших приміщень. Тут виникає необхідність дослідити функціональне призначення та комунікаційно-інформаційний потенціал Муніципального публічного реєстру щодо забезпечення правового інтересу членів територіальних громад із питання припинення територіального зростання міст, в тому числі внаслідок військової руйнації. Саме про показники деурбанізації такого характеру йдеться у даному дослідженні.

Також потенційні інвестори у відбудову нашої країни, цивілізовані країни світу та міжнародні організації є суб'єктами споживання реєстрової інформації про стан руйнування населених пунктів. Ця інформація орієнтує на обрання конкретних ключових завдань повоєнного відновлення України. Наприклад, Save the Children у співпраці з Центром Підтримки Бізнесу та Економічного Розвитку оголосили проєкт Грантової допомоги для відновлення та підтримки економічного розвитку в постраждалих районах Миколаївської області.

Вищезазначений підхід до виявлення показників припинення територіального зростання міст, в тому числі внаслідок військової руйнації, є актуальним для них. Отже гостро затребуваними стають вимоги до отримувача реєстрової інформації, тобто користувача, який відповідно до закону має право на її отримання у порядку електронної інформаційної взаємодії публічних електронних реєстрів.

Натомість розробка організаційно-правового механізму задоволення зазначених інтересів потребує дослідження низки питань функціонального призначення Муніципального публічного реєстру та його гнучкості щодо реагування на задоволення правового інтересу замовників. Затребувані для інвесторів відповідні відомості можуть мітитися не лише у базових реєстрах, але й реєстрах територіальних громад України.

Актуальною проблемою слід визнати співвідношення статусу та правових наслідків неналежного функціонування локальних та глобальних, а також - міжнародних публічних реєстрів та їх модифікацій.

Спрямування державної політики цифровізації економіки на створення дієвих механізмів захисту та реалізації права кожного на доступ до публічної інформації потребує правової визначеності при

використанні реєстрової інформації, здійсненні дозвільної діяльності, наданні адміністративних, соціальних та інших публічних послуг, виконанні управлінської діяльності та реалізації функцій державного регулювання. У багатьох успішних країнах зведення у ефективну систему публічних електронних реєстрів, як показує зарубіжний досвід, відбувалося, в основному, еволюційним шляхом. Еволюційний підхід дозволяє не лише ставити безпосередні, але й враховувати суміжні завдання щодо протидії корупції, забезпечення електронного урядування, залучення громадськості до формування та реалізації державної політики у сфері відносин цифрової економіки.

Контроль (державний та самоконтроль) щодо стану ресурсів публічних реєстрів в Україні слід визнати незбалансованим. Так, у реєстрі юридичних осіб має місце відображення неактуальних даних. Йдеться про економічно неактивні підприємства на непідконтрольній території Донецької та Луганської областей. За наявності законодавчого врегулювання особливих спрощених процедур ліквідації підприємств з боргами за рішенням власника така проблема могла б бути вирішена. Наприклад, за умови внесення відповідної редакції у законодавство про банкрутство така можливість може бути реалізованою шляхом звернення утримувача реєстру до скороченої судової процедури ліквідації таких підприємств із наступним внесенням відповідних відомостей до реєстру. Критичною є ситуація із контролем за оцінкою ризиків при складанні електронних податкових накладних у розрізі ризикових суб'єктів господарювання-платників податків. Фактично виявляється та заноситься до відповідного реєстру лише 20 % всіх виконавців ризикованих господарських операцій.

Однією з гарантій забезпечення безпеки функціонування електронної інформаційної взаємодії є належна формалізація вимог до реалізації контрольних функцій у сфері утримання реєстрів та звернення до їх ресурсів з метою використання. У Законі "Про публічні електронні реєстри" визначаються засади контролю та державного нагляду у сфері публічних електронних реєстрів. В ньому прописано статус центральних органів виконавчої влади, що реалізують держав-

ну політику із здійснення державного нагляду (контролю) у сфері формування і використання національних електронних інформаційних ресурсів, а також - держателя публічного електронного реєстру як особи, уповноваженої здійснювати контроль та управління публічним електронним реєстром[1].

Порядок здійснення контролю у сфері реєстрів розробляється Кабінетом Міністрів України згідно з вимогами законів, якими створено відповідні реєстри. Отже, пріоритетним шляхом підвищення ціннісного потенціалу цифрових публічних реєстрів у системі економіко-правової політики нашої держави стає досягнення дієвості контролю за їх утриманням та функціонуванням. Дієвість може бути підвищена, якщо виокремити коло суспільних відносин контролю, що виникають у сфері базових публічних електронних реєстрів, самостійним предметом правового регулювання Закону України «Про публічні електронні реєстри»[2]. За такого підходу доцільно конкретизувати вимоги до контролю базових реєстрів і вимоги - до контролю додаткових реєстрів. Вимоги мають бути диференційованими, а не спільними для цих класифікаційних рядів. До того ж вимоги до контролю базових реєстрів потребують системного закріплення у законодавстві, спираючись на принципи інституціалізації контролю.

Особливу увагу інформаційно-комунікативна функція публічних реєстрів привертає через запровадження механізмів досягнення ефективності результатів контролю у сфері господарювання. Отже у правовій науці дуже повільно опрацьовуються відомі та напрацьовуються нові знання щодо реалізації потенціалу контролю, використовуючи ресурс електронних публічних реєстрів.

Аналіз можливості забезпечення ефективності функціонування публічних реєстрів для здійснення контролю показав, що їх стан може надавати переваги у системі правових засобів контролю. коли йдеться про протидію зловживанням у сфері господарювання.

---

[1] Інформаційне суспільство в Україні: глобальні виклики та національні можливості: аналіт. доп. / Д. В. Дубов, О. А. Ожеван, С. Л. Гнатюк. Київ : НІСД. 2010. С. 29.

[2] Про публічні електронні реєстри : Проєкт Закону України від 10.09.2019 р. № 2110. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=66772.

В Україні утримувачами Єдиних та Державних реєстрів є: Міністерство юстиції України, Державна виконавча служба України, Державна служба з питань захисту персональних даних України. Для суб'єктів господарювання актуальними є: Єдині та Державні реєстри інформаційної мережі Міністерства юстиції України. Зокрема, Державний реєстр обтяжень рухомого майна, Єдиний реєстр громадських формувань, Єдиний реєстр підприємств, щодо яких порушено провадження у справі про банкрутство, Єдиний державний реєстр юридичних осіб, фізичних осіб – підприємців та громадських формувань, Реєстр громадських об'єднань, Єдиний реєстр громадських формувань, Державний реєстр речових прав на нерухоме майно.

Зорієнтованість узагальнюючого аналізу на наявні недостатньо вивчені правові проблеми, дозволила виявити можливості розширення функціоналу електронних публічних реєстрів. Зокрема новою є сама постановка проблеми сприйняття електронних публічних реєстрів юридичною гарантією реалізації цифрових прав.

## 7.2. Функціонал публічних електронних реєстрів як юридична гарантія реалізації цифрових прав

Проблеми реалізації цифрових прав вивчалися вітчизняними та зарубіжними дослідниками. Вагомих здобутків отримано О.М. Вінник у монографії «Право цифрової економіки»[1] та циклі статей, в яких визначено межі цифрової свободи, переваги і ризики цифровізації.

Реформаторським заходом у визначенні єдиних вимог до реєстрової інформації та її статусу став Закон України «Про публічні електронні реєстри». На законодавчому рівні було прописано правовий статус/режим реєстрів (будь-якої їх складової). Вони перебувають у власності держави, відповідної територіальної громади або відпо-

[1] Вінник О. Право цифрової економіки: монографія. Київ: НДІ приватного права і підприємництва імені академіка Ф. Г. Бурчака НАПрН України, 2021. 350 с.

відної саморегулівної організації в особі держателя відповідного реєстру.

Максимально широкий перелік завдань та вимоги до суб'єктів формування відомостей Реєстру, а також – до порядку обігу реєстрової інформації закладається у Положення про Муніципальний реєстр міста. Але й воно не може бути визнано змістовно повним. Як показав аналіз практики розробки Положень про Муніципальний реєстр із різних міст в них наводяться терміни, які вживаються у значно біднішому значенні порівняно з їх функціональним призначенням та визначенням у нормативно-правових актах про публічні реєстри.

У Муніципальних реєстрах доцільно формувати первинні показники «деурбанізації» українських населених пунктів. Але така пропозиція призводить до необхідності виділення окремої групи «цифрових прав», до якої слід віднести право на доступ до офіційно встановлених показників деурбанізації українських населених пунктів. Електронні публічні реєстри, в тому числі Муніципальні, за умови їх належного функціонування виступають юридичною гарантією реалізації відповідних цифрових прав. Цифрові права – це такі права людини, які дозволяють отримувати доступ, використовувати, створювати та публікувати цифрові носії або отримувати доступ до комп'ютерів, інших електронних пристроїв або мереж зв'язку.

Результати дослідження зазначеної проблематики є важливими для поширення практики користування цифровими правами в умовах запровадження економіки відновлення, для популяризації знань про цифровізацію економіки, потенціал публічних електронних реєстрів та інш. Фундаментальні наукові дослідження з проблеми розвитку потенціалу цифрових прав мають вагоме значення для підвищення цифрової зрілості нашої держави та суспільства[1].

[1] Шаповалова О. В. Показники «деурбанізації» у муніципальних реєстрах: правовий інтерес щодо їх актуалізації. *Збірник наукових праць НДІ ПЗІР НАПрН України : Цифрові трансформації України 2023: виклики та реалії* : за матеріалами IV Круглого столу (м. Харків, 29 вересня 2023 року) / за ред. С. В. Глібка та ін. Харків: НДІ ПЗІР НАПрН України, 2023. С. 27–34.

Визначення поняття цифрової держави як певної сукупності реєстрів, баз даних, які між собою взаємодіють має суто практичне забарвлення. Воно широко розповсюджено у публіцистичних та інших ненаукових джерелах. Саме у такому значенні сприймали загрози її існуванні у перші дні російсько-української війни. Але «цифрова держава не похитнулась і продовжила розвиватись і працювати» довів М. Федоров, надаючи (як міністр цифрової трансформації України ) звіт про технологічні досягнення України у 2022 році[1].

Попри повномасштабну агресію з боку Росії, наша країна опікується розширенням можливостей щодо реалізації цифрових прав як фізичними особами так і юридичними. Україна має суттеві успіхи у захисті персональних даних своїх громадян. Законом України «Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів» передбачено можливість створення резервних копій державних інформаційних ресурсів та систем на окремих фізичних носіях у зашифрованому вигляді та їх зберігання, у тому числі за межами України (зокрема в закордонних дипломатичних установах України) протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування[2].

Так, як превентивний зсіб захисту персональних даних своїх громадян нашою державою забороняється розміщення та зберігання резервних копій державних інформаційних ресурсів та систем на території України, де органи державної влади України тимчасово не здійснюють свої повноваження, територіях держав, визнаних Верховною Радою України державами-агресорами, територіях держав, щодо

[1] Яковлева О. Цифрова держава не похитнулась і продовжила розвиватись і працювати – Інтерв'ю з Михайлом Федоровим. Матеріали ЗМІ від 11 січня 2023 р. URL: https://vikna.tv/istorii/interviu/intervyu-myhajla-fedorova-pro-dosyagnennya-ukrayiny-v-czyfrovizacziyi/.

[2] Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів: Закон України від 15.03.2022 № 2130-IX. URL: https://zakon.rada.gov.ua/laws/show/2130-20#Text.

яких застосовані санкції відповідно до Закону України «Про санкції», та територіях держав, які входять до митних та воєнних союзів з такими державами, забороняється.

Зараз в Україні нараховується понад 350 реєстрів. З них було сформовано групу реєстрів, критерієм відбору до якої була теоретична можливість (на думку авторів) їх подальшого використання для надання інформаційної підтримки щодо розробки та проведення соціальної політики держави.

З метою з'ясування придатності наявної в Україні множини електронних адміністративних реєстрів для створення на їх базі повноцінної системи реєстрів, здійснено докладний аналіз електронних інформаційних ресурсів основного переліку. Автори свідомі того, що досліджені реєстри / бази даних є тільки частиною значно більшої кількості електронних інформаційних ресурсів, які створені та використовуються переважно органами влади та самоврядування для виконання ними власних функцій, хоча існують і реєстри професійних об'єднань, організацій, компаній, підприємств[1].

Аналіз показав, що існує перелік угрупувань та окремих цифрових прав, забезпечення реалізації яких потребує нормативного врегулювання.

Дослідники виокремлюють самостійну групу цифрових прав, яка за важливістю та значимістю для суспільства потребують конституціоналізації. Важливість дослідницького інтересу щодо можливість реалізації даних прав значною мірою впливає на реалізацію не лише цифрових прав, але й багатьох конституційних прав. Зокрема, таких як право на освіту.

Освітня компонента відіграє велике значення для опанування цифровою грамотністю. Саме в освітньому процесі студентами та аспірантами набуваються індивідуальні навички надбання цифрових прав та їх реалізації. Наприклад, досвід викладання дисципліни «Розробка докторського проекту» (для здобувачів вищої освіти ІІІ освітнього рівня спеціальності 081 «Право») підтверджує відповідну зо-

[1] Електронні реєстри: стан в Україні: кол. моногр. / за ред. О.М. Гладуна; НАН України, Ін-т демографії та соціальних досліджень імені М.В. Птухи. Київ, 2021. 636 с.

рієнтованість освітнього процесу у Східноукраїнському національному університеті імені Володимира Даля.

Так, для аспірантів передбачено вивчення теми «Концепція цифровізації економіки України». Стислий зміст теми показує наявність для розгляду наступних важливих питань підвищення цифрової грамотності.

1. Зміна напрямів економічної політики під впливом цифровізації економіки.

2. Цифровізація економіки у протидії зловживанням та корупції.

3. Концепція розвитку цифрової економіки та суспільства України. Реформування системи електронних публічних реєстрів.

4. Загальні засади та проблеми правового регулювання відносин у сфері цифрової економіки.

5. Дослідження щодо модернізації національного законодавства та правової інфраструктури цифрової економіки.

6. Набуття суб'єктами господарювання цифрових компетенцій як одне з очікувань від запровадження Концепції.

7. Цифрова інфраструктура контролю у сфері господарювання.

На практичних заняттях аспіранти здійснюють критичний аналіз щодо обрання державними фіскальними органами України моделі блокуючого контролю при адмініструванні податку на додану вартість. Вони проектують моделі руйнування злочинних схем з ПДВ та надають науково-практичний коментар Постанови Кабінету Міністрів України від 23 грудня 2022 року за №1428 щодо змін до Порядку блокування податкових накладних.

Важливим завданням практичного заняття за вказаною темою є доведення прозорості поведінки користувачів платформами «Уряд для бізнесу», «Бізнес для бізнесу», «Бізнес для споживачів», «Бізнес для уряду», «Споживачі для бізнесу», «Споживачі для споживачів», «Споживачі для уряду».

Теоретико-практичне забарвлення містить постановка проблеми врегулювання та/або вирішення конфліктів і спорів у сфері цифрової економіки. Також на практичному занятті аспіранти працюють з реєстром судових рішень та виокремлюють у рішеннях (для подальшо-

го аналізу) специфіку провадження та процедурні особливості щодо окремих категорій врегулювання та/або вирішення конфліктів і спорів у сфері цифрової економіки.

Щоб активізувати членів суспільства щодо оволодіння цифровою грамотністю, необхідно розвивати в освіті нові напрямки критичної цифрової обізнаності. Обізнаність дозволяє розпізнавати виклики їхнім цифровим правам, а також прищеплювати мотивацію та навички вимагати їх[1].

Корегування правової організації системи електронних публічних реєстрів під впливом зміни державної політики вже визнається сталою практикою цивілізованих країн. В Україні до визнаної ними практики, в основному, адаптовано підходи до реалізації державної політики цифрового розвитку.

Зокрема, ця політика грунтується на принципах: орієнтованості на громадян (полягає в забезпеченні першочергового врахування потреб та очікувань громадян під час прийняття рішень щодо форм чи способів здійснення функцій держави); інклюзивності та доступності (орієнтація на забезпечення можливості для всіх громадян користуватися новітніми досягненнями інформаційних технологій доступу до сервісів); безпечності та конфіденційності (полягає в забезпеченні для громадян і суб'єктів господарювання безпечного та надійного середовища, в якому відбувається електронна взаємодія з державою, включаючи повну його відповідність правилам і вимогам, встановленим законами України щодо захисту персональних даних та інформації, що належить державі, електронної ідентифікації та довірчих послуг); багатомовності (передбачає забезпечення надання громадянам і суб'єктам господарювання адміністративних, інформаційних та інших послуг, включаючи транскордонні, з використанням мови за їх вибором); підтримки прийняття рішень (полягає в забезпеченні використання новітніх інформаційних технологій для розроблення програмних продуктів, які підтримують прийняття рішень органами виконавчої влади під час реалізації владних повноважень); адміністра-

[1] Pangrazio L., Sefton-Green J. Digital Rights, Digital Citizenship and Digital Literacy: What's the Difference? *Journal of New Approaches in Educationa Research.* 2021. 9(2). DOI: 10.7821/naer.2021.1.616.

тивного спрощення (орієнтація на забезпечення прискорення та спрощення адміністративних процесів шляхом їх цифрового розвитку); збереження інформації (полягає в забезпеченні зберігання рішень, інформації, записів та даних, достовірності та цілісності, а також їх доступності відповідно до політики безпеки та конфіденційності протягом певного часу); оцінювання ефективності та результативності (передбачає проведення всебічного оцінювання та порівняння не менш як двох альтернативних рішень для забезпечення ефективності та результативності реалізації владних повноважень) .

Закладами вищої освіти проводяться навчальні заходи задля набуття відповідних професійних компетентностей державними службовцями, які займають посади категорії «Б» та «В» та посадовими особами місцевого самоврядування. Зокрема, йдеться про загальну короткострокову програму підвищення кваліфікації «Державна політика цифрового розвитку України» та інші пропозиції ЗВО.

Уявлення науковців, державних службовців та інших фахівців щодо обігу реєстрової інформації на зазначених принципах, спонукає до виявлення/оцінки достатності та належності системно-структурних і змістовних зв'язків між відповідними нормативними актами загального й спеціального рівня регулювання.

Обізнаність у зазначеній сфері живиться не лише досвідом, але й – вагомими результатами економіко-правових досліджень. Взагалі зростає роль правової науки та відбуваються зміни у формуванні світогляду науковців та майбутніх докторів філософії.

Правовим проблемам забезпечення державою соціального спрямування цифровізації були присвячені дослідження О.М. Вінник. Вчена виявляє недоліки захисту цифрових прав громадян у разі їх порушення та притягнення до відповідальності за зловживання зазначеними правами та обґрунтовує пропозиції щодо прийняття Цифрового кодексу України та відповідного корегування положень інших кодексів та законів України з ціллю закріплення в них особливостей реалізації цифрових прав та цифрових обов'язків учасників відносин у відповідних сферах суспільного буття[1].

[1] Вінник О. М. Конституційні засади цифровізації. *Взаємодія норм міжнародного і національного права крізь призму процесів глобалізації та інтеграції*: Матеріали

Науковою спільнотою, хоча й повільно, але вже напрацьовуються підходи до визначення поняття цифрового громадянства. Відомо ставлення до цифрового громадянства як до норми належної, відповідальної поведінки щодо використання технологій. Зокрема, таке ставлення відбувається через певні елементи цифрового громадянства такі як: цифровий доступ, цифрова комерція, цифрова комунікація, цифрова грамотність, цифровий етикет, цифрове право, цифрові права та обов'язки, Digital Health & Wellness: фізичне та психологічне благополуччя у світі цифрових технологій, електронні запобіжні заходи для гарантування безпеки[1].

Втілення зазначених елементів у визначення таким чином поняття цифрового громадянства не є безспірним. Більш дієвими можна визнати інші підходи, за якими перспективу становлення так званого цифрового громадянства розглядають паралельно із цифровими правами та цифровою грамотністю. Його дієвість проявляється у зорієнтованості на усвідомлення проблем, пов'язаних з цифровими правами членів суспільства.

На ефективність відповідних вимог, виходячи з вищезазначеного визначення, має прямий вплив визнання та конкретизація цифрового статусу учасників суспільних відносин в певних сферах.

О.М. Вінник обґрунтувала важливість проблеми цифрового громадянства, адже від її вирішення залежить і визначення цифрового статусу учасників суспільних відносин в певних сферах. Для досягнення цього результату логічною та вчасною стає пропозиція вченої про закріплення в Конституції цифрових прав та цифрових обов'язків громадян[2]. Отже, наша країна повинна спрямовувати свою економіч-

Міжнародної науково-практичної конференції викладачів, співробітників закладів вищої освіти і наукових організацій, магістрантів, аспірантів, докторантів, представників громадських організацій, органів державної влади та органів місцевого самоврядування, підприємств та іншихустанов (09 листопада 2022 р.). Київ: видвоСНУім. В. Даля, 2022. С.12 (216 с.)

[1] Nine elements of digital citizenship. 2017. WACC COMUNICATION FOR ALL. https://waccglobal.org/nine-elements-of-digital-citizenship/.

[2] Вінник О. М. Цифрові права в умовах війни. Деокупація. *Юридичний фронт*: матеріали Міжнародного експертного круглого столу (Київ, 18 березня 2022 р.). Державний торговельно-економічний університет, Українська асоціація порівняль-

ну та правову політику на підвищення зрілості цифрового громадянства.

Необхідність підвищення обумовлена тим, що «цифровізаційні процеси підняли проблему цифрового громадянства як такого, що має забезпечувати баланс приватних і публічних інтересів при реалізації цифрових можливостей, а також має дати поштовх до визначення цифрового статусу учасників відносин в різних сферах суспільного буття, включно з економікою[1].

Вперше в Україні на монографічному рівні О.М. Вінник комплексно досліджує питання взаємозв'язку цифровізації з інститутами громадянського суспільства та розвитком інформаційної сфери та пов'язаних з цим проблем правового регулювання. Внаслідок проведеного нею аналізу конкретизується та деталізується значимість державної економіко-правової політики щодо цифровізації та правового забезпечення соціального спрямування цифрової економіки та меж цифрової свободи[2].

Фінансова можливість підвищення цифрової грамотності розширюється. Для України стали доступними чотири основні напрями, за якими можна отримати фінансування задля позитивного впливу на здобутки цифрової грамотності.

Фахівці пойменували ці чотири напрями наступним чином: Високопродуктивний комп'ютинг – 2,2 млрд євро. Сюди подаються проекти, які обчислюють великі масиви даних для рішень у сфері економіки, охорони здоров'я або оборонної промисловості.

Штучний інтелект, дані та хмарні послуги – 2,1 млрд євро. Сюди подаються проекти, які створюють продукти на базі штучного інте-

---

ного правознавства, Українська асоціація міжнародного права, Асоціація реінтеграції Криму; упоряд. інаук. ред. О.В. Кресін. Київ: Держ. торг.-екон. ун-т, 2022. С. 147-149 (224 с.) URL: https://mail.google.com/mail/u/0/?pli=1#inbox/QgrcJHsBqLqFpgQsLwkkvvXbJRsWkKGTZBQ?projecto r=1.

[1] Вінник О. М. Правове регулювання відносин цифровізації: місце і роль в правовій системі та системі господарського права України. *Актуальні проблеми права: теорія і практика: збірник наукових праць.* 2022. No 1 (43). С. 23.

[2] Вінник О. Право цифрової економіки: монографія. Київ: НДІ приватного права і підприємництва імені академіка Ф. Г. Бурчака НАПрН України, 2021. 350 с.

лекту для полегшення роботи підприємств, держадміністрацій або дослідницьких установ.

Цифрові навички – 580 млн євро. Сюди подаються проекти, які створюють можливості для набуття нових навичок у сфері ІТ.

Використання цифрових технологій в економіці та суспільстві – 1,1 млрд євро. Сюди подаються проекти, які впроваджують цифровізацію у бізнес або у сферу електронного урядування, охорони здоров'я, навколишнього середовища, технологій Smart City, освіти[1].

Дороговказом у вивченні правових питань досягнення балансу цифрової зрілості держави та суспільства може слугувати монографія О.М. Вінник «Право цифрової економіки». В ній напрацьовано сучасні підходи до розв'язання значної частини нових проблем щодо правового забезпечення відносин цифрової економіки та її соціального спрямування. Зокрема, вчена виокремлює брак виваженого ставлення до подвійної за наслідками природи цифрових технологій, які можуть використовуватися як на благо, так і на шкоду не лише окремим особам, а й суспільству в цілому. Вона обґрунтовує значні переваги та (водночас) виявляє ризики цифровізації економіки та пов'язані з цим проблеми правового регулювання[2].

У монографії пропонується низка виважених заходів, спрямованих на забезпечення контролю за використанням електронних ресурсів (зокрема державна реєстрація відповідальних за їх використання у сфері бізнесу та інших публічних сферах осіб; визначення основних засад відповідальності за недобросовісне та/або неконтрольоване чи ризиковане їх використання у сфері економіки; покладення низки додаткових обов'язків на відповідальний за цифровіза-

[1] Скрипін В. Україна долучилася до програми «ЦифроваЄвропа» – з бюджетом 7,5 млрд євро. URL: https://itc.ua/ua/novini/ukrayina-doluchilasya-do-programi-tsifrova-yevropa-z-byudzhetom-7-5-mlrd-yevro-na-superkomp-yuteri-shtuchnij-intelekt-kiberbezpeku-ta-shhe-dva-tsifrovi-napryamki/.

[2] Вінник О. Право цифрової економіки: монографія. Київ: НДІ приватного права і підприємництва імені академіка Ф. Г. Бурчака НАПрН України, 2021. С. 40–49.

цію уповноважений орган) та закріплення подібних механізмів у кодифікованому акті[1].

Надаючи оцінку цифрової зрілості нашої держави як суб'єкта створення, адміністрування, використання інформаційно-комунікаційних ресурсів, а також – зрілості суспільства як суб'єктів споживання інформаційно-комунікаційного ресурсу, слід зробити наступні висновки:

1. Після 24 лютого 2022 року в Україні вібулися важливі зміни економічної політики ситуативного характеру. За своїм змістом зміни ситуативного характеру актуалізували необхідність дослідження передусім наступних правових проблем: а) вдосконалення цифрового контролю та самоконтролю у сфері господарювання в умовах воєнного стану та післявоєнного відновлення економіки; б) розширення функціоналу електронних публічних реєстрів як юридичної гарантії реалізації цифрових прав; в) збалансування обсягу цифрової грамотності сусільства з рівнем цифровізації державних інституцій, внаслідок запровадження дієвих механізмів популяризації сучасних онлайн-процесів та інше.

2. Функціонування цифрових публічних реєстрів у системі контролю як фундаментальних інструментів відповідної політики України забезпечується низкою оновлених законів та підзаконних актів. З прийняттям Закону України «Про цифровий контент та цифрові послуги» потребується напрацювання теоретичних засад системного тлумачення співвідношення цього Закону з Законом України «Про публічні електронні реєстри». Орієнтація на наявні правові проблеми правового статусу низки реєстрі залишає дискусійним питання їх впливу на формування юридичних гарантій реалізації цифрових прав.

3. Аналіз аргументів доводить високий рівень цифрової зрілості нашої держави як суб'єкта створення, адміністрування, використання надбань цифровізації та невідповідний рівень цифрової зрілості

[1] Вінник О. Право цифрової економіки: монографія. Київ: НДІ приватного права і підприємництва імені академіка Ф. Г. Бурчака НАПрН України, 2021. С. 50.

суспільства як узагальненого суб'єкта споживання та використання цифрових послуг. Україна отримала статус учасниці програми Європейського Союзу «Цифрова Європа». Міжнародні зобов'язання нашої країни щодо наближення сучасного праворозуміння до правового простору ЄС залишаються актуальними, але стають багатовекторними. Опосередкування адаптації щодо питання правового забезпечення розвитку технологій цифрової економіки та суспільства цілком виправдано розглядати (поруч з іншими ракурсами проблеми) і в аспекті доведення значимості розв'язання проблеми досягнення балансу цифрової зрілості держави та цифрової зрілості суспільства.

4. Важливими подіями цифрової трансформації нашої країни у сфері освіти та комунікації стало вивчення у режимах онлайн американського досвіду формування докторських програм, Зальцбургських принципів та Європейського досвіду, вимог щодо акредитації PhD програм та багато інш. Серед низки проблем досягнення балансу потенціалу цифрової зрілості нашої держави та цифрової зрілості суспільства, що потребують розв'язання, гостро постала необхідність методологічного забезпечення відповідних тем освітнього процесу, які доводять важливу роль в суспільному житті України підвищення масштабів оволодіння суспільством цифровою грамотністю.

5. Вагоме значення для підвищення цифрової зрілості нашої держави мають фундаментальні наукові дослідження з найбільш важливих проблем розвитку потенціалу цифрової держави та досягненню співмірності йому цифрового потенціалу суспільства. Зокрема, узагальнення результатів фундаментального дослідження проблем функціонування електронних публічних реєстрів у межах теми НДІ ПЗІР НАПрН України «Правове забезпечення розвитку технологій цифрової економіки та суспільства».

# ДОДАТОК

## Порівняльна таблиця Директиви (ЄС) 2019/770 та Закону України «Про цифровий контент та цифрові послуги»

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| Ст. 1. Предмет і мета. Метою цієї Директиви є сприяння належному функціонуванню внутрішнього ринку, одночасно забезпечуючи високий рівень захисту споживачів, шляхом встановлення загальних правил щодо певних вимог щодо контрактів між торговцями та споживачами щодо постачання цифрового контенту чи цифрових послуг, зокрема, правила щодо:<br>— відповідність цифрового контенту або цифрової послуги договору,<br>— засоби правового захисту у разі відсутності такої відповідності або ненадання постачання, а також способи застосування цих засобів правового захисту, а також<br>— модифікація цифрового вмісту або цифрової послуги. | Аналог відсутній. |
| П. 1. Ст. 2. **«цифровий контент»** означає дані, створені та надані в цифровій формі; | П. 10. Ст. 2. **цифровий контент** - дані, які створюються і надаються в цифровій формі. До цифрового контенту належать, зокрема, комп'ютерні програми, застосунки, відеофайли, аудіофайли, музичні файли, цифрові ігри та електронні книги |
| П. 2. Ст. 2. **«цифрова послуга»** означає:<br>(а) послуга, яка дозволяє споживачеві створювати, обробляти, зберігати або отримувати доступ до даних у цифровій формі; або | П. 9. Ст. 2. **цифрова послуга** - послуга, що надає можливість споживачу створювати, обробляти, зберігати та поширювати дані у цифровій формі або отримувати доступ до таких даних, а також здійснювати будь-які інші дії з даними у цифровій формі, що були створені чи завантажені споживачем або іншими користувачами такої послуги. |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| (б) послуга, яка дозволяє обмінюватися даними в цифровій формі, завантаженими або створеними споживачем чи іншими користувачами цієї послуги, або будь-яку іншу взаємодію з ними; | До цифрових послуг належать, зокрема такі, що дають змогу створювати, обробляти, отримувати доступ або зберігати дані в цифровій формі, включаючи хостинг файлів, обробку текстів або гри, які пропонуються в середовищі хмарних обчислень і соціальних мережах |
| П. 3 Ст. 2. «**товари з цифровими елементами**» означає будь-які матеріальні рухомі об'єкти, які включають або взаємопов'язані з цифровим контентом чи цифровою послугою таким чином, що відсутність такого цифрового контенту чи цифрової послуги перешкоджає виконанню товарами своїх функцій; | П. 7. Ст. 2. «**товар з цифровими елементами**» - рухома річ, що містить у собі або пов'язана з використанням цифрового контенту та/або цифрової послуги таким чином, що відсутність цифрового контенту та/або цифрової послуги унеможливлює виконання таким товаром його функцій; |
| П. 4 Ст. 2 «**інтеграція**» означає зв'язування та об'єднання цифрового контенту або цифрової послуги з компонентами цифрового середовища споживача для того, щоб цифровий контент або цифрова послуга використовувалися відповідно до вимог щодо відповідності, передбачених цією Директивою; | П. 3 Ст. 2. «**інтеграція**» - поєднання цифрового контенту та/або цифрової послуги з елементами цифрового середовища споживача з метою використання цифрового контенту та/або цифрової послуги згідно з вимогами щодо відповідності, визначеними цим Законом; |
| П. 5 Ст. 2. «**торговець**» (**trader**) означає будь-яку фізичну або юридичну особу, незалежно від того, чи є вона приватною чи державною, яка діє, в тому числі через будь-яку іншу особу, що діє від імені цієї фізичної чи юридичної особи або від імені цієї особи, для цілей, пов'язаних із торгівлею, бізнесом цієї особи, ремесла або професії стосовно контрактів, на які поширюється дія цієї Директиви; | П. 1 Ст. 2. **виконавець** - фізична або юридична особа незалежно від форми власності, яка на підставі укладеного із споживачем договору надає або зобов'язується надати йому цифровий контент та/або цифрову послугу (самостійно або через іншу особу, що діє від її імені або за її дорученням) у межах підприємницької діяльності, що здійснюється такою особою. Виконавець є суб'єктом електронної комерції в розумінні Закону України «Про електронну комерцію». Виконавцем може вважатися постачальник послуг проміжного характеру в розумінні Закону України «Про електронну комерцію», якщо такий постачальник виступає як безпосередня сторона договору, укладеного із споживачем, щодо надання цифрового контенту та/або цифрової послуги; |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| | Ч. 2 Ст. 2. Терміни «споживач» та «**продавець**» вживаються в цьому Законі у значеннях, наведених у Законі України «Про захист прав споживачів».<br>П. 18 Ст. 1 Закону України «Про захист прав споживачів»: «продавець» - суб'єкт господарювання, який згідно з договором реалізує споживачеві товари або пропонує їх до реалізації; |
| П. 6 Ст. 2. «**споживач**» означає будь-яку фізичну особу, яка стосовно контрактів, на які поширюється дія цієї Директиви, діє з метою, що виходить за межі торгівлі, бізнесу, ремесла чи професії цієї особи; | Ч. 2 Ст. 2. Терміни «**споживач**» та «продавець» вживаються в цьому Законі у значеннях, наведених у Законі України «Про захист прав споживачів».<br>П. 22 Ст. 1 Закону України «Про захист прав споживачів»: «споживач» - фізична особа, яка придбаває, замовляє, використовує або має намір придбати чи замовити продукцію для особистих потреб, безпосередньо не пов'язаних з підприємницькою діяльністю або виконанням обов'язків найманого працівника; |
| П. 7 Ст. 2 «**ціна**» означає гроші або цифрове відображення вартості, яка має бути сплачена в обмін на постачання цифрового контенту чи цифрової послуги; | «Про ціни і ціноутворення»: Закон України від 21.06.2012 № 5007-VI15.<br>П. 15 Ст. 1. «**ціна**» - виражений у грошовій формі еквівалент одиниці товару; |
| П. 8 Ст. 2. «**персональні дані**» означає персональні дані, як визначено в пункті (1) статті 4 Регламенту (ЄС) 2016/679;<br><br>«персональні дані» означає будь-яку інформацію, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати («суб'єкт даних»); фізична особа, яку можна ідентифікувати, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами як ім'я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор або за одним чи декількома факторами, що є визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної сутності такої фізичної особи; | Ч. 2. Ст. 2. … терміни «**персональні дані**» та «обробка персональних даних» вживаються в цьому законі у значеннях, наведених у Законі України «Про захист персональних даних». (стаття 2)<br><br>«персональні дані» - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована; |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| П. 9 Ст. 2 «**цифрове середовище**» означає апаратне забезпечення, програмне забезпечення та будь-яке мережеве з'єднання, яке використовується споживачем для доступу або використання цифрового контенту чи цифрової послуги; | П. 10 Ст. 2 «**цифрове середовище**» - апаратне, програмне забезпечення та будь-яке мережеве підключення, що використовується з метою отримання доступу до цифрового контенту та/або цифрової послуги та забезпечує можливість їх використання споживачем; |
| П. 10 Ст. 2 «**сумісність**» означає здатність цифрового контенту або цифрової послуги функціонувати з апаратним або програмним забезпеченням, з яким зазвичай використовується цифровий контент або цифрові послуги того самого типу, без необхідності конвертувати цифровий контент або цифрову послугу; | П. 6 Ст. 2 **сумісність** - придатність цифрового контенту та/або цифрової послуги до взаємодії з апаратним чи програмним забезпеченням, що зазвичай використовується з таким цифровим контентом та/або цифровою послугою, без необхідності їх перетворення; |
| П. 11 Ст. 2 «**функціональність**» означає здатність цифрового контенту або цифрової послуги виконувати свої функції з урахуванням їх призначення; | П. 8 Ст. 2 **функціональність** - придатність цифрового контенту та/або цифрової послуги до виконання своїх функцій відповідно до призначення цифрового контенту та/або цифрової послуги; |
| П. 12 Ст. 2 «**інтероперабельність**» означає здатність цифрового контенту або цифрової послуги функціонувати з апаратним або програмним забезпеченням, відмінним від тих, з якими зазвичай використовується цифровий контент або цифрові послуги того самого типу; | П. 4 Ст. 2 «**інтероперабельність**» - придатність цифрового контенту та/або цифрової послуги до взаємодії з апаратним чи програмним забезпеченням, відмінним від того, що зазвичай використовується з цифровим контентом та/або цифровою послугою того самого типу; |
| П. 13. Ст. 2 «**довговічний носій**» означає будь-який інструмент, який дозволяє споживачеві або продавцю зберігати інформацію, адресовану особисто цій особі, у спосіб, доступний для подальшого використання, протягом періоду часу, відповідного цілям інформації, і який дозволяє відтворювати її без змін. збереженої інформації. | П. 2 Ст. 2 «**довговічний носій**» - засіб, що дає змогу виконавцю чи споживачу зберігати адресовані йому особисто дані у спосіб, що надає можливість їх подальшого використання протягом строку, достатнього з точки зору характеру таких даних, а також відтворення інформації, яка зберігається на носії, у незмінному вигляді; |
| Стаття 3 **Область застосування**<br>1. Ця Директива застосовується до будь-якого контракту, за яким продавець постачає або зобов'язується надати цифровий контент або цифрову послугу споживачеві, а споживач платить або зобов'язується сплатити ціну. | Стаття 1. **Сфера регулювання** цього Закону<br>1. Цей Закон регулює відносини між виконавцем та споживачем щодо надання цифрового контенту та/або цифрової послуги. |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| Ця Директива також застосовується, якщо продавець постачає або зобов'язується надавати цифровий контент або цифрову послугу споживачеві, а споживач надає або зобов'язується надавати персональні дані продавцю, за винятком випадків, коли персональні дані, надані споживачем, обробляються виключно трейдер з метою надання цифрового контенту чи цифрової послуги відповідно до цієї Директиви або для того, щоб дозволити торговцю відповідати юридичним вимогам, яким підпорядковується торговець, і торговець не обробляє ці дані з будь-якою іншою метою.<br>2. Ця Директива також застосовується, якщо цифровий контент або цифрові послуги розроблені відповідно до специфікацій споживача.<br>3. За винятком статей 5 і 13, ця Директива також застосовується до будь-якого матеріального носія, який служить виключно носієм цифрового контенту. | 2. Дія цього Закону поширюється також на:<br>1) відносини, в яких виконавець на підставі договору надає або зобов'язується надати цифровий контент та/або цифрову послугу споживачу, а споживач надає або зобов'язується надати свої персональні дані, крім випадків, якщо їх надання необхідне виключно для одержання цифрового контенту та/або цифрової послуги, без наміру подальшого використання персональних даних для досягнення будь-яких інших цілей;<br>2) відносини, в яких цифровий контент та/або цифрові послуги розробляються відповідно до специфікації споживача;<br>3) відносини, в яких виконавець на підставі договору надає або зобов'язується надати цифровий контент на матеріальному носії, що використовується виключно для зберігання такого цифрового контенту.<br>3. Дія положень Закону України «Про захист прав споживачів» поширюється на суб'єктів, визначених цим Законом у частині відносин, не врегульованих цим Законом. |
| Стаття 3. Область застосування<br>4. Ця Директива **не застосовується** до цифрового контенту чи цифрових послуг, які включені в товари або взаємопов'язані з товарами у значенні пункту (3) статті 2, і які надаються разом з товарами згідно з договором купівлі-продажу щодо цих товарів, незалежно від того, надається такий цифровий вміст або цифрова послуга продавцем чи третьою стороною. У разі сумніву щодо того, чи є постачання об'єднаного чи взаємопов'язаного цифрового контенту або об'єднаної чи взаємопов'язаної цифрової послуги частиною договору купівлі-продажу, вважатиметься, що цифровий вміст чи цифрова послуга підпадають під дію договору купівлі-продажу. | Стаття 1. Сфера регулювання цього Закону<br>4. Дія цього Закону **не поширюється** на регулювання відносин щодо:<br>1) надання цифрового контенту та/або цифрових послуг, що входять до складу товарів з цифровими елементами або взаємопов'язані з такими товарами і надаються разом з ними за договором купівлі-продажу, незалежно від того, здійснюється надання цифрового контенту та/або цифрової послуги продавцем таких товарів чи третьою особою. Цифровий контент та/або цифрова послуга вважаються такими, що надаються у складі товару з цифровими елементами або є взаємопов'язаними з таким товаром, якщо інше прямо не зазначено в договорі купівлі-продажу такого товару, а також якщо товар може використовуватися за цільовим призначенням і без відповідного цифрового |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| | контенту та/або цифрової послуги, за умови укладення споживачем окремого договору про надання такого цифрового контенту та/або цифрової послуги, який не є частиною договору купівлі-продажу товару з цифровими елементами; |
| Ч. 5 Ст. 3. Ця Директива **не застосовується** до контрактів щодо:<br>(a) надання послуг, окрім цифрових послуг, незалежно від того, чи цифрові форми чи засоби використовуються торговцем для отримання результату послуги або для доставки чи передачі її споживачеві;<br><br>(b) послуги електронного зв'язку, як визначено в пункті (4) статті 2 Директиви (ЄС) 2018/1972, за винятком послуг міжособистісного зв'язку, незалежних від номера, як визначено в пункті (7) статті 2 цієї Директиви;<br><br>(c) охорона здоров'я, як визначено в пункті (a) статті 3 Директиви 2011/24/ЄС;<br><br>(d) послуги азартних ігор, а саме послуги, які передбачають ставку з грошовою вартістю в азартних іграх, включаючи такі з елементом навичок, як-от лотереї, ігри в казино, ігри в покер і ставки, за допомогою електронних засобів або будь-якої іншої технології для полегшення спілкування та за індивідуальним бажанням отримувача таких послуг;<br><br>(e) фінансові послуги, як визначено в пункті (b) статті 2 Директиви 2002/65/ЄС;<br><br>(f) програмне забезпечення, що пропонується торговцем за безкоштовною ліцензією з відкритим вихідним кодом, де споживач не платить ціну, а персональні дані, надані споживачем, обробляються виключно продавцем з метою покращення безпеки, сумісності чи взаємодії цього конкретного програмне забезпечення; | Ч. 4 Ст. 1. Дія цього Закону **не поширюється** на регулювання відносин щодо:<br>2) надання послуг, крім цифрових послуг, в яких електронна форма подання інформації використовується виконавцем виключно як засіб передачі результатів надання таких послуг та/або інших даних споживачу;<br><br>3) надання електронних комунікаційних послуг у розумінні Закону України «Про електронні комунікації», крім послуг міжособистісної електронної комунікації без використання нумерації;<br><br>4) надання медичних послуг;<br><br>5) надання фінансових послуг;<br><br>6) надання послуг у сфері азартних ігор за допомогою онлайн-систем та на підставі індивідуального запиту отримувача таких послуг;<br><br>7) передачі виконавцем програмного забезпечення або надання виконавцем доступу до програмного забезпечення на підставі безоплатної публічної ліцензії з відкритим вихідним кодом, якщо персональні дані, надані споживачем, використовуються виконавцем виключно з метою вдосконалення надійності, сумісності та інтероперабельності такого програмного забезпечення;<br><br>8) постачання цифрового контенту необмеженому колу осіб, крім випадків передачі цифрового контенту, який є частиною |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| (g) постачання цифрового контенту, коли цифровий контент стає доступним для широкої громадськості, крім передачі сигналу як частини вистави чи події, наприклад, цифрові кінематографічні проекції;<br><br>(h) цифровий контент, наданий відповідно до Директиви 2003/98/ЕС Європейського Парламенту та Ради (21) органами державного сектору держав-членів. | вистави чи показу певної події, засобами сигнальної трансляції;<br><br>9) надання цифрового контенту суб'єктами владних повноважень, іншими розпорядниками публічної інформації відповідно до Закону України «Про доступ до публічної інформації». |
| Ч. 6. Ст. 3 Без шкоди параграфу 4 цієї статті, якщо єдиний договір між тим самим продавцем і тим самим споживачем включає в пакет елементи постачання цифрового контенту або цифрової послуги та елементи надання інших послуг або товарів, ця Директива застосовується лише до елементів договору, що стосуються цифрового вмісту або цифрової послуги.<br><br>Стаття 19 цієї Директиви не застосовується, якщо пакет у значенні Директиви (ЄС) 2018/1972 включає елементи послуги доступу до Інтернету, як визначено в пункті (2) статті 2 Регламенту (ЄС) 2015/2120 Європейського Союзу. Парламенту та Ради (22) або послугу міжособистісного зв'язку на основі номерів, як визначено в пункті (6) статті 2 Директиви (ЄС) 2018/1972.<br>Без шкоди для частини 2 статті 107 Директиви (ЄС) 2018/1972 наслідки, які припинення дії одного елемента пакетного контракту може мати на інші елементи пакетного контракту, регулюються національним законодавством. | Ч. 6 Ст. 1. У разі якщо договір між виконавцем і споживачем включає елементи постачання цифрового контенту та/або цифрової послуги та елементи надання інших послуг або товарів, дія цього Закону поширюється лише на положення договору, що стосуються цифрового контенту та/або цифрової послуги. |
| Ч. 7. Ст. 3 Якщо будь-яке положення цієї Директиви суперечить положенню іншого акта Союзу, що регулює певний сектор або предмет, положення цього іншого акта Союзу має пріоритет над цією Директивою. | Аналог відсутній. |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| Ч 8. Ст. 3 Закон Союзу про захист персональних даних застосовується до будь-яких персональних даних, що обробляються у зв'язку з контрактами, зазначеними в частині 1.<br>Зокрема, ця Директива не порушує Регламент (ЄС) 2016/679 та Директиву 2002/58/ЄС. У разі суперечності між положеннями цієї Директиви та законодавством Союзу щодо захисту персональних даних, останні мають переважну силу.<br>Ч. 9. Ст. 3 Ця Директива не порушує законодавство Союзу та національне законодавство про авторське право та суміжні права, включаючи Директиву 2001/29/ЄС Європейського Парламенту та Ради (23).<br>Ч. 10. Ст. 3 Ця Директива не впливає на свободу держав-членів регулювати аспекти загального договірного права, такі як правила щодо укладання, дійсності, недійсності або наслідків контрактів, включаючи наслідки припинення контракту, оскільки вони є не регулюється цією Директивою, або право на відшкодування збитків. | |
| Стаття 4. Рівень гармонізації. Держави-члени не повинні зберігати або запроваджувати у своєму національному законодавстві положення, що відрізняються від тих, що викладені в цій Директиві, включаючи **більш або менш суворі** положення для забезпечення різного рівня захисту споживачів, якщо інше не передбачено цією Директивою. | Ч. 5. Ст. 1. Умови договорів про надання цифрового контенту та/або цифрових послуг, які **погіршують** становище споживача порівняно з тим, що передбачено цим Законом, є нікчемними. |
| Стаття 5. Постачання цифрового контенту або цифрових послуг<br>1. Продавець надає цифровий контент або цифрову послугу споживачеві. Якщо сторони не домовилися про інше, продавець надає цифровий контент або цифрову послугу без невиправданої затримки після укладення договору. | Стаття 3. Надання цифрового контенту та/або цифрової послуги<br>1. Виконавець зобов'язується надати споживачу цифровий контент та/або цифрову послугу у розумний строк, без невиправданих зволікань, після укладення договору, якщо інше не встановлено договором. |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| 2. Продавець повинен виконати зобов'язання щодо постачання, якщо:<br>(a) цифровий вміст або будь-які засоби, придатні для доступу чи завантаження цифрового вмісту, надаються або доступні споживачеві або фізичному чи віртуальному об'єкту, обраному споживачем для цієї мети;<br>(б) цифрова послуга стає доступною для споживача або для фізичного чи віртуального об'єкта, обраного споживачем для цієї мети. | 2. Обов'язок виконавця вважається виконаним, якщо:<br>1) цифровий контент чи будь-які засоби, які уможливлюють доступ до цифрового контенту чи його завантаження, стають доступними для споживача безпосередньо або за допомогою фізичного чи віртуального пристосування, обраного споживачем для таких цілей;<br>2) цифрова послуга стає доступною для споживача безпосередньо або за допомогою фізичного чи віртуального пристосування, обраного споживачем для таких цілей. |
| Стаття 6 **Відповідність** цифрового контенту або цифрової послуги<br>Продавець надає споживачеві цифровий контент або цифрову послугу, яка відповідає вимогам, викладеним у статтях 7, 8 і 9, якщо це застосовно, без шкоди для статті 10 (щодо прав треті осіб). | Стаття 4. **Відповідність** цифрового контенту та/або цифрової послуги<br>1. Виконавець надає або зобов'язується надати цифровий контент та/або цифрову послугу, що відповідають вимогам статей 5-7 цього Закону, без шкоди для третіх осіб, права яких визначені статтею 8 цього Закону. |
| Стаття 7. **Суб'єктивні вимоги** до відповідності<br>Для того, щоб відповідати контракту, цифровий контент або цифрова послуга повинні, зокрема, у відповідних випадках:<br>(a) відповідати опису, кількості та якості, а також володіти функціональністю, сумісністю, сумісністю та іншими характеристиками, як того вимагає договір;<br>(b) бути придатним для будь-якої конкретної мети, для якої споживач цього вимагає і про яку споживач повідомив продавця не пізніше, ніж під час укладення договору, і щодо якої торговець дав згоду;<br>(c) постачатися з усіма аксесуарами, інструкціями, включно з установкою, та наданням **допомоги клієнту**, як того вимагає контракт; і<br>(d) оновлюватися, як це передбачено договором. | Стаття 5. **Суб'єктивні критерії** відповідності цифрового контенту та/або цифрової послуги<br>1. Цифровий контент та/або цифрова послуга вважаються такими, що відповідають умовам договору, якщо:<br>1) опис цифрового контенту, його кількість, якість, функціональність, інтероперабельність, сумісність та інші ознаки відповідають умовам укладеного договору;<br>2) надані виконавцем цифровий контент та/або цифрова послуга придатні для використання у визначених споживачем цілях, погоджених сторонами на момент укладення договору;<br>3) споживачу надається цифровий контент та/або цифрова послуга разом з усіма додатками, приналежностями, застосунками та інструкціями, включаючи **рекомендації щодо інсталяції**, згідно з умовами договору; |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| | 4) цифровий контент та/або цифрова послуга надаються у найновішій існуючій версії з подальшим оновленням, якщо інше не передбачено умовами договору. |
| Стаття 8. **Об'єктивні вимоги** до відповідності<br>1. Окрім відповідності будь-яким суб'єктивним вимогам щодо відповідності, цифровий контент або цифрова послуга повинні:<br>(a) бути придатним для цілей, для яких зазвичай використовується цифровий контент або цифрові послуги того самого типу, беручи до уваги, де це застосовно, будь-яке існуюче законодавство Союзу та національне законодавство, технічні стандарти або, за відсутності таких технічних стандартів, застосовні галузеві- спеціальні галузеві кодекси поведінки;<br>(b) мати таку кількість і володіти якостями та характеристиками продуктивності, у тому числі щодо функціональності, сумісності, доступності, безперервності та безпеки, які є звичайними для цифрового вмісту чи цифрових послуг того самого типу та яких споживач може розумно очікувати, враховуючи природу цифровий контент або цифрові послуги та беручи до уваги будь-яку публічну заяву, зроблену трейдером або від його імені, або іншими особами в попередніх ланках ланцюга операцій, зокрема в рекламі чи на маркуванні, якщо трейдер не покаже, що:<br><br>(i) трейдер не був і не міг знати про відповідну публічну заяву;<br><br>(ii) до моменту укладення контракту публічна заява була виправлена таким же чином або у спосіб, який можна порівняти з тим, як вона була зроблена; або | Стаття 6. **Об'єктивні критерії** відповідності цифрового контенту та/або цифрової послуги<br>1. Цифровий контент та/або цифрова послуга, крім суб'єктивних вимог щодо відповідності, повинні також відповідати таким критеріям:<br>1) придатність для використання відповідно до мети, з якою зазвичай використовуються цифровий контент та/або цифрова послуга такого самого виду, з урахуванням технічних вимог, передбачених нормативно-правовими актами та/або нормативними документами;<br><br>2) надання у кількості та відповідність вимогам щодо якості, включаючи інтероперабельність, функціональність, сумісність, доступність, безперервність надання та безпечність використання, які є звичайними для цифрового контенту та/або цифрової послуги такого самого виду та на отримання яких споживач може обґрунтовано розраховувати за умовами договору або виходячи із змісту будь-якої публічної заяви виконавця або інших осіб, які брали участь у ланцюзі надання цифрового контенту та/або цифрової послуги, розміщеної у будь-якій формі, придатній для сприйняття споживачем, у тому числі в рекламі чи на етикетці матеріального носія цифрового контенту, крім випадків, якщо:<br>а) виконавець не знав і за обставин, що склалися, об'єктивно не міг знати про відповідну публічну заяву; або<br>б) цифровий контент та/або цифрова послуга надаються у кількості та якості, що відповідають умовам зміненої публічної заяви, якщо такі зміни були внесені у |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| (iii) публічна заява не могла вплинути на рішення придбати цифровий контент або цифрову послугу;<br><br>(c) у відповідних випадках постачатися разом із будь-якими аксесуарами та інструкціями, які споживач може обґрунтовано очікувати отримати; і<br><br>(d) дотримуватися будь-якої пробної версії або попереднього перегляду цифрового вмісту чи цифрової послуги, наданої трейдером до укладення контракту. | той самий спосіб, у який була розміщена попередня публічна заява;<br>в) публічна заява не могла би вплинути на рішення споживача придбати цифровий контент або замовити цифрову послугу;<br><br>3) надання разом з усіма додатками, приналежностями, застосунками та інструкціями, включаючи рекомендації щодо інсталяції згідно з умовами договору, на отримання яких споживач може обґрунтовано розраховувати;<br><br>4) відповідність демоверсії цифрового контенту та/або цифрової послуги, що надавалася виконавцем споживачу для ознайомлення до моменту укладення договору. |
| 2. Продавець повинен забезпечити, щоб споживач був проінформований і забезпечений оновленнями, включаючи оновлення безпеки, які необхідні для підтримки цифрового контенту або цифрових послуг у відповідності, протягом періоду часу:<br>(a) протягом якого цифровий контент або цифрова послуга мають надаватися згідно з контрактом, якщо контракт передбачає безперервне постачання протягом певного періоду часу; або<br>(b) що споживач може обґрунтовано очікувати, враховуючи тип і призначення цифрового контенту чи цифрової послуги та беручи до уваги обставини та характер договору, якщо договір передбачає один акт постачання або серію окремих актів постачання. | 2. Виконавець зобов'язаний інформувати споживача про необхідність оновлення програмного забезпечення, що підтримує належне функціонування цифрового контенту та/або цифрової послуги, включаючи оновлення програмного забезпечення, спрямованого на захист даних у цифровій формі і збереження відповідності цифрового контенту, що надається, умовам укладеного договору, та забезпечувати надання такого оновлення споживачу:<br>1) за договором, що передбачає безперервне надання цифрового контенту та/або цифрової послуги протягом встановленого строку, - упродовж усього такого строку;<br>2) за договором, що передбачає одноразове чи кількаразове надання цифрового контенту та/або цифрової послуги, - упродовж строку, протягом якого споживач може обґрунтовано розраховувати на їх отримання, зважаючи на тип, мету цифрового контенту та/або цифрової послуги та враховуючи умови договору. |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| Стаття 8. Об'єктивні вимоги до відповідності<br>3. Якщо споживач не інсталює протягом розумного часу оновлення, надані торговцем відповідно до параграфа 2, торговець не несе відповідальності за будь-яку невідповідність, що є наслідком виключно відсутності відповідного оновлення, за умови, що:<br><br>(a) продавець повідомив споживача про наявність оновлення та наслідки невстановлення споживачем;<br><br>(b) збій споживача встановити або неправильне встановлення споживачем оновлення не було спричинено недоліками в інструкціях зі встановлення, наданих торговцем. | Стаття 6 Об'єктивні критерії відповідності<br>[…]<br>3. У разі нездійснення споживачем інсталяції наданих виконавцем оновлень протягом розумного строку виконавець не несе відповідальності за недоліки цифрового контенту та/або цифрової послуги, які виникли в результаті відсутності відповідного оновлення програмного забезпечення, якщо:<br>1) виконавець повідомив споживачу про необхідність оновлення програмного забезпечення та можливі наслідки відсутності такого оновлення;<br>2) відсутність оновлення або некоректне оновлення споживачем програмного забезпечення не є наслідком недоліків інструкцій щодо здійснення такого оновлення, наданих виконавцем. |
| Стаття 8 **Об'єктивні вимоги** до відповідності<br>4. Якщо контракт передбачає безперервне постачання цифрового контенту або цифрової послуги протягом певного періоду часу, цифровий контент або цифрова послуга повинні бути відповідними протягом усього цього періоду.<br><br>5. Не має бути невідповідності у значенні параграфа 1 або 2, якщо під час укладення договору споживач був спеціально проінформований про те, що певна характеристика цифрового контенту або цифрової послуги відхиляється від мети вимогам щодо відповідності, викладеним у пункті 1 або 2, і споживач прямо та окремо погодився з цим відхиленням під час укладення договору. | Стаття 6 **Об'єктивні критерії** відповідності<br>[…]<br>4. Цифровий контент та/або цифрова послуга, що надаються за договором, який передбачає безперервне надання цифрового контенту та/або цифрової послуги протягом встановленого строку, повинні відповідати умовам договору протягом усього такого строку.<br><br>5. Цифровий контент та/або цифрова послуга не вважаються такими, що не відповідають критеріям, передбаченим частинами першою і другою цієї статті, якщо споживачу було повідомлено про відхилення цифрового контенту та/або цифрової послуги від критеріїв щодо відповідності, визначених частиною першою або другою цієї статті, при укладенні договору про надання цифрового контенту та/або цифрової послуги і він прямо і зрозуміло висловив згоду на отримання цифрового контенту та/або цифрової послуги з таким відхиленням. |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| 6. Якщо сторони не домовилися про інше, цифровий контент або цифрова послуга надаються в найновішій версії, доступній на момент укладення договору. | 6. Цифровий контент та/або цифрова послуга надаються у найновішій існуючій версії, якщо інше не передбачено умовами договору. |
| Стаття 7. Інтеграція цифрового контенту та/або цифрової послуги<br>1. Будь-яка невідповідність цифрового контенту та/або цифрової послуги, що виникла внаслідок неправильної інтеграції у цифрове середовище споживача, вважається невідповідністю цифрового контенту та/або цифрової послуги, якщо:<br>1) інтеграція цифрового контенту та/або цифрової послуги здійснювалася виконавцем або особою, яка діяла за його дорученням;<br>2) інтеграція цифрового контенту та/або цифрової послуги здійснювалася споживачем відповідно до наданих виконавцем інструкцій, що містять недоліки. | Стаття 9 Неправильна інтеграція цифрового контенту або цифрової послуги<br>Будь-яка невідповідність, яка є результатом неправильної інтеграції цифрового контенту або цифрової послуги в цифрове середовище споживача, вважається невідповідністю цифрового контенту або цифрової послуги, якщо:<br>(а) цифровий контент або цифрову послугу було інтегровано торговцем або під його відповідальність; або<br>(б) споживач мав намір інтегрувати цифровий контент або цифрову послугу, а неправильна інтеграція сталася через недоліки в інструкціях щодо інтеграції, наданих торговцем. |
| Стаття 10. **Права третіх осіб**<br>Якщо обмеження, спричинене порушенням будь-якого права третьої сторони, зокрема прав інтелектуальної власності, перешкоджає або обмежує використання цифрового контенту чи цифрової послуги відповідно до статей 7 і 8, держави-члени забезпечують, щоб споживач мав право на засоби захисту від невідповідності, передбачені статтею 14, якщо національне законодавство не передбачає недійсності або розірвання контракту на постачання цифрового контенту або цифрової послуги в таких випадках. | Стаття 8. **Права третіх осіб**<br>1. Виконавець гарантує споживачу, що надані ним цифровий контент та/або цифрова послуга не порушують права третіх осіб, у тому числі права інтелектуальної власності.<br>2. Якщо обмеження, що виникає внаслідок порушення будь-якого права третьої особи, зокрема права інтелектуальної власності, унеможливлює або обмежує використання цифрового контенту та/або цифрової послуги відповідно до статей 5, 6 цього Закону, споживач має право на застосування способів захисту, визначених статтею 12 цього Закону. |
| Стаття 11. **Відповідальність торговця**<br>1. Продавець несе відповідальність за будь-яку ненадання цифрового контенту або цифрової послуги відповідно до статті 5. | Стаття 9. **Відповідальність виконавця**<br>1. Виконавець несе відповідальність за будь-яке порушення обов'язку щодо надання цифрового контенту та/або цифрової послуги відповідно до цього Закону. |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| 2. Якщо контракт передбачає один акт постачання або серію окремих актів постачання, продавець несе відповідальність за будь-яку невідповідність відповідно до статей 7, 8 і 9, яка існує на момент постачання, без шкоди для пункту (b) частини 2 статті 8. Якщо, відповідно до національного законодавства, торговець несе відповідальність лише за невідповідність, яка стає очевидною протягом певного періоду часу після постачання, цей період не може бути менше двох років з моменту постачання, без шкоди для пункту (b) Стаття 8(2).<br>Якщо згідно з національним законодавством права, викладені в статті 14, також підлягають або лише підпадають під дію терміну позовної давності, держави-члени повинні забезпечити, щоб такий період позовної давності дозволяв споживачеві скористатися засобами правового захисту, викладеними в статті 14, щодо будь-якої невідповідності, що існує в момент, зазначений у першому абзаці, і стає очевидним протягом періоду часу, зазначеного в другому абзаці. | 2. Якщо договором передбачено разове або кількаразове надання цифрового контенту та/або цифрової послуги, виконавець несе відповідальність за будь-яку невідповідність вимогам, передбаченим статтями 5-7 цього Закону, яка існувала на момент надання цифрового контенту та/або цифрової послуги і була виявлена протягом двох років з моменту надання цифрового контенту та/або цифрової послуги.<br><br>Положення цієї частини не застосовуються у випадках, передбачених пунктом 2 частини другої статті 6 цього Закону. |
| 3. Якщо контракт передбачає безперервне постачання протягом певного періоду часу, торговець несе відповідальність за невідповідність відповідно до статей 7, 8 і 9, яка виникає або стає очевидною протягом періоду часу, протягом якого цифровий вміст або цифрові Послуга надається за договором.<br>Якщо згідно з національним законодавством права, викладені в статті 14, також підлягають або лише підпадають під дію терміну позовної давності, держави-члени повинні забезпечити, щоб такий період позовної давності дозволяв споживачеві скористатися засобами правового захисту, викладеними в статті 14, щодо будь-якої невідповідності, що відбувається або стає очевидним протягом періоду часу, зазначеного в першому абзаці. | 3. Якщо договором передбачено безперервне надання цифрового контенту та/або цифрової послуги упродовж встановленого договором строку, виконавець несе відповідальність за будь-яку невідповідність вимогам статей 5-7 цього Закону, яка існувала та/або була виявлена протягом такого строку. |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| Стаття 12 **Тягар доведення**<br>1. Тягар доведення щодо того, чи цифровий контент або цифрова послуга були надані відповідно до статті 5, покладається на торговця.<br><br>2. У випадках, зазначених у частині 2 статті 11, тягар доведення того, чи наданий цифровий контент або цифрова послуга були відповідними на момент постачання, покладається на продавця щодо невідповідності, яка стає очевидною протягом протягом одного року з моменту надання цифрового контенту або цифрової послуги.<br><br>3. У випадках, зазначених у частині 3 статті 11, тягар доведення стосовно того, чи цифровий контент або цифрова послуга були відповідними протягом періоду часу, протягом якого цифровий контент або цифрова послуга мають бути надані згідно з контрактом покладається на трейдера за невідповідність, яка стає очевидною протягом цього періоду.<br><br>4. Параграфи 2 і 3 не застосовуються, якщо продавець демонструє, що цифрове середовище споживача несумісне з технічними вимогами до цифрового контенту чи цифрової послуги, і якщо продавець поінформував споживача про такі вимоги в чіткій та зрозумілій формі до укладення договору.<br><br>5. Споживач повинен співпрацювати з торговцем, наскільки це можливо та необхідно, щоб з'ясувати, чи причина невідповідності цифрового контенту або цифрової послуги на час, зазначений у статті 11(2) або (3), якщо це застосовно, лежати в цифровому середовищі споживача. Зобов'язання щодо співпраці обмежується технічно доступними засобами, які є найменш нав'язливими для споживача. | Стаття 10. **Тягар доказування**<br>1. Тягар доказування надання цифрового контенту та/або цифрової послуги відповідно до статті 3 цього Закону покладається на виконавця.<br><br>2. У випадках, передбачених частиною другою статті 9 цього Закону, тягар доказування відповідності наданого цифрового контенту та/або цифрової послуги на момент надання покладається на виконавця, якщо невідповідність була виявлена протягом одного року з моменту надання цифрового контенту та/або цифрової послуги.<br><br>3. У випадках, передбачених частиною третьою статті 9 цього Закону, тягар доказування відповідності цифрового контенту та/або цифрової послуги протягом встановленого договором строку надання цифрового контенту та/або цифрової послуги покладається на виконавця, якщо невідповідність була виявлена протягом такого строку.<br><br>4. Положення частин другої, третьої цієї статті не застосовуються, якщо виконавець доведе, що цифрове середовище споживача несумісне з технічними вимогами цифрового контенту та/або цифрової послуги, і чітко та зрозуміло повідомив споживачу про такі вимоги до укладення договору.<br><br>5. Споживач зобов'язаний співпрацювати з виконавцем тією мірою, наскільки це можливо і необхідно для того, щоб з'ясувати, чи є причиною невідповідності цифрового контенту та/або цифрової послуги на момент надання цифрового контенту та/або цифрової послуги, зазначений у частинах другій, третій статті 9 цього Закону, несумісність із цифровим середовищем споживача. |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| Якщо споживач відмовляється співпрацювати та якщо продавець поінформував споживача про таку вимогу в чіткий і зрозумілий спосіб до укладення договору, тягар доведення щодо того, чи існувала невідповідність у час, зазначений у статті 11 (2) або (3), залежно від обставин, належить споживачеві. | Обов'язок співпраці обмежується технічно доступними засобами, які є найменш обтяжливими для споживача. Якщо споживач не виконує обов'язок співпраці, і виконавець чітко і зрозуміло повідомив споживачу про таку вимогу до укладення договору, тягар доказування невідповідності на момент, зазначений у частинах другій, третій статті 9 цього Закону, покладається на споживача. |
| Стаття 13 **Засоби захисту у разі ненадання**<br>1. Якщо торговець не надав цифровий контент або цифрову послугу відповідно до статті 5, споживач повинен звернутися до торговця з проханням надати цифровий контент або цифрову послугу. Якщо потім продавець не надає цифровий контент або цифрову послугу без невиправданої затримки або протягом додаткового періоду часу, чітко погодженого сторонами, споживач має право розірвати договір.<br><br>2. Параграф 1 не застосовується, і споживач має право негайно розірвати договір, якщо:<br>(a) продавець заявив, або це так само зрозуміло з обставин, що продавець не буде надавати цифровий контент або цифрову послугу;<br>(b) споживач і продавець домовилися, або це зрозуміло з обставин укладення договору, що певний час для постачання є важливим для споживача, і продавець не надає цифровий контент або цифрову послугу до або в цей час час.<br><br>3. Якщо споживач розриває договір відповідно до частини 1 або 2 цієї статті, відповідно застосовуються статті 15-18. | Стаття 11. **Правові наслідки ненадання цифрового контенту та/або цифрової послуги**<br>1. У разі ненадання виконавцем цифрового контенту та/або цифрової послуги відповідно до статті 3 цього Закону споживач має право вимагати надання таких цифрового контенту та/або цифрової послуги.<br>У разі ненадання виконавцем цифрового контенту та/або цифрової послуги протягом додатково погодженого сторонами строку, а якщо такий строк не погоджено - протягом розумного строку, споживач має право відмовитися від договору.<br><br>2. Положення частини першої цієї статті не застосовуються, а споживач має право відмовитися від договору негайно, якщо:<br>1) за наявних обставин є очевидним або виконавець заявив про те, що цифровий контент та/або цифрову послугу не буде надано;<br>2) споживач та виконавець домовилися або це випливає з обставин укладення договору, що певний строк надання цифрового контенту та/або цифрової послуги має істотне значення для споживача, а виконавець не надав цифровий контент та/або цифрову послугу протягом такого строку.<br><br>3. У разі відмови споживача від договору відповідно до частин першої, другої цієї статті застосовуються положення статей 13-16 цього Закону. |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| Стаття 14 **Засоби захисту від невідповідності**<br>1. У разі невідповідності споживач має право вимагати приведення цифрового контенту або цифрової послуги у відповідність, отримання пропорційного зниження ціни або розірвання контракту на умовах, викладених у цій статті. | Стаття 12. **Правові наслідки невідповідності цифрового контенту та/або цифрової послуги**<br>1. У разі невідповідності наданих цифрового контенту та/або цифрової послуги вимогам, визначеним статтями 5-7 цього Закону, споживач має право вимагати надання цифрового контенту та/або цифрової послуги, приведених у відповідність, або пропорційного зменшення ціни чи відмовитися від договору. |
| 2. Споживач має право на приведення цифрового контенту або цифрової послуги у відповідність, якщо це не буде неможливим або призведе до непропорційних витрат для продавця, беручи до уваги всі обставини справи, включаючи:<br><br>(a) цінність цифрового контенту чи цифрових послуг, якби не було недоліків у відповідності; і<br>(b) значення невідповідності. | 2. Споживач має право вимагати надання цифрового контенту та/або цифрової послуги, приведених у відповідність, крім випадків, якщо це неможливо або потребує непропорційних витрат виконавця, з урахуванням усіх обставин, включаючи:<br><br>1) вартість цифрового контенту та/або цифрової послуги, якщо вони відповідають вимогам статей 5-8 цього Закону;<br>2) ступінь невідповідності цифрового контенту та/або цифрової послуги. |
| 3. Продавець повинен привести цифровий контент або цифрову послугу у відповідність згідно з параграфом 2 протягом розумного часу з моменту, коли споживач проінформував продавця про невідповідність, безкоштовно та без будь-яких значних незручностей для споживача, беручи до уваги характер цифрового контенту або цифрової послуги та мету, з якою споживачу потрібен цифровий контент або цифрова послуга. | 3. Виконавець зобов'язаний безоплатно привести цифровий контент та/або цифрову послугу у відповідність протягом розумного строку з моменту повідомлення споживачем про невідповідність без будь-яких значних незручностей для споживача, враховуючи характер цифрового контенту та/або цифрової послуги та мету, з якою споживач замовляв цифровий контент та/або цифрову послугу. |
| 4. Споживач має право або на пропорційне зниження ціни відповідно до пункту 5, якщо цифровий контент або цифрова послуга надається в обмін на оплату ціни, або на розірвання договору відповідно до параграфа 6, у будь-якому з наступних випадків: | 4. Виконавець зобов'язаний безоплатно привести цифровий контент та/або цифрову послугу у відповідність протягом строку, погодженого із споживачем, а якщо такий строк не погоджено - протягом розумного строку |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| (a) засіб правового захисту для приведення цифрового контенту або цифрової послуги у відповідність є неможливим або непропорційним відповідно до пункту 2;<br>(b) торговець не привів цифровий контент або цифрову послугу у відповідність до пункту 3;<br>(c) відсутність відповідності з'являється, незважаючи на спробу продавця привести цифровий контент або цифрову послугу у відповідність;<br>(d) невідповідність є настільки серйозною, що виправдовує негайне зниження ціни або розірвання контракту; або<br>(e) продавець заявив, або це зрозуміло з обставин, що продавець не приведе цифровий контент або цифрову послугу у відповідність протягом розумного часу або без значних незручностей для споживача.<br><br>5. Зниження ціни має бути пропорційним до зменшення вартості цифрового контенту або цифрової послуги, яка була надана споживачеві, порівняно з вартістю, яку цифровий контент або цифрова послуга мали б, якби вони відповідали вимогам. | та без будь-яких значних незручностей для споживача, враховуючи характер цифрового контенту та/або цифрової послуги та мету, з якою споживач замовляв цифровий контент та/або цифрову послугу.<br><br>5. У разі якщо договором передбачено платне надання цифрового контенту та/або цифрової послуги, споживач має право вимагати пропорційного зменшення ціни або відмовитися від договору відповідно до частини шостої цієї статті у таких випадках:<br>1) приведення цифрового контенту та/або цифрової послуги у відповідність з умовами договору є неможливим або відповідно до частини другої цієї статті потребує непропорційних витрат виконавця;<br>2) виконавець відповідно до частини третьої цієї статті не привів цифровий контент та/або цифрову послугу у відповідність;<br>3) після приведення виконавцем цифрового контенту та/або цифрової послуги у відповідність невідповідність виявлена повторно;<br>4) невідповідність цифрового контенту та/або цифрової послуги є настільки істотною, що негайне зменшення ціни або відмова від договору є більш виправданими способами захисту за таких обставин;<br>5) за наявних обставин є очевидним або виконавець заявив про те, що цифровий контент та/або цифрова послуга не будуть приведені у відповідність у розумний строк або без істотних незручностей для споживача.<br>6. Зменшення ціни договору повинно бути пропорційним зменшенню вартості цифрового контенту та/або цифрової послуги, що були надані споживачу, порівняно з ціною цифрового контенту та/або цифрової послуги, що відповідають вимогам, передбаченим статтями 5-8 цього Закону. |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| Якщо в контракті передбачено, що цифровий контент або цифрова послуга постачаються протягом певного періоду часу в обмін на оплату ціни, зниження ціни застосовується до періоду часу, протягом якого цифровий контент або цифрова послуга не були доступні відповідність.<br><br>6. Якщо цифровий контент або цифрова послуга надається в обмін на оплату ціни, споживач має право розірвати договір, лише якщо невідповідність є незначною. Тягар доведення того, чи невідповідність є незначною, покладається на торговця. | Якщо договором передбачено платне надання цифрового контенту та/або цифрової послуги упродовж встановленого договором строку, зменшення ціни застосовується до тієї частини зазначеного строку, протягом якої існувала невідповідність цифрового контенту та/або цифрової послуги вимогам, передбаченим статтями 5-8 цього Закону.<br><br>7. Якщо договором передбачено платне надання цифрового контенту та/або цифрової послуги, споживач має право відмовитися від договору, якщо невідповідність цифрового контенту та/або цифрової послуги вимогам, передбаченим статтями 5-8 цього Закону, є істотною. Тягар доказування того, що невідповідність цифрового контенту та/або цифрової послуги не є істотною, покладається на виконавця. |
| Стаття 15 **Здійснення права розірвання**<br>Споживач реалізує право на розірвання договору шляхом звернення до продавця із заявою про рішення розірвати договір. | Стаття 13. **Право споживача на відмову від договору**<br>1. Споживач має право на відмову від договору шляхом повідомлення виконавця про відмову від договору. Повідомлення про відмову від договору може бути подано в електронній (цифровій) формі. У такому разі договір вважається припиненим з моменту отримання виконавцем заяви споживача про відмову від договору. |
| Стаття 16 **Обов'язки торговця у разі припинення**<br>1. У разі розірвання договору продавець відшкодовує споживачеві всі суми, сплачені за договором.<br>Однак у випадках, коли договір передбачає постачання цифрового контенту або цифрової послуги в обмін на оплату ціни та протягом певного періоду часу, і цифровий контент або цифрова послуга відповідали вимогам протягом періоду часу до до розірвання договору продавець відшкодовує споживачеві лише пропорційну частину | Стаття 14. **Правові наслідки відмови від договору для виконавця**<br>1. У разі відмови споживача від договору виконавець зобов'язаний повернути споживачу всі сплачені за договором кошти.<br>Якщо договором передбачено платне надання цифрового контенту та/або цифрової послуги впродовж встановленого договором строку і цифровий контент та/або цифрова послуга відповідали вимогам, передбаченим статтями 5-8 цього Закону, протягом певного періоду, що передував відмові від договору, виконавець |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| сплаченої ціни, що відповідає періоду часу, протягом якого цифровий контент або цифрова послуга не відповідали вимогам, а також будь-яку частину ціни, сплачену споживача заздалегідь за будь-який період дії договору, який залишився б, якби договір не було розірвано. | зобов'язаний повернути споживачу частину сплачених за договором коштів пропорційно до періоду, протягом якого цифровий контент та/або цифрова послуга не відповідали вимогам, визначеним статтями 5-8 цього Закону, а також частину сплачених споживачем наперед коштів за період дії договору, який залишився б, якби споживач не відмовився від договору. |
| 2. Стосовно персональних даних споживача продавець повинен дотримуватися зобов'язань, що застосовуються згідно з Регламентом (ЄС) 2016/679. | 2. При здійсненні обробки персональних даних споживача виконавець зобов'язаний дотримуватися вимог Закону України «Про захист персональних даних». |
| 3. Торговець утримується від використання будь-якого контенту, окрім персональних даних, який надав або створив споживач під час використання цифрового контенту чи цифрової послуги, наданої торговцем, за винятком випадків, коли такий контент:<br>(a) не має жодної користі поза контекстом цифрового вмісту чи цифрових послуг, що надаються торговцем;<br>(b) стосується лише діяльності споживача під час використання цифрового контенту чи цифрових послуг, що надаються торговцем;<br>(c) була об'єднана з іншими даними трейдером і не може бути дезагрегована або лише з непропорційними зусиллями; або<br>(d) було створено спільно споживачем та іншими, і інші споживачі можуть продовжувати використовувати вміст. | 3. Виконавець зобов'язаний утримуватися від використання будь-якого контенту, відмінного від персональних даних, який наданий або створений споживачем у зв'язку з використанням цифрового контенту та/або цифрової послуги, наданих виконавцем, крім випадків, якщо такий контент:<br>1) не має жодної користі без цифрового контенту та/або цифрової послуги, наданих виконавцем;<br>2) пов'язаний виключно з діяльністю споживача під час використання цифрового контенту та/або цифрової послуги, наданих виконавцем;<br>3) об'єднаний виконавцем з іншими даними і не може бути виокремлений або таке виокремлення потребує непропорційних зусиль;<br>4) створений споживачем спільно з іншими споживачами, які мають можливість продовжити використання такого контенту. |
| 4. За винятком ситуацій, зазначених у пунктах (a), (b) або (c) параграфа 3, продавець на вимогу споживача повинен надати споживачеві будь-який вміст, крім персональних даних, який був надається або створюється споживачем під час використання цифрового контенту чи цифрової послуги, наданої торговцем. | 4. Виконавець зобов'язаний на вимогу споживача надати йому будь-який контент, відмінний від персональних даних, який наданий чи створений споживачем при використанні цифрового контенту та/або цифрової послуги, наданих виконавцем, крім випадків, передбачених пунктами 1-3 частини третьої цієї статті. |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| Споживач має право отримати цей цифровий вміст безкоштовно, без перешкод з боку продавця, протягом розумного часу та у загальновживаному та машинозчитуваному форматі.<br><br>5. Продавець може запобігти будь-якому подальшому використанню цифрового контенту або цифрової послуги споживачем, зокрема, зробивши цифровий контент або цифрову послугу недоступною для споживача або вимкнувши обліковий запис користувача споживача, без шкоди для пункту 4. | Споживач має право отримати такий контент безоплатно та безперешкодно протягом розумного строку у загальновживаному та машинозчитуваному форматі.<br><br>5. Виконавець, не порушуючи положень частини четвертої цієї статті, має право унеможливити будь-яке подальше використання споживачем цифрового контенту та/або цифрової послуги, наданих виконавцем, у тому числі зробити такий цифровий контент та/або цифрову послугу недоступними для споживача або відключити обліковий запис споживача. |
| Стаття 17 **Обов'язки споживача у разі розірвання**<br>1. Після припинення дії договору споживач повинен утримуватися від використання цифрового контенту або цифрової послуги та від надання їх третім особам.<br><br>2. Якщо цифровий вміст було надано на матеріальному носії, споживач повинен на вимогу та за рахунок продавця повернути матеріальний носій продавцю без невиправданої затримки. Якщо продавець вирішив вимагати повернення матеріального носія, така вимога повинна бути подана протягом 14 днів з дня, коли продавець був поінформований про рішення споживача розірвати договір.<br><br>3. Споживач не несе відповідальності за будь-яке використання цифрового контенту або цифрової послуги в період до розірвання договору, протягом якого цифровий контент або цифрова послуга не відповідали. | Стаття 15. **Правові наслідки відмови від договору для споживача**<br>1. У разі відмови від договору споживач зобов'язується утримуватися від використання цифрового контенту та/або цифрової послуги, наданих виконавцем, та від надання їх третім особам.<br><br>2. Якщо цифровий контент був наданий на матеріальному носії, споживач зобов'язаний на вимогу та за рахунок виконавця повернути йому матеріальний носій у розумний строк.<br>Вимога про повернення матеріального носія має бути пред'явлена виконавцем протягом 14 днів з дня отримання ним заяви споживача про відмову від договору.<br><br>3. Споживач не зобов'язаний оплачувати будь-яке використання цифрового контенту та/або цифрової послуги у період до відмови від договору, протягом якого цифровий контент та/або цифрова послуга не відповідали вимогам, визначеним статтями 5-8 цього Закону. |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| Стаття 18 **Терміни та способи відшкодування торговцем**<br>1. Будь-яке відшкодування, яке має продавець споживачеві згідно зі статтею 14(4) і (5) або 16(1), у зв'язку зі зниженням ціни або розірванням договору, має бути здійснено без невиправданої затримки та, у будь-якому випадку протягом 14 днів з дати, коли продавця було повідомлено про рішення споживача скористатися правом споживача на зниження ціни або розірвати договір.<br><br>2. Продавець здійснює відшкодування за допомогою тих самих платіжних засобів, які використовував споживач для оплати цифрового контенту або цифрової послуги, якщо споживач прямо не погоджується на інше, і за умови, що споживач не несе жодної комісії в результаті таке відшкодування.<br><br>3. Продавець не стягує зі споживача жодної комісії щодо відшкодування. | Стаття 16. **Строки та способи задоволення вимог споживача**<br>1. Виконавець зобов'язаний задовольнити вимоги споживача щодо пропорційного зменшення ціни або повернення сплачених ним коштів відповідно до частин четвертої, п'ятої статті 12, частини першої статті 14 цього Закону у розумний строк, але не пізніше 14 днів з дня отримання ним такої вимоги або заяви про відмову від договору.<br><br>2. Виконавець зобов'язаний задовольнити вимоги споживача, передбачені частиною першою цієї статті, щодо часткового або повного повернення сплачених ним коштів у тій самій формі, в якій споживач оплатив вартість цифрового контенту та/або цифрової послуги (у тому числі з використанням тих самих платіжних інструментів), якщо домовленістю із споживачем не обумовлено інше, без покладення на споживача обов'язку із сплати будь-якої комісії чи інших аналогічних платежів, пов'язаних із здійсненням розрахунків.<br><br>3. Виконавець не має права вимагати від споживача будь-яку додаткову плату за виконання ним обов'язків, передбачених цією статтею. |
| Стаття 19 **Зміна цифрового контенту або цифрової послуги**<br>1. Якщо в договорі передбачено, що цифровий контент або цифрова послуга надається або стає доступною для споживача протягом певного періоду часу, продавець може модифікувати цифровий контент або цифрову послугу понад те, що необхідно для підтримки цифрового контенту або цифрових обслуговування відповідно до статей 7 і 8, якщо виконуються такі умови: | Стаття 17. **Правові наслідки модифікації цифрового контенту та/або цифрової послуги**<br>1. Якщо договором передбачено надання цифрового контенту та/або цифрової послуги упродовж встановленого договором строку, виконавець має право модифікувати цифровий контент та/або цифрову послугу, навіть якщо така модифікація не є необхідною для забезпечення відповідності цифрового контенту та/або цифрової послуги вимогам цього Закону, якщо виконуються такі умови: |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| (a) договір дозволяє таку зміну та містить поважну причину для такої зміни;<br>(b) така модифікація проводиться без додаткових витрат для споживача;<br>(c) споживач чітко та зрозуміло інформується про модифікацію; і<br>(d) у випадках, зазначених у параграфі 2, споживача достатньо завчасно інформують на тривалому носії про особливості та час зміни та про право розірвати договір відповідно до пункту 2 або про можливість підтримувати цифровий вміст або цифрову послугу без такої зміни відповідно до пункту 4. | 1) договір передбачає можливість та вагому причину для такої модифікації;<br>2) така модифікація проводиться без додаткових витрат споживача;<br>3) споживач поінформований у чіткий і зрозумілий спосіб про таку модифікацію;<br>4) у випадках, передбачених частиною другою цієї статті, споживачу повідомлено завчасно на довговічному носії про особливості і час здійснення модифікації та про право відмовитися від договору відповідно до частини другої цієї статті або про можливість збереження цифрового контенту та/або цифрової послуги без такої модифікації відповідно до частини четвертої цієї статті. |
| 2. Споживач має право розірвати договір, якщо модифікація негативно впливає на доступ споживача до цифрового контенту чи цифрової послуги або на їх використання, за винятком випадків, коли такий негативний вплив є незначним. У цьому випадку споживач має право безкоштовно розірвати договір протягом 30 днів з моменту отримання інформації або моменту, коли цифровий контент або цифрова послуга були змінені торговцем, залежно від того, що настане пізніше. | 2. Споживач має право відмовитися від договору, якщо модифікація негативно впливає на доступ або використання цифрового контенту та/або цифрової послуги споживачем і такий негативний вплив не є незначним. Споживач має право відмовитися від договору без покладення на нього будь-яких пов'язаних з цим платежів протягом 30 днів з дня отримання від виконавця інформації про модифікацію або з дня здійснення виконавцем модифікації цифрового контенту та/або цифрової послуги, залежно від того, яка з цих подій настане пізніше. |
| 3. Якщо споживач розриває договір відповідно до частини 2 цієї статті, відповідно застосовуються статті 15-18. | 3. У разі відмови споживача від договору на підставі частини другої цієї статті застосовуються положення статей 13-16 цього Закону. |
| 4. Параграфи 2 і 3 цієї статті не застосовуються, якщо продавець дозволив споживачеві без додаткових витрат підтримувати цифровий контент або цифрову послугу без модифікації, і цифровий контент або цифрова послуга залишаються відповідними. | 4. Положення частин другої, третьої цієї статті не застосовуються, якщо виконавець дозволив споживачу без додаткових витрат підтримувати цифровий контент та/або цифрову послугу без модифікації, і при цьому цифровий контент та/або цифрова послуга відповідають вимогам статей 5-8 цього Закону. |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| Стаття 20 **Право на відшкодування**<br>Якщо продавець несе відповідальність перед споживачем через будь-яку ненадання цифрового контенту чи цифрової послуги або через відсутність відповідності внаслідок дії чи бездіяльності особи в попередніх ланках ланцюга операцій, продавець повинен бути має право використовувати засоби правового захисту проти особи або осіб, відповідальних у ланцюжку комерційних операцій. Особа, проти якої торговець може вимагати засобів правового захисту, а також відповідні дії та умови здійснення визначаються національним законодавством. | Стаття 18. **Право виконавця на зворотну вимогу**<br>1. У разі якщо ненадання цифрового контенту та/або цифрової послуги або невідповідність цифрового контенту та/або цифрової послуги є наслідком дій чи бездіяльності третіх осіб, виконавець, який задовольнив відповідні вимоги споживача, набуває право на зворотну вимогу (регрес) до таких третіх осіб відповідно до закону. |
| Стаття 21 **Примусове виконання**<br>1. Держави-члени забезпечують наявність відповідних та ефективних засобів для забезпечення дотримання цієї Директиви.<br>2. Засоби, зазначені в параграфі 1, включають положення, згідно з якими один або більше з наступних органів, як визначено національним законодавством, можуть вживати заходів відповідно до національного законодавства до судів або компетентних адміністративних органів для забезпечення того, щоб національні положення, що транспонують це Директиви застосовуються:<br>(a) державні органи або їх представники;<br>(b) організації споживачів, які мають законний інтерес у захисті споживачів;<br>(c) професійні організації, які мають законний інтерес у діяльності;<br>(d) некомерційні органи, організації чи асоціації, що діють у сфері захисту прав і свобод суб'єктів даних, як визначено в статті 80 Регламенту (ЄС) 2016/679. | Стаття 19. **Захист прав споживачів цифрового контенту та цифрових послуг**<br>1. Центральний орган виконавчої влади, що реалізує державну політику у сфері державного нагляду (контролю) за додержанням законодавства про захист прав споживачів, зобов'язаний забезпечувати належний рівень захисту споживачів цифрового контенту та цифрових послуг.<br>Повноваження центрального органу виконавчої влади, що реалізує державну політику у сфері державного нагляду (контролю) за додержанням законодавства про захист прав споживачів, які визначені Законом України «Про захист прав споживачів», поширюються на захист прав споживачів, визначених цим Законом.<br>2. Захист прав споживачів цифрового контенту та цифрових послуг здійснюється відповідно до цього Закону, Закону України «Про захист прав споживачів» та інших законів України.<br>Виконавець зобов'язаний зареєструватися на Єдиному державному веб-порталі для споживачів у сфері електронної комерції (далі - Портал е-покупець) у порядку і строки, визначені законом. |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| Стаття 22. **Обов'язковий характер**<br>1. Якщо інше не передбачено цією Директивою, будь-яка договірна умова, яка на шкоду споживачу виключає застосування національних заходів, що транспонують цю Директиву, відступає від них або змінює їхній вплив до невиконання постачання або невідповідності. доводиться до відома торговця споживачем або до того, як торговець доводить до відома споживача модифікацію цифрового контенту чи цифрової послуги відповідно до статті 19, не є обов'язковим для споживача.<br>2. Ця Директива не перешкоджає торговцю пропонувати споживачеві договірні угоди, які виходять за межі захисту, передбаченого цією Директивою. | Споживач має право здійснювати захист своїх прав, що виникають у зв'язку з отриманням цифрового контенту та/або цифрових послуг, у спосіб та формі, визначені Законом України «Про захист прав споживачів» та іншими законами України, у тому числі шляхом подання скарги до виконавця через Портал е-покупець.<br>3. Центральний орган виконавчої влади, що реалізує державну політику у сфері державного нагляду (контролю) за додержанням законодавства про захист прав споживачів, здійснює державний нагляд (контроль) за додержанням цього Закону у порядку, встановленому Законом України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності», з урахуванням особливостей, визначених цим Законом та Законом України «Про захист прав споживачів».<br><br>Стаття 20. **Відповідальність за порушення прав споживачів, передбачених цим Законом**<br>1. За порушення вимог цього Закону до суб'єктів господарювання застосовуються санкції у вигляді штрафу у разі:<br>1) порушення передбачених цим Законом прав споживачів, пов'язаних з наданням цифрового контенту та/або цифрової послуги, - у десятикратному розмірі вартості цифрового контенту та/або цифрової послуги виходячи з цін, що діяли на час придбання такого цифрового контенту та/або цифрової послуги, але не менше п'яти неоподаткованих мінімумів доходів громадян;<br>2) порушення передбачених цим Законом прав споживачів, пов'язаних з відповідністю цифрового контенту та/або цифрової послуги, - у розмірі 300 відсотків вартості наданих цифрового контенту та/або цифрової послуги з порушенням вимог цього Закону |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| | щодо відповідності цифрового контенту та/або цифрової послуги, але не менше двадцяти п'яти неоподатковуваних мінімумів доходів громадян, а у разі якщо відповідно до закону суб'єкт господарювання не веде обов'язковий облік доходів і витрат або якщо цифровий контент та/або цифрова послуга були надані в обмін на персональні дані споживача - у розмірі п'ятдесяти неоподатковуваних мінімумів доходів громадян.<br>2. Суб'єкт господарювання несе відповідальність за своєчасне та повне погашення нарахованих штрафних санкцій і має право їх оскаржити в адміністративному та/або судовому порядку.<br>3. Суб'єкт господарювання зобов'язаний сплатити суми штрафних санкцій у порядку та строки, визначені Законом України «Про захист прав споживачів».<br>4. Наслідки несплати або неналежної сплати суми штрафів визначаються Законом України «Про захист прав споживачів». |
| Стаття 24. **Транспозиція**<br>1. До 1 липня 2021 року держави-члени повинні ухвалити та опублікувати заходи, необхідні для дотримання цієї Директиви. Вони негайно повідомляють про це Комісію. Вони застосовують ці заходи з 1 січня 2022 року.<br>Коли держави-члени приймають ці заходи, вони повинні містити посилання на цю Директиву або супроводжуватися таким посиланням у разі їх офіційної публікації. Методи такого посилання повинні бути встановлені державами-членами.<br>Держави-члени повідомляють Комісії тексти положень національного законодавства, які вони ухвалюють у сфері, охопленій цією Директивою. | **Прикінцеві положення**<br>1. Цей Закон набирає чинності через шість місяців з дня його опублікування, крім пункту 2 цього розділу, який набирає чинності з дня опублікування цього Закону.<br><br>2. Кабінету Міністрів України:<br>у шестимісячний строк з дня опублікування цього Закону подати Верховній Раді України пропозиції щодо удосконалення механізму застосування адміністративно-господарських санкцій до суб'єктів господарювання за порушення вимог цього Закону та механізму адміністративного оскарження рішень щодо застосування відповідних санкцій;<br>забезпечити введення в дію нормативно-правових актів, що випливають із цього Закону, одночасно із набранням чинності цим Законом. |

| **Директива (ЄС) 2019/770 Європейського Парламенту та Ради від 20 травня 2019 року про певні аспекти контрактів на постачання цифрового контенту та цифрових послуг. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770** | **Про цифровий контент та цифрові послуги: Закон України від 10.08.2023 № 3321-IX. URL: https://zakon.rada.gov.ua/laws/show/3321-20#Text** |
|---|---|
| 2. Положення цієї Директиви застосовуються до постачання цифрового контенту або цифрових послуг, яке відбувається з 1 січня 2022 року, за винятком статей 19 і 20 цієї Директиви, які застосовуються лише до контрактів, укладених з цієї дати.<br><br>Стаття 25. Огляд<br>Комісія повинна не пізніше 12 червня 2024 року переглянути застосування цієї Директиви та подати звіт Європейському Парламенту, Раді та Європейському економічно-соціальному комітету. У звіті розглядається, серед іншого, питання гармонізації правил, застосовних до контрактів на постачання цифрового контенту або цифрових послуг, крім тих, що охоплюються цією Директивою, включно з рекламою.<br><br>Стаття 26 Набрання чинності<br>Ця Директива набуває чинності на двадцятий день після її публікації в Офіційному журналі Європейського Союзу.<br><br>Стаття 27 Адресати<br>Ця Директива адресована державам-членам. | |

*Наукове видання*

# ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ РОЗВИТКУ ТЕХНОЛОГІЙ ЦИФРОВОЇ ЕКОНОМІКИ ТА СУСПІЛЬСТВА

Колективна монографія

*за редакцією О. В. Шаповалової, К. В. Єфремової*

Комп'ютерне макетування *А. Г. Якшиної*

Формат 60×84 $^{1}/_{16}$. Гарнітура Minion.
Обл.-вид. арк. 15,35.
Підписано до друку 13.12.2023.

Адреса редакційної колегії:
НДІ правового забезпечення інноваційного розвитку НАПрН України 61002,
Харків, вул. Чернишевська, 80
Тел.: (057) 700-06-64
E-mail: ndipzir@gmail.com
Сайт: ndipzir.org.ua

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготівників і розповсюджувачів видавничої
продукції – серія ДК № 4814 від 17.12.2014 р.