Державна наукова установа «Інститут інформації, безпеки і права
Національної академії правових наук України»
Науково-дослідний інститут інтелектуальної власності
Національної академії правових наук України

СОЦІАЛЬНА І ЦИФРОВА ТРАНСФОРМАЦІЯ: ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ

МАТЕРІАЛИ
III ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

Київ, 23 листопада 2023 року

Київ
2023

УДК 34:004(477)
С 69

Рекомендовано до друку
вченою радою Державної наукової установи «Інститут інформації,
безпеки і права Національної академії правових наук України»
(протокол № 12 від 28 листопада 2023 р.)

Науковий керівник конференції – ***О. А. Баранов***
Упорядники – ***М. В. Дубняк, С. О. Дорогих***

С 69 Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання : матеріали III Всеукр. наук.-практ. конф. (Київ, 23 листоп. 2023 р.) / наук. керівник конф. О. А. Баранов ; упоряд.: М. В. Дубняк, С. О. Дорогих. – Київ, 2023. – 150 с.
ISBN 978-617-8395-18-6

У збірнику висвітлено матеріали III Всеукраїнської науково-практичної конференції «Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання» – щодо оцінки сучасного стану та розвитку складових правового забезпечення соціальної трансформації внаслідок використання цифрових технологій, проблемних питань правового забезпечення у сфері соціальних комунікацій в умовах цифрової трансформації. Визначено особливості правового забезпечення розвитку сучасної інформаційної інфраструктури суспільства та проблем правового регулювання суспільних відносин у сфері застосування технологій Інтернету речей. Запропоновано напрями вдосконалення законодавства з питань захисту прав людини в умовах використання цифрових технологій.

Конференція відбулася під час військової агресії – війни, яку розв'язала російська федерація проти України. Неподалік той час, коли війна закінчиться і Україна буде відновлюватись та перебудовуватись. Саме тому теоретичні та практичні Рекомендації, які були запропоновані для обговорення в рамках цієї конференції, є актуальними. Результати досліджень можуть бути корисними при визначенні шляхів вдосконалення законодавства задля реформування економіки держави, посилення демократичних процесів, реалізації стратегії цифрової трансформації різних сфер суспільного життя – укріплення судової системи, розвитку сфери культури, надання адміністративних та інших послуг, створення єдиної системи електронних реєстрів, захисту різноманітних прав людини, зокрема права інтелектуальної власності, забезпечення безпеки критичної інфраструктури тощо.

Видання розраховано на фахівців, експертів і вчених в галузі права, студентів, аспірантів і науково-педагогічний склад вищих навчальних закладів та інших зацікавлених осіб.

Матеріали подано в авторській редакції.

УДК 342.53:004(477)

ISBN 978-617-8395-18-6

ЗМІСТ

РЕКОМЕНДАЦІЇ
учасників ІІІ Всеукраїнської науково-практичної конференції «СОЦІАЛЬНА І ЦИФРОВА ТРАНСФОРМАЦІЯ: ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ»

23 листопада 2023 року *Державною науковою установою «Інститут інформації, безпеки і права Національної академії правових наук України»* спільно з *Науково-дослідним інститутом інтелектуальної власності Національної академії правових наук* України проведено ІІІ Всеукраїнську науково-практичну конференцію ***«Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання»***.

В ході конференції розглянуто наступні питання:

- *правове забезпечення соціальної та цифрової трансформації;*
- *вирішення проблеми правового забезпечення інформаційних прав людини в умовах цифрової трансформації;*
- *розвиток законодавства у сфері цифровізації суспільних процесів на основі застосування технологій Інтернету речей, штучного інтелекту, робототехніки, блокчейн, великих даних (big data, соціальних мереж та електронних комунікацій, хмарних технологій тощо;*
- *вдосконалення законодавства щодо захисту прав, інтересів та безпеки людини, суспільства і держави в процесі застосування цифрових технологій.*

В ході активного експертного обговорення вказаних питань учасники науково-практичної конференції ***констатували:***

- світова спільнота пов'язує успіх будь-якої соціальної трансформації з проведенням широкомасштабних цифрових трансформацій на основі активного впровадження та використання досягнень Четвертої промислової революції: технологій Інтернету речей; Індустрії 4.0; штучного інтелекту; робототехніки; блокчейну; великих даних (big data); розумних контрактів; соціальних мереж та електронних комунікацій; хмарних та нано-, біотехнологій тощо;
- більшість держав світу прийняли або розглядають можливість прийняття національних стратегій впровадження технологій Інтернету речей; одночасно, близько 70 держав – національних стратегій розвитку штучного інтелекту та робототехніки, вважаючи це базовою умовою розвитку;
- масштабні соціальні та цифрові трансформації, які необхідно буде реалізовувати в процесі виходу людства з кризи та досягнення ці-

лей сталого розвитку, можуть бути успішним за умови гармонізованого оновлення комплексу галузей права та істотного перегляду всієї системи права;

– для усунення правової сингулярності необхідно на основі соціально-правових моделей майбутнього суспільства організовувати комплексні дослідження щодо пошуку, ідентифікації та локалізації правових проблем, які з великою ймовірністю матимуть місце в процесі проведення масштабних соціальних та цифрових трансформацій;
– Україна як демократична держава, що має власну систему соціальних цінностей, які більшою мірою співпадають з цінностями держав Європейського Союзу, США та інших демократичних країн світу, має розвиватись на основі консенсусної Національної стратегії розбудови нової, модерної країни;
– актуальним є питання організації належного правового забезпечення соціальної та цифрової трансформації суспільства, а також покладання завдання щодо розробки концептуальних засад розвитку законодавства на профільні наукові установи НАН України і НАПрН України та Дослідницьку службу Верховної Ради України.

Розглянувши зазначені та інші актуальні проблемні питання учасники ІІІ Всеукраїнської науково-практичної конференції ***рекомендували:***

1. Запропонувати Верховній Раді України розглянути та прийняти за поданням Кабінету Міністрів України Національну програму правового забезпечення соціальної та цифрової трансформації в процесі реалізації стратегії розбудови нової, модерної держави – України.

2. Запропонувати Кабінету Міністрів України розробити та подати на затвердження Верховній Раді України Національну програму правового забезпечення соціальної та цифрової трансформації в процесі реалізації стратегії розбудови нової, модерної держави – України, *передбачивши*:

– формування теоретико-методологічних засад створення нових (удосконалених) соціально-правових моделей у різних сферах життєдіяльності, зокрема, у сфері публічного управління, правосуддя, національної безпеки та оборони, в економічній, енергетичній, інформаційній сферах, у сфері охорони здоров'я, освіти і науки, культури тощо;
– розгляд питань щодо зміни інституційної структури і функцій загальнодержавних та місцевих систем публічного управління й регулювання, систем галузевого саморегулювання та інститутів громадянського суспільства;

– розробку філософських і теоретико-правових основ формування та розвитку суспільних відносин в умовах цифрової трансформації; теорії, методології і напрямів правового забезпечення цифрової трансформації у різних сферах життєдіяльності людини, суспільства, держави та міжнародної спільноти, з урахуванням застосування технологій штучного інтелекту;
– створення теоретико-методологічних і правових засад щодо визначення понять, критеріїв, змісту та обсягів правоздатності (дієздатності, деліктоздатності) штучного інтелекту і робототехніки, а також опрацювання проблем визначення їх спеціальної або загальної правосуб'єктності та юридичної відповідальності у цій сфері;
– визначення напрямів розвитку національного законодавства з питань регулювання ринку технологій Інтернету речей, штучного інтелекту, робототехніки, електронних комунікацій, користування радіочастотним ресурсом, криптовалют, технологій блокчейн, «хмарних» технологій, «великих даних» тощо;
– вдосконалення й оновлення законодавства в частині податків та митних зборів, монопольної діяльності, лібералізації та конкуренції для регульованих ринків цифрових технологій; захисту прав споживачів; обігу неперсоніфікованих та персональних даних; визначення юридичної відповідальності; забезпечення конфіденційності, інформаційної безпеки та кібербезпеки; захисту інтелектуальної власності та авторського права тощо, з урахуванням розвитку транскордонного співробітництва;
– розробку системи правового забезпечення функціонування опорних кластерів розвитку цифрової трансформації у промисловості (Індустрія 4.0), в банківський сфері, енергетиці, транспорті, державному управлінні, ретейлі, у сільському господарстві, «розумному» містобудуванні, у системі охорони здоров'я, науці та освіті тощо;
– формування теоретико-правових основ захисту прав та безпеки людини, законних інтересів суспільства і держави, забезпечення інформаційної безпеки та кібербезпеки в умовах застосування штучного інтелекту, робототехніки, хмарних технологій та технологій блокчейну, соціальних мереж, а також визначення юридичної відповідальності за правопорушення у цій сфері;
– гармонізацію та імплементацію норм правових актів Європейського Союзу та міжнародного права в законодавство України відповідно до її зобов'язань, правових засад міжнародного співробітництва у сфері цифрового майбутнього;

– розробку комплексу правових (публічно-правових, приватно-правових) засобів, попередження та зменшення можливих негативних наслідків і ризиків цифровізації (зростання кількості зловживань цифровими технологіями, випадків їх недбалого, непродуманого, легковажного або відверто антисуспільного використання тощо).

3. Запропонувати Верховній Раді України, Кабінету Міністрів України та іншим державним органам, органам місцевої влади та місцевого самоврядування, інститутам громадянського суспільства забезпечити публічний розгляд та розробку пропозицій щодо створення всеосяжної системи стимулів, мотивації та заохочень для усіх учасників процесу цифрової трансформації з метою забезпечення ефективності проведення необхідних реформ та вирішення соціальних проблем.

ПЛЕНАРНЕ ЗАСІДАННЯ

Баранов О. А.
доктор юридичних наук, професор, керівник Наукового центру цифрової трансформації та права Державної наукової установи «Інститут інформації, безпеки і права НАПрН України».

РОЛЬ ЦИФРОВИХ ТЕХНОЛОГІЙ У РОЗВИТКУ ЦИВІЛІЗАЦІЇ[1]

На стику тисячоліть сформувалася низка надзвичайно небезпечних цивілізаційних викликів: виснаження планетарних ресурсів, таких як: чисте повітря, вуглеводні, корисні копалини, ліси, прісна вода, родючі землі; зниження стійкості екосистеми людства; перенасичення: міст, інфраструктур, виробництв, автомобілів тощо; глобальна нестача продовольства; погіршення екології та зміна клімату; надзвичайно високі темпи соціальних процесів; низька ймовірність достовірності прогнозування природних, соціальних, політичних, економічних, технічних та технологічних процесів та явищ тощо.

Пошуку виходу з критичного стану людської цивілізації було присвячено Генеральну асамблею ООН, яка у 2015 році ухвалила Резолюцію "Перетворення нашого світу: Порядок денний у сфері сталого розвитку на період до 2030 року" [1]. Генеральний секретар ООН у своїй узагальнюючій доповіді щодо порядку денного в якості причин, що призвели до критичного стану людства, визначає такі [2]: недостатність обсягу інформації для прийняття рішень; нерішучість і відсутність сміливості у вищого керівництва держав при формуванні політики змін у суспільстві та змін в управлінні економікою; необґрунтованість стратегічних рішень; відсутність цілісних та комплексних підходів щодо вирішення масштабних проблем розвитку.

Однією із системних, базових причин деградації планети та людської цивілізації слід визнати загальну ситуацію у світі з вкрай низькою якістю прийнятих рішень. Що більша складність рішень, то більше вони не відповідають критерію оптимальності. В переважній більшості випадків

[1] Тези підготовлено в межах фундаментальної теми «Правове забезпечення застосування цифрових технологій в умовах трансформації суспільства» (номер державної реєстрації 0119U003166).

рішення тривіально не є релевантними поставленим цілям та реальному стану соціальних процесів та навіть обставинам, у яких вони приймалися. Певна частка визначених стратегічних цілей як результат прийнятих рішень не відповідають ні поточному стану існування цивілізації, ні його очікуваному (бажаному) майбутньому стану, що також слід зарахувати до базової причини деградації планети та людської цивілізації.

Задля протидії цивілізаційним викликам останні десятиліття набирають обертів процеси цифрової трансформації, як процеси впровадження різноманітних цифрових технологій. З ускладненням та масштабуванням процес впровадження цифрових технологій історично послідовно мав такі назви: автоматизація, комп'ютеризація, інформатизація, розвиток інформаційного суспільства, цифровізація та цифрова трансформація. Але сьогодні ще не вирішена проблема недосконалого усвідомлення на рівні всього людства, окремих держав, суспільств, галузей економіки, бізнесів та окремих людей стратегічного значення організації одночасного, повсюдного, синхронізованого та змістовно зрозумілого процесу цифрової трансформації. Отже, обґрунтування та усвідомлення ролі та системного значення цифрової трансформації для розвитку цивілізації є актуальним завданням.

Історичний розвиток людства призводить до майже експоненціального збільшення обсягу інформаційних відносин, що особливо наочно проявилося в останні півтора-два століття у вигляді: безперервної інтенсифікації інформаційних процесів у суспільстві; щорічного збільшення обсягів нової інформації; неухильного зростання обсягів та швидкості передачі інформації; збільшення джерел, потоків і видів інформації, що циркулює в суспільстві; ускладнення структури та змісту інформації, інформаційних потоків та процесів тощо.

Отже, інформація, інформаційні відносини та інформаційна взаємодія завжди були, є і будуть надзвичайно важливими та необхідними для реалізації всіх соціальних процесів, здійснення всіх видів та типів людської діяльності. Саме тому стан та розвиток інформаційного права є основою забезпечення високої якості інформаційної взаємодії в процесі реалізації суспільних відносин, що є базовою умовою здійснення ефективної діяльності в будь-яких сферах та сегментах соціальної активності.

Проте, вже з середини дев'ятнадцятого століття людство стало явно усвідомлювати збільшення труднощів у сфері інформаційної взаємодії. Ці проблеми надзвичайно загострилися в останні 60-70 років в наслідок посилення багатозв'язності та взаємозумовленості сучасного світу, що значно ускладнило прийняття рішень, оскільки: а) стало необхідно мати великі обсяги своєчасної, актуальної, повної та достовірної інформації:

про соціальний процес та його параметри, про суб'єктів та об'єкти, про навколишній світ, про суспільні відносини у конкретних сферах людської діяльності, що мають відношення до цього процесу; б) дедалі частіше стало потрібно приймати рішення в режимі обмеженості ліміту часу або навіть у режимі реального часу через велику швидкоплинність та високу динаміку змін різних соціальних і природних процесів.

Але подолати проблеми інформаційної взаємодії ставало все важче, а, іноді, й неможливо через: сумнозвісні природні обмеження когнітивних можливостей людини, обмеження в одночасній обробці змінних у робочій (оперативній) пам'яті людини, обмежений час зберігання в короткочасній зоровій пам'яті, невеликий ліміт часу на зберігання інформації у пам'яті людини, незначну швидкість когнітивних процесів, обмежену здатність людини сприймати, утримувати в пам'яті та подумки обробляти інформацію.

Історично когнітивні обмеження людства можна визначити через три цивілізаційних когнітивних протиріччя, які на певному етапі розвитку людства суттєво негативно впливали на якість рішень [3].

Рішення *– це інтегральний результат людської діяльності, насамперед функціонування інтелекту, як системи когнітивних функцій людини, метою якої є вибір найкращого варіанта поведінки або дій для конкретної сукупності параметрів змінних стану внутрішнього та навколишнього середовища.* При цьому, не викликає сумніву те, що надзвичайно важливою умовою прийняття якісних рішень є забезпечення використання інформації, яка б відповідала певним вимогам до таких показників її якості як *актуальність, своєчасність, повнота та достовірність.*

Сьогодення характеризується незліченною кількістю помилок у прийнятті рішень тотально у всіх сферах людської діяльності на всіх соціальних рівнях. В результаті спостерігаємо величезну купу з року в рік нагромаджуваних одне на одне політичних, управлінських, соціальних, особистих, технологічних та технічних помилкових рішень. Саме помилкові рішення стають справжньою причиною різноманітних локальних та глобальних криз, частота появи яких зростає тому, що відбувається стрімке скорочення періоду впевненого прогнозування та планування соціальної діяльності, різке зменшення можливостей довготривалого, інноваційного інвестування тощо.

Людство, як це відбувалося раніше, на появу цивілізаційних викликів, зокрема проявів негативного впливу трьох цивілізаційних когнітивних протирічь на якість прийняття різноманітних рішень будь-якого суспільного статусу та рівня, відповіло впровадженням та використанням досягнень Четвертої промислової революції. До основних здобут-

ків Четвертої промислової революції відносять: комп'ютери та цифрові технології, такі як: технологій Інтернету речей; Індустрії 4.0; штучного інтелекту; робототехніки; блокчейну; великих даних (big data); розумних контрактів; соціальних мереж та електронних комунікацій; хмарних технологій тощо.

Висновки.

Джерелом сучасного повсюдного та тотального прийняття помилкових рішень є наявність першого, другого та третього цивілізаційних когнітивних протиріч, існування яких природно обумовлено обмеженнями можливостей інтелекту людини як системи когнітивних функцій.

Системна цифрова трансформація створює умови для прийняття ефективних рішень в будь-який сфері соціальної активності завдяки нівелюванню загрозливого впливу на розвиток цивілізації природних обмежень когнітивних можливостей людини.

Отже, роль сучасних цифрових технологій полягає у забезпеченні досягнення цілей сталого людства та порятунку цивілізації завдяки створенню сприятливих умов для прийняття максимально ефективних рішень в будь-який сфері соціальної активності.

Використана література

1. UN General Assembly. Transforming our world: the 2030 Agenda for Sustainable Development. Resolution adopted by the General Assembly on 25 September 2015, A/RES/70/1.URL: https://sdgs.un.org/2030agenda.

2. UN Secretary-General. The Road to Dignity by 2030: Ending Poverty, Transforming All Lives and Protecting the Planet Synthesis. URL: https://digitallibrary.un.org/record/785641.

3. Баранов О. А. Трансформація: соціальна & цифрова & правова : монографія у 3-х т. Т. 1. Порятунок цивілізації: економіка результату. Одеса : Видавничий дім «Гельветика». 2022. 272 с.

Карчевський М. В.
доктор юридичних наук, професор, професор кафедри кримінального права і кримінології Львівського державного університету внутрішніх справ, головний науковий співробітник відділу дослідження проблем кримінального права Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України

ЯК І ЧОМУ ЗМІНЮЄТЬСЯ ЮРИДИЧНИЙ ДИСКУРС ЩОДО ШТУЧНОГО ІНТЕЛЕКТУ[1]

Як змінилася юридична дискусія щодо штучного інтелекту. Предметом залишилося питання соціалізації штучного інтелекту, поміщення технологій у соціальний контекст, мінімізація негативних наслідків їх використання та забезпечення максимально можливих переваг. Водночас, зміст обговорюваних проблем змінився від доцільності заборони чи регулювання та визнання штучного інтелекту суб'єктом права до класифікації сфер використання штучного інтелекту, визначення та оцінки ризиків використання, формулювання юридичних запобіжників цих ризиків.

Чому так змінився юридичний дискурс. Відповідь полягає у значному розширенні сфери фактичного застосування технологій штучного інтелекту. За останні двадцять років штучний інтелект пройшов шлях від наукової абстракції та концептуальних моделей до практичних задач та повсякденного використання. Системи штучного інтелекту використовуються практично в усіх сферах діяльності людини.

Початок юридичних рефлексій щодо штучного інтелекту нами був досліджений раніше [8]. Відправною позицією сучасного юридичного дискурсу щодо штучного інтелекту є поділ технологій на «сильний» та «слабкий» штучний інтелект. Сильний являє собою гіпотетичний пристрій, який має здатність мислити, усвідомлювати оточуючий світ та себе як особистість, виконувати всі завдання, як і людина, або навіть перевищувати її інтелектуальні здібності. Слабкий штучний інтелект – фактично існуючі технології, орієнтовані на автоматизацію певних видів

[1] Тези підготовлено в межах фундаментальної теми «Теоретичні, законодавчі та правозастосовні проблеми кримінально-правової охорони інформаційної безпеки в Україні» (номер державної реєстрації 0121U114324).

діяльності людини або кількох завдань, які виконує людина. Наприклад, керування транспортним засобом, гра в шахи, розпізнавання обличчя, голосу, рукописного тексту тощо.

Експерти визначають чотири загальні групи ризиків [1] використання технологій, що фактично існують, «слабкого» штучного інтелекту.

Нова якість порушення таємниці приватного життя. Автоматизована обробка даних про людину створює новий рівень загроз для людини. Аналіз уподобань у соціальних мережах [3], історії покупок [4], інтернет з'єднань [5] з використанням технологій штучного інтелекту здатен більш ніж істотно порушити таємницю приватного життя конкретної людини.

Маніпулювання поведінкою. Технології «слабкого» штучного інтелекту вже сьогодні чинять істотний вплив на поведінку споживачів шляхом таргетованої реклами, індивідуалізованих рекомендацій пошукових сервісів, персоналізованих стрічок новин тощо. Значною є небезпека маніпуляцій з використанням штучного інтелекту у політичній діяльності [6; 7]. Існує навіть спеціальний термін – «астротурфінг» , яким позначають імітацію громадської підтримки ініціатив[1].

Дискримінація. Через особливості машинного навчання, технології яка лежить в основі «слабкого» штучного інтелекту, недостатня якість даних, використаних в процесі розробки системи може призвести до системних порушень її функціонування. Прикладом означеної проблеми може слугувати упередженість автоматизованих систем відбору персоналу. «Навчальний» набір даних для таких систем як правило представляє собою відомості щодо успішних рішень з підбору персоналу. Оскільки цей процес у багатьох сферах не є гендернонейтральним, мали місце випадки уведення в експлуатацію систем, які помножували гендрену нерівність під час функціонування [2].

Непрозорість. Правові гарантії інтелектуальної власності та конкурентна боротьба на ринку інформаційних технологій зумовлюють закритість алгоритмів систем штучного інтелекту, що унеможливлює перевірку правильності рішень та ефективний контроль за їх станом. У тих сферах де неправильна робота систем штучного інтелекту здатна заподіяти значну шкоду, така ситуація створює небезпеку.

Накопичений досвід та «критична» маса загроз неконтрольованого розширення сфери застосування систем штучного інтелекту зумовили появу законодавчих ініціатив, спрямованих на створення комплексної нормативно-правової бази для забезпечення відповідального розвитку штучного інтелекту, захисту основних прав і сприяння інноваціям. В якості найбільш актуальних слід відзначити розпочаті урядом США 13

квітня 2023 року громадські обговорення щодо «політики підзвітного штучного інтелекту»[9], а також обговорення проєкту, презентованого Європейською Комісією у квітні 2021 під назвою «The proposal for a regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act, AIA) and Amending Certain Union Legislative Acts»[10].

AIA використовує поняття «система штучного інтелекту» (ШІ) та визначає його наступним чином: програмне забезпечення, яке

а) розроблене з використанням одного або кількох підходів, що відносяться до:

- методів машинного навчання, включаючи контрольоване, неконтрольоване та навчання з підкріпленням, з використанням різноманітних методів, у тому числі глибокого навчання;
- методів, що ґрунтуються на логіці та знаннях, включаючи представлення знань, індуктивне (логічне) програмування, бази знань, логічні та дедуктивні механізми, (символічні) міркування та експертні системи;
- статистичних методів, включаючи байєсовську оцінку, методи пошуку та оптимізації;

б) може, для заданого набору визначених людиною цілей, генерувати результати, такі як контент, прогнози, рекомендації, або рішення, що впливають на середовище, з яким вони взаємодіють.

Визначення з усією очевидністю свідчить про фокус європейських законодавців на суто практичних питаннях використання продуктів, які вже існують або можуть бути створені.

У AIA програми штучного інтелекту класифікуються на основі потенційних рівнів ризику. Категорія «неприйнятний ризик штучного інтелекту» забороняє розробку та використання певних програм штучного інтелекту, наприклад систем соціального скорингу. До «штучного інтелекту високого ризику» віднесено системи, які можуть поставити під загрозу безпеку людей або порушити їхні основні права.

Авторами AIA реалізовано ідею нормативної мінімізації вказаних раніше соціальних ризиків впровадження ШІ. Порушення приватності пропонується контролювати у спосіб класифікованих за рівнем ризику вимог щодо розробки, введення в експлуатацію та використання систем ШІ.

Небезпеки впливу на поведінку людини, мінімізуються шляхом заборони окремих видів ШІ, які пропонується відносити до «Prohibited Artificial Intelligence Practices» (Article 5, AIA). Такі системи характеризуються «неприйнятним ризиком» та поділяються на 4 категорії: дві з

них стосуються когнітивного поведінкового маніпулювання людьми або певними вразливими групами; інші 2 заборонені категорії це системи соціального скорингу та системи біометричної ідентифікації в режимі реального часу та на відстані. Однак для кожної категорії є винятки з основного правила [11].

Непрозорість пропонується долати шляхом обов'язкового документування створення, використання та вдосконалення високоризикованих систем ШІ, постійної актуалізації технічної документації таких систем, наявністю обов'язку виробника надавати контролюючим органам вичерпну інформацію щодо поточного стану системи ШІ, які віднесено до високоризикованих.

Нарешті, мінімізація упередженості забезпечується шляхом контролю за змістом та репрезентативністю навчальних, валідаційних та тестових наборів даних.

Важливими є положення AIA щодо підтримки досліджень та інновації в області ШІ. Зокрема, пропонується механізм «регуляторних пісочниць» (regulatory sandboxes), регуляторних інструментів, які дозволяють підприємствам тестувати та експериментувати з новими та інноваційними продуктами чи послугами під наглядом регулятора протягом обмеженого періоду часу. Регуляторні пісочниці виконують подвійну роль: 1) вони сприяють бізнес-навчанню, тобто розробці та тестуванню інновацій у реальному середовищі; та 2) підтримка регуляторного навчання, тобто формулювання експериментальних правових режимів для керівництва та підтримки бізнесу в їх інноваційній діяльності під наглядом регуляторного органу. На практиці підхід спрямований на те, щоб уможливити експериментальні інновації в рамках контрольованих ризиків і нагляду, а також покращити розуміння регуляторами нових технологій[12].

Законопроєкт отримав переважно схвальні відгуки науковців, водночас були представлені й критичні позиції. Наприклад, на думку М. Веле та Ф. Зуйдервена Боргесіуса, AIA "зібраний із законодавства про безпеку продукції 1980-х років, захисту основних прав, нагляду та захисту споживачів", такий підхід не дозволяє розглядати законопроєкт як всеосяжний та позбавлений істотних пробілів. Наприклад, положення про прозорість або мало додають до чинного законодавства, або викликають більше запитань, ніж відповідей, коли розглядаються їхні наслідки [13]. Новий виток дискусії зумовлений появою ChatGPT. Виникло питання, чи може генеративний штучний інтелект загального призначення бути використаним для заподіяння шкоди, чи може він стати частиною злочинного використання ШІ та, відповідно, чи не підлягатиме він забороні як один з видів «Prohibited Artificial Intelligence Practices»[14] Дискусія триває.

В ситуації, що склалася важливо відзначити, що Україна не перебуває осторонь процесів розширення сфери використання штучного інтелекту. Збройна агресія рф прискорила практичне впровадження технологій штучного інтелекту в роботу національних правоохоронних органів. Розслідування воєнних злочинів, діяльності колаборантів, пропаганди на користь агресора вимагають оперативного опрацювання значних масивів даних. Правоохоронці активно використовують системи розпізнавання обличчя, відеоаналітику, транскрибування відео та аудіозаписів. І це лише один з напрямів використання штучного інтелекту в Україні. Тому існує очевидна потреба правового регулювання використання систем ШІ в Україні. Чинна система норм видається недостатньою[15]. Бажано щоб український закон про використання систем штучного інтелекту містив такі положення:

- визначення, побудоване на основі європейського підходу, яке б чітко обмежило сферу нормативного впливу, структурувало національний юридичний та технічний дискурс;
- класифікація сфер використання штучного інтелекту за небезпекою можливих ризиків;
- залежний від цієї класифікації розподіл вимог до використання систем ШІ;
- можливість як створювати системи ШІ, орієнтовані на конкретні сфери застосування, так і проводити локалізацію систем ШІ загального призначення;
- обов'язкова диверсифікація систем ШІ, сфери використання яких характеризуються найбільшим ризиком;
- гнучкий механізм підтвердження відповідності системи ШІ вимогам, що пред'являються до її використання у певній сфері, такий підхід стимулюватиме розроблення нових технічних рішень та забезпечуватиме необхідну динаміку використовуваних технологій;
- можливість періоду експериментального правового регулювання систем ШІ, протягом такого періоду контролюючі органи зобов'язуються надати пропозиції розробникам щодо проходження процедури відповідності (regulatory sandboxes);
- правові засоби лібералізації інвестиційної діяльності в сфері використання систем ШІ.

Список використаних джерел:

1. Dupont B., Stevens Y., Westermann H., Joyce M. Artificial Intelligence in the Context of Crime and Criminal Justice , Korean Institute of Criminology, Canada Research Chair in Cybersecurity, ICCC, Université de Montréal,

(2018). URL : https://www.cicc-iccc.org/public/media/files/prod/publication_files/Artificial-Intelligence-in-the-Context-of-Crime-and-Criminal-Justice_KICICCC_2019.pdf

2. Examples of Biased Artificial Intelligence // Logically. 30.07. 2019. URL : https://www.logically.ai/articles/5-examples-of-biased-ai

3. Michal Kosinski, David Stillwell & Thore Graepel, “Private traits and attributes are predictable from digital records of human behavior” (2013) 110:15 Proceedings of the National Academy of Sciences 5802.

4. Kashmir Hill, “How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did”, Forbes (16 February 2012), online: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

5. Zalnieriute, Monika, Big Brother Watch and Others v. the United Kingdom (July 14, 2022). American Journal of International Law, 2022, Vol 116(3), pp. 585-592., Available at SSRN: https://ssrn.com/abstract=4162965

6. Yuval Noah Harari argues that AI has hacked the operating system of human civilisation. – The Economist. 6.05.2023. – URL: https://www.economist.com/by-invitation/2023/04/28/yuval-noah-harari-argues-that-ai-has-hacked-the-operating-system-of-human-civilisation

7. Guggenberger N., Salib P. From Fake News to Fake Views: New Challenges Posed by ChatGPT-Like AI. – The Lawfare Institute. 20.01.2023. – URL: https://www.lawfaremedia.org/article/fake-news-fake-views-new-challenges-posed-chatgpt-ai

8. Karchevskyi, M., Losych, S., & Germanov, S. (2023). Socialization of artificial intelligence and transhumanism: legal and economic aspects. Baltic Journal of Economic Studies, 9(1), 61-70. https://doi.org/10.30525/2256-0742/2023-9-1-61-70

9. AI Accountability Policy Request for Comment. A Notice by the National Telecommunications and Information Administration on 13.04.2023 // Federal Register. https://www.federalregister.gov/documents/2023/04/13/2023-07776/ai-accountability-policy-request-for-comment

10. European Commission. Proposal For a Regulation of The European Parliament and of The Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final, 2021/0106(COD), 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

11. Kop M. EU Artificial Intelligence Act: The European Approach to AI // Stanford – Vienna Transatlantic Technology Law Forum, Transatlantic Antitrust and IPR Developments, Stanford University, Issue No. 2/2021. –

URL: https://law.stanford.edu/publications/euartificial-intelligence-act-the-european-approach-to-ai/

12. Madiega T., Van De Po A. L. Artificial intelligence act and regulatory sandboxes. – European Parliamentary Research Service. PE 733.544 – June 2022. – URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733544/EPRS_BRI(2022)733544_EN.pdf

13. Veale M. Zuiderveen Borgesius F. Demystifying the Draft EU Artificial Intelligence Act // Computer Law Review International. – 2021 (4). https://doi.org/10.9785/cri-2021-220402

14. Карчевський М. В. Правове регулювання штучного інтелекту: ризик-орієнтований підхід у європейській дискусії / Карчевський М. В., Штанько В. А., ChatGPT // Актуальні питання права та соціально-економічних відносин : зб. ст. – Кропивницький, 2023. – С.20–29. – Режим доступу: http://dspace.wunu.edu.ua/bitstream/316497/48146/1/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA-2023%20%281%29.pdf#page=20 . – Назва з екрана. – Дата перегляду: 23 серп. 2023 р.

15. Karchevskyi M., Radutniy O. Ukrainian Report on Traditional Criminal Law Categories and AI (Artificial Intelligence) / Traditional Criminal Law Categories and AI: Crisis or Palingenesis? (International Colloquium Section I, Siracusa, 15-16 September 2022) Edited by Lorenzo Picotti, Beatrice Panattoni. RIDP, Vol. 94 issue 1, 2023. – 385 p. – pp. 363 – 383

Андрощук Г. О.
кандидат економічних наук, доцент, головний науковий співробітник НДІ інтелектуальної власності НАПрН України

«ДЕКЛАРАЦІЯ БЛЕТЧЛІ» З БЕЗПЕКИ ВИКОРИСТАННЯ ШІ: АНАЛІЗ ОСНОВНИХ ПОЛОЖЕНЬ

У 1950 році талановитий британський математик і криптограф Алан Тюрінг опублікував в журналі «Mind» академічну статтю «Обчислювальні машини й розум» (Computing Machinery and Intelligence), метою якої була відповідь на запитання «Чи можуть машини мислити?». Для відповіді знадобилося майже 12 000 слів. Проте закінчення статті лаконічне: «Ми можемо бачити лише обмежене майбутнє, проте і так ми можемо побачити, як багато всього ще треба зробити». Через сім десятиліть ця теза стала ілюстрацією для саміту з безпеки штучного інтелекту (ШІ) (AI

Safety Summit), який зібрав у Великобританії провідних політиків, дослідників і технічних лідерів. Учасниками заходу стали топ-менеджери технологічних і ШІ-компаній Anthropic, Google DeepMind, IBM, Meta, Microsoft, Nvidia, OpenAI, Tencen та представники неурядових організацій. Сучасні лідери держав і технологій обговорили своє бачення майбутнього ШІ в маєтку Блечлі-парк: там де раніше знаходилась Урядова школа кодів і шифрів, а 1–2 листопада 2023 року тривали дискусії щодо правил існування ШІ. **Хто та як саме прагне «керувати» ШІ?** Підписаний за підсумками саміту документ «Декларація Блетчлі», (Policy paper The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023) за назвою садиби Блетчлі-парк поблизу Лондона, де під час Другої світової війни в головному шифрувальному підрозділі Великобританії було зламано код німецької машини «Енігма».

На думку головного організатора, британського прем'єра Ріші Сунака, цей захід мав позиціонувати країну як лідера глобальних перегонів у гамуванні та регулюванні ШІ. Варто зазначити, що Великобританія останнім часом дійсно виявляє значну активність у галузі ШІ. До відкриття Саміту ШІ був залучений навіть король Чарльз ІІІ, який надіслав відеопривітання учасникам заходу. «Ми є свідками одного з найбільших технологічних проривів в історії людської цивілізації. Існує чітка потреба пересвідчитися в тому, що ця технологія, яка стрімко розвивається, буде безпечною та надійною», – зазначив він. Проте Великобританія не єдина країна, що має лідерські амбіції. 30 жовтня, за два дні до саміту США анонсували 100 аркушів законодавчої ініціативи щодо врегулювання технології ШІ. Міністер торгівлі та співочільниця делегації США Джина Раймондо на саміті, заявила, що США збираються розробити «найкращі у своєму роді» стандарти. врегулювання ШІ. Варто зазначити, що учасників цих перегонів багато: «Закон про ШІ» від ЄС найближчим часом має бути узгоджений, існують також законодавчі ініціативи від КНР. **Про що вдалося домовитися п**редставникам урядів 29 країн, зокрема США, Ктаю, Австралії, країн Євросоюзу та України, яку на саміті представив заступник міністра цифрової трансформації Георгій Дубинський? 1 листопада 2023 року уряд Великобританії оприлюднив документ «Декларація Блечлі» (Policy paper The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023). Його підписали представники країн – учасниць саміту, серед яких США та Китай. У документі попереджається про небезпеку, що її потенційно можуть нести найбільш розвинуті ШІ-системи. «Існує можливість серйозної, навіть катастрофічної шкоди, навмисної чи ненавмисної, яку здатні завдати найсучасніші ШІ-моделі. Багато ризиків, пов'язаних із ШІ, мають міжнародний характер,

тому їх найкраще вирішувати шляхом міжнародної співпраці. Ми маємо намір працювати разом, щоб забезпечити орієнтованість на людину, надійність і відповідальність штучного інтелекту», – йдеться в декларації. Підписаний документ передбачає співпрацю урядів у дослідженнях безпеки ШІ. Одна з головних цілей декларації – колективна домовленість країн щодо розробки та імплементації ризик-орієнтованих політик регулювання ШІ, які б унеможливлювали негативні наслідки. На саміті наголосили, що ШІ є корисною технологією для економічного зростання та сталого розвитку, але не може розвиватися без будь-якого нагляду й потребує встановлених "правил гри". Метою декларації є встановлення порядку денного, на який винесено: виявлення ризиків, що викликає найбільше занепокоєння в урядів, оскільки незрозуміло, яким буде вплив ШІ на навколишній світ; формування наукових алгоритмів, здатних передбачати й аналізувати ризики; розробка міждержавних політик задля пом'якшення впливу ризиків на довкілля. Водночас, уряди намагаються передбачити або принаймні запобігти ризикам, що створює технологія ШІ. Відправною точкою стала презентація ChatGPT минулого року, яка запустила глобальний бум довкола технології. Велика мовна модель, яка лежала в основі ChatGPT, показала, що майбутні покоління ШІ-систем можуть пришвидшити постановку діагнозів, допомогти в боротьбі зі змінами клімату та поліпшити виробничі процеси, а також нести загрози робочим місцям, інформаційній і національній безпеці. У звіті, оприлюдненому урядом Великобританії, вказується, що ШІ «може допомогти зловмисникам вчиняти кібератаки, проводити дезінформаційні кампанії та створювати біологічну чи хімічну зброю». Важливим позитивним фактором щодо «Декларації Блетчлі» є підписи представників Пекіну та Вашингтону, які останнім часом нечасто можна побачити на одному документі.

Викладемо основні позиції цього важливого міжнародного документу. Штучний інтелект (ШІ) відкриває величезні глобальні можливості: він має потенціал для перетворення та підвищення добробуту людей, миру та процвітання. Щоб реалізувати це, ми заявляємо, що для загального блага ШІ повинен проектуватися, розроблятися, впроваджуватися та використовуватися безпечним чином, таким чином, щоб він був орієнтований на людину, заслуговував на довіру і був відповідальним. Ми вітаємо зусилля міжнародного співтовариства зі співробітництва в галузі ШІ з метою сприяння інклюзивному економічному зростанню, сталому розвитку та інноваціям, захисту прав людини та основних свобод, а також зміцнення суспільної довіри та впевненості в тому, що системи ШІ повною мірою реалізують свій потенціал. моделях. Системи ШІ вже

використовуються в багатьох сферах повсякденного життя, включаючи житло, зайнятість, транспорт, освіту, охорону здоров'я, доступність та правосуддя, і їх використання, ймовірно, розширюватиметься. Ми визнаємо, що це унікальний момент для того, щоб діяти та підтвердити необхідність безпечного розвитку ШІ та використання перетворюючих можливостей ШІ на благо та для всіх на інклюзивній основі у наших країнах та у всьому світі. Це включає громадські послуги, такі як охорона здоров'я та освіта, продовольча безпека, наука, чиста енергія, біорізноманіття та клімат, для реалізації прав людини та для активізації зусиль для досягнення Цілей сталого розвитку Організації Об'єднаних Націй. Поряд із цими можливостями, ШІ також створює значні ризики, у т. ч. у цих сферах повсякденного життя. У зв'язку з цим ми вітаємо відповідні міжнародні зусилля щодо вивчення та усунення потенційного впливу ШІ-систем на існуючі форуми та інші відповідні ініціативи, а також визнання того, що необхідно вирішувати питання захисту прав людини, транспарентності та зрозумілості, справедливості, підзвітності, регулювання, безпеки, належного людського нагляду, етики, пом'якшення упередженості, недоторканності приватного життя та захисту даних. Відзначається можливість непередбачених ризиків, пов'язаних з можливістю маніпулювання контентом або створення контенту, що вводить в оману. Всі ці питання є критично важливими, і учасники підтверджують необхідність та актуальність їх вирішення. Особливі ризики для безпеки виникають на «передньому краї» ШІ, під яким розуміються високопродуктивні моделі ШІ загального призначення, у т. ч. базові моделі, які можуть виконувати широкий спектр завдань, а також відповідні специфічні вузькі ШІ, які можуть демонструвати можливості, які завдають шкоди. Ці проблеми частково пов'язані з тим, що ці можливості не до кінця вивчені і тому їх важко передбачити. Ми особливо стурбовані такими ризиками в таких областях, як кібербезпека та біотехнології, а також там, де передові системи ШІ можуть посилювати такі ризики, як дезінформація. Існує ймовірність серйозних, навіть катастрофічних збитків, навмисних або ненавмисних, у зв'язку з найбільш значними можливостями цих моделей ШІ. Враховуючи швидкі та невизначені темпи змін у галузі ШІ, а також у контексті прискорення інвестицій у технології, ми підтверджуємо, що поглиблення нашого розуміння цих потенційних ризиків та дій щодо їх усунення є особливо невідкладним. Багато ризиків, пов'язаних з ШІ, за своєю природою мають міжнародний характер, тому їх найкраще усувати в рамках міжнародного співробітництва. Ми сповнені рішучості працювати разом на інклюзивній основі, щоб забезпечити безпеку ШІ, орієнтована на людину, яка заслуговує на довіру і

відповідає загальному благу за допомогою існуючих міжнародних форумів та інших відповідних ініціатив, а також сприяти співпраці з метою усунення широкого спектру ризиків, пов'язаних з ШІ. При цьому ми визнаємо, що країнам слід враховувати важливість орієнтованого на інновації та пропорційного підходу до управління та регулювання, який максимізує вигоди та враховує ризики, пов'язані з ШІ. Це може включати, у разі потреби, класифікацію та категоризацію ризиків на основі національних умов та застосовних правових рамок. Ми також наголошуємо на актуальності співробітництва, де це доцільно, за такими підходами, як загальні принципи та кодекси поведінки. Що стосується конкретних ризиків, які, швидше за все, будуть виявлені у зв'язку з передовим ШІ, ми сповнені рішучості активізувати та підтримувати нашу співпрацю, а також розширювати її з іншими країнами, щоб виявляти, розуміти та, за необхідності, діяти в рамках існуючих міжнародних форумів та інших відповідних ініціатив, включаючи майбутні міжнародні саміти з безпеки ШІ. Усі зацікавлені сторони мають відігравати свою роль у забезпеченні безпеки ШІ: країни, міжнародні форуми та інші ініціативи, компанії, громадянське суспільство та наукові кола повинні працювати разом. Відзначаючи важливість інклюзивного ШІ та подолання цифрового розриву, ми знову підтверджуємо, що міжнародне співробітництво має бути спрямоване на залучення широкого кола партнерів у міру необхідності, та вітаємо підходи та політику, орієнтовані на розвиток, які могли б допомогти країнам, що розвиваються, зміцнити потенціал у галузі ШІ та використовувати стимулюючу роль ШІ для підтримки сталого зростання та усунення розриву у розвитку. Ми стверджуємо, що, незважаючи на те, що безпека повинна враховуватися на ті системи ШІ, які є надзвичайно потужними та потенційно небезпечними, несуть особливо серйозну відповідальність за безпеку цих ШІ-систем, у т. ч. за допомогою систем тестування безпеки, оцінок та інших належних заходів. Ми закликаємо всіх відповідних суб'єктів забезпечити відповідну контексту транспарентність та підзвітність щодо своїх планів щодо вимірювання, моніторингу та пом'якшення потенційно небезпечних можливостей та пов'язаних з ними наслідків, які можуть виникнути, зокрема, для запобігання неправомірному використанню та проблемам контролю, а також посилення інших ризиків. У контексті нашої співпраці, а також з метою інформування про дії на національному та міжнародному рівнях наш порядок денний щодо усунення ризиків, пов'язаних з передовим ШІ, буде зосереджений на: виявлення загроз безпеки ШІ, що викликають загальну занепокоєність, формування загального наукового обґрунтованого розуміння цих ризиків та підтримання цього розуміння в міру подальшого

розширення можливостей у контексті ширшого глобального підходу до розуміння впливу ШІ на наші суспільства. Розробка відповідних політик, заснованих на оцінці ризиків, у наших країнах для забезпечення безпеки у світлі таких ризиків, співпраця в міру потреби, визнання того, що наші підходи можуть відрізнятися залежно від національних обставин та правових рамок. Це включає поряд з підвищенням прозорості з боку приватних суб'єктів, які розробляють передові можливості в галузі ШІ, належні оціночні показники, інструменти для тестування безпеки, а також розвиток відповідного потенціалу державного сектору та наукових досліджень. У рамках реалізації цього порядку денного ми сповнені рішучості підтримувати міжнародну інклюзивну мережу наукових досліджень у галузі безпеки передового ШІ, яка охоплює та доповнює існуючу та нову багатосторонню, плюрилатеральну та двосторонню співпрацю, у т. ч. в рамках існуючих міжнародних форумів та інших відповідних ініціатив, з метою сприяння наданню найкращих наукових даних, доступних для розробки політики та суспільного блага. Визнаючи перетворюючий позитивний потенціал ШІ та в рамках забезпечення ширшої міжнародної співпраці в галузі ШІ, ми сповнені рішучості підтримувати інклюзивний глобальний діалог за участю існуючих міжнародних форумів та інших відповідних ініціатив та вносити відкритий внесок у ширші міжнародні дискусії, а також продовжувати дослідження в галузі передового ШІ Безпека, щоб гарантувати, що переваги технології можуть бути використані відповідально на благо і для всіх. Ми протягом усього життєвого циклу ШІ, суб'єкти, які розробляють передові можливості ШІ, зокрема з нетерпінням чекаємо на нову зустріч у 2024 році.

У рамках узгодження подальшого процесу міжнародної співпраці щодо безпеки ШІ на кордоні Республіки Корея погодилася спільно провести віртуальний саміт з ШІ протягом наступних 6 місяців. Відтак Франція прийматиме наступний особистий саміт через рік. "Це визначне досягнення, яке свідчить про те, що найбільші світові держави в галузі штучного інтелекту погоджуються з нагальністю розуміння ризиків штучного інтелекту, допомагаючи забезпечити довгострокове майбутнє наших дітей і онуків", – сказав прем'єр-міністр Великобританії Ріші Сунак. Україна розробила власну дорожню карту з регулювання ШІ, яка допоможе українцям навчитися захищати себе від ризиків ШІ. Український уряд розпочав роботу над нормативним полем для використання ШІ. У Мінцифри наголосили, що це важливо для розвитку країни, оскільки Україна «повинна не відставати від всього світу, а очолити тренд ШІ». Високопоставлений посадовець Міністерства оборони США Крейг Мартелл, який займається питаннями ШІ, заявив, що відомство хоче дізнати-

ся більше про інструменти ШІ, перш ніж воно погодиться взяти на себе зобов'язання використовувати цю технологію. Центральне розвідувальне управління США анонсувало запуск функції, подібної до ChatGPT, яка використовуватиме ШІ для надання аналітикам кращого доступу до відкритих джерел інформації. Американська корпорація конгломерату соціальних мереж Meta представила функції ШІ у своїх програмах, які нададуть 3 мільярдам користувачів компанії можливості, подібні до ChatGPT OpenAI. Декларація Блетчлі не є нормативною базою як такою, а закликом до її розробки шляхом міжнародної співпраці. Вона постає як ознака міжнародної єдності, яка має на меті суттєво змінити глобальні стандарти та практики безпеки ШІ. Її ширші наслідки розкривають далекоглядну дорожню карту, яка проголошує більш стандартизований підхід до безпеки ШІ в країнах. Завдяки пропаганді підвищених стандартів безпеки він створює прецедент, який, ймовірно, гармонізує правила безпеки штучного інтелекту, розвиваючи більш глобально єдиний підхід до управління ризиками ШІ.

Список використаних джерел:

1.Policy paper The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023 Published 1 November 2023.URL: The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023 – GOV. UK (www.gov.uk)

2. Світ нарешті починає регулювати штучний інтелект. URL: https://informer.today/tehnologii/svit-nareshti-pochina%d1%94-regulyuvati-shtuchnij-intelekt/

Корж І. Ф.
доктор юридичних наук, старший науковий співробітник, заступник керівника наукового центру електронного парламенту та правової інформації Державної наукової установи «Інститут інформації, безпеки і права НАПрН України»

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ СОЦІАЛЬНОЇ ТА ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Необхідно зазначити, що на сьогодні головною можливістю для подальшого розвитку як суспільства в цілому, так і для держав зокрема є цифрова трансформація суспільного життя. Одночасно вона ж є і головною проблемою соціального життя суспільства. Здійснюючи планування щодо проведення цифрових перетворень, керівники держав та різних організацій мають враховувати ті культурні зміни, з якими вони стикаються у повсякденному житті, оскільки і лідери, і працівники мають пристосовуватися до прийняття та використання незнайомих для них нових технологій.

Зазначимо, що цифрова трансформація створила унікальні умови та можливості для ринку праці, оскільки роботодавці можуть конкурувати з конкурентами, які користуються відповідними перевагами, що забезпечує така технологія. Окрім того, завдяки високій важливості запровадженим сьогодні технологіям та їх широкому використанню, результати оцифрування доходів, прибутку та можливостей мають значний потенціал для зростання.

Основною рушійною силою цифрової трансформації, а фактично цифрової революції, стало широке поширення обчислювальної техніки, перш за все – персональних комп'ютерів, всеосяжне проникнення Інтернету, масове застосування персональних портативних комунікаційних пристроїв тощо.

За результатами 2022 року Індекс цифрової трансформації регіонів України, який розробила команда регіональної цифровізації Мінцифри України, становила 0,651 з 1 можливого. Зазначений індекс – це один з інструментів для вимірювання процесів інформатизації та цифровізації у 24 регіонах України. Такий аналіз дозволяє визначити ефективність органів влади у напрямі цифровізації, а також побачити потреби у цифровій трансформації. Найвище значення мають Дніпропетровська [0.916], Тернопільська [0.910] та Одеська [0.836] області. Серед основних субін-

дексів найвищі значення спостерігаються у «Розвиток ЦНАП» [0.771], «Режим «без паперів» [0.691] та «Розвиток інтернету» [0.683] [2].

Згідно зі щорічним звітом Global Digital Overview, станом на початок 2023 року Інтернетом користувалися 5,16 млрд. людей, а це приблизно 64% від населення Землі. При цьому серед міського населення інтернет-юзерів 78,3%, а серед сільського лише 45,8% [1].

Проблема цифрової нерівності в Україні зумовлена двома головними чинниками:

– відсутністю швидкісного Інтернету (дротового та мобільного) у низці населених пунктів, особливо в сільській місцевості;
– низьким рівнем цифрової грамотності частини населення.

Згідно з дослідженням Міністерства цифрової трансформації України, у 2021 році частка українців віком від 18 до 70 років, цифрові навички яких нижче позначки «базовий рівень», становить 47,8% населення. А кількість тих, що не мають жодних цифрових навичок, – 11,2%. У порівнянні з 2019 роком ці показники зменшилися на 5,2% та 4% відповідно.

Дослідження КМІС показує, що за останні 3 роки рівень користування електронними послугами найбільше зріс серед людей старших вікових категорій:

– на 52% серед людей віком 70 і більше;
– на 30% серед людей віком 50-69 років;
– на 18% серед людей віком 30-49 років;
– на 11% серед людей віком 18-29 років [1].

До повномасштабного вторгнення в Україні планували забезпечити доступом до Інтернету всі населені пункти у 2022 році і підключити 95% українців до мережі до кінця 2023-го. Наскільки вдалося виконати ці плани, говорити складно, адже мільйони українців мусили залишити свої домівки, інфраструктуру пошкодили обстріли, а частина територій перебуває під окупацією.

І у Мінцифри України, і у Національній комісії електронних комунікацій (НКЕК) подолання цифрового розриву називають одним з ключових пріоритетів в Україні. Вирішення проблеми цифрового розриву суттєво ускладнює російське вторгнення та знищення і пошкодження інфраструктури. Тим не менш, робота в цьому напрямку ведеться – є відповідні програми Мінцифри України, є бажання телеком-операторів відновлювати та розвивати свої мережі, в тому числі надавати послуги швидкісного Інтернету якомога більшій частині населення.

Водночас, необхідно зазначити, що для того, щоб послуги зв'язку надавалися якісно, необхідні тендери на забезпечення проблемних зон

Інтернетом, де до уваги будуть братися не лише ціна і локальний статус (чи ні) учасника, але також його спроможність виконати озвучені задачі.

Однак, станом на 4 травня 2023 року SPEKA (онлайн медіа про технології та підприємництво) не знайшла на сайті Prozorro тендерів на надання послуг зв'язку (мобільного або дротового), у віддалених населених пунктах, де замовниками виступали б Мінцифри України чи НКЕК [1].

Попри те, що на остаточне вирішення проблеми цифрового розриву можна очікувати не раніше перемоги над Росією, і держава, і оператори зв'язку мають докласти максимальних зусиль, щоб забезпечити Інтернетом максимальну кількість українців, особливо у віддалених населених пунктах. Як показує дослідження КМІС, сьогодні це може стати питанням життя чи смерті.

Доброю підмогою у вирішенні згаданих проблем може бути поширення на цивільне населення та бізнес користування абонентськими супутниковими терміналами системи SpaceX. Однак для зазначеного мають бути прийняті відповідні рішення Нацкомісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв'язку, а також Національного центру оперативно-технічного управління мережами телекомунікацій (НЦУ), якими мають бути приведення умов використання Starlink в правові рамки. Поява документів регулятора та НЦУ призведе використання Starlink в правових рамках.

Як зазначив Голова Держспецзв'язку Юрій Щиголь, на період воєнного стану Starlink можуть використовувати всі охочі, в тому числі й пересічні громадяни, органи влади та підприємства будь-якої форми власності [3].

Список використаних джерел:

1. Скільки українців не мають доступу до Інтернету і коли ми подолаємо цифровий розрив. URL: https://speka.media/skilki-ukrayinciv-dosi-nemayut-dostupu-do-internetu-i-shho-robiti-z-cifrovim-rozrivom-plg4x9 (дата звернення: 28.10.2023).

2. Результати цифрової трансформації в регіонах України. URL: https://thedigital.gov.ua/news/rezultati-tsifrovoi-transformatsii-v-regionakh-ukraini-1 (дата звернення: 29.10.2023).

3. В Україні всі можуть використовувати Starlink – Держспецзв'язку. URL: https://ms.detector.media/trendi/post/29369/2022-04-20-v-ukraini-vsi-mozhut-vykorystovuvaty-starlink-derzhspetszvyazku/ (дата звернення: 30.10.2023).

Батиргареєва В. С.
доктор юридичних наук, професор,
головний науковий співробітник
Державної наукової установи
«Інститут інформації, безпеки і
права» НАПрН України

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ЯК ЗАСІБ ВЧИНЕННЯ ДІЙ, ПОВ'ЯЗАНИХ ІЗ ГЛОРИФІКАЦІЄЮ АГРЕСОРА

Однією з визначальних особливостей сьогодення є трансформація укладу життя з формату постіндустріального суспільства на суспільство інформаційне. Це, безумовно, викликає необхідність впровадження й широкого використання інформаційно-комунікаційних технологій практично в усіх сферах життєдіяльності сучасної людини. Ще в Основних засадах розвитку інформаційного суспільства в Україні на 2007-2015 роки зазначалося, що Україна має власну історію розвитку базових засад інформаційного суспільства: діяльність всесвітньо відомої школи кібернетики; формування на початку 90-х років минулого століття концепції та програми інформатизації; створення різноманітних інформаційно-комунікаційних технологій і загальнодержавних інформаційно-аналітичних систем різного рівня та призначення [1]. Як справедливо наголошується у спеціальній літературі, «жива комунікація невід'ємна від інформаційних технологій, тому на сучасному етапі розвитку технічних і програмних засобів інформаційні технології називають інформаційно-комунікаційними» [2].

Разом із тим дедалі проблема інформатизації стає питанням правового і навіть філософського звучання, оскільки відносини «людина – інформаційно-комунікаційні технології» не є настільки однозначними, щоб не бачити пасток і ризиків, які буквально увірвалися у життя кожного з нас. У цьому зв'язку дискусія про темний бік сервісів інформаційно-комунікаційних технологій згодом лише набиратиме обертів, а інструменти правової оцінки ставатимуть невід'ємним атрибутом цифрового буття.

Крайнім виразом деструкції зазначених вище відносин є злочинність. На наш погляд, злочинність зараз «оцифровується», адже все більше і більше протиправних діянь переміщується до Інтернет-простору. Кібертероризм, кібершпигунство, продаж наркотиків через так звані Інтернет-магазини, кібершахрайство, кібермобінг, легалізація доходів, одержаних злочинним шляхом, поширення порнографії, порушення приватності і безпеки в онлайн-середовищі та ін. – таким є далеко неповний перелік

правопорушень, вчинення яких стає можливим завдяки можливостям інформаційно-комунікаційних технологій. До того ж частина таких діянь характеризується значною латентністю, зокрема, внаслідок неперсоніфікованості учасників відповідної комунікації, транснаціонального характеру діянь, а так само значним поширенням, великою швидкістю модифікацій правопорушень, складністю їх викриття тощо. У цьому плані не є виключенням й правопорушення, що з'явилися через збройну агресію рф проти України.

У березні 2022 року розділ XX Особливої частини КК Украйни (Кримінальні правопорушення проти миру, безпеки людства та міжнародного правопорядку) був доповнений статей 436^2, в якій установлено заборону виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікації її учасників [3]. Запровадження нового нормативного матеріалу і накопичення практики розгляду цієї категорії кримінальних проваджень викликає необхідність кримінологічного аналізу сутності цього явища та його причин, особи правопорушника, а так само розробки заходів запобігання цим правопорушенням.

За даними Офісу Генерального прокурора, станом на 1 листопада 2023 р. зареєстровано 1 354 факти вчинення злочинів, передбачених ст.436^2 КК України (далі – глорифікація). За 10 місяців 2023 р. зафіксовано ще 1 233 випадки. Станом на 1 жовтня 2023 р. судами розглянуто 728 кримінальних проваджень. За результатами узагальнення цих проваджень нам вдалося визначити місце і роль інформаційно-комунікаційних технологій у процесі вчинення зазначеного правопорушення.

Недивлячись на те, що переважна кількість глорифікаторів – особи передпенсійного і пенсійного віку (їх частка складає 66,1%), однак під час вчинення відповідних правопорушень пальма першості у поширенні наративів «руського миру» та звеличенні російського агресора як такого належить саме можливостям інформаційно-комунікаційних технологій, які у даному разі з позитивних важелів цифрової трансформації соціуму перетворюються на зло. Адже ці технології стають своєрідними судинами, по яких розносяться шкідливі ідеї, думки, погляди тощо.

Отже, визначимо, які саме інформаційно-комунікаційні технології використовуються винними особи, що вчиняються кримінально каране правопорушення, передбачене ст. 436^2 КК України? Насамперед йдеться про використання соціальних мереж Інтернету та різних комунікаторів у мобільній телефонії. Як відомо, сьогодні не обов'язково наживо спілкуватися один з одним, щоб обмінюватися думками, щось планувати, замислювати та ін., оскільки особисте спілкування все більше й біль-

ше «оцифровується», що, втім, є загальною тенденцією в інформаційно глобалізованому світі. Проте подібне спілкування за допомогою високих технологій інколи набуває негативного суспільного резонансу через той контент, який стає надбанням гласності та водночас містить небезпечні для суспільства позиції.

За результатами проаналізованих вироків у 83,1% (!) випадків місцем вчинення злочину є Інтернет-простір. Особливою популярністю у глорифікаторів користуються: 1) соціально орієнтована мережа «Одноклассники» (рос.) – 61,7%; 2) Телеграм-канал – 7,0%; 3) «ВКонтакте» (рос.) – 6,3% та 4) Фейсбук – 4,6%. Принагідно слід зауважити, що перенесення ідеологічних баталій до Інтернет-простору є одним із проявів гібридної війни, яку чимало років рф не без успіху здійснювала щодо України. Таким чином, зв'язок глорифікаторів один з одними, а так само можливе поширенням ідей серед необмеженого кола осіб відбувається насамперед за допомогою Інтернет-інструментів соціального контактування.

Але таким уже необмеженим є коло осіб, які наражаються на ворожі наративи глорифікаторів, якщо використовуються інформаційно-комунікаційні технології? На наш погляд, інформація щодо виправдовування, визнання правомірною, заперечення збройної агресії рф проти України, розпочатої у 2014 році, заперечення тимчасової окупації частини території України, глорифікація її учасників, розміщена у заборонених в Україні соціальних мережах («Одноклассники», «ВКонтакте» (рос.)), є доступною лише для користувачів відповідних мереж. Тому їх вплив в національному сегменті Інтернет-простору є, вочевидь, не настільки визначальним.

Дійсно, масовим «народним» інструментом поширення наративів російської пропаганди є такі соціальні мережі, як «Одноклассники» та «ВКонтакте» (рос.). Поява цих російських медіапродуктів датована березнем 2006 р. та жовтнем 2006 р. відповідно. За даними SimilarWeb – компанії, що здійснює діяльність у сфері інформаційних технологій, у 2021 р. сайт «ВКонтакте», наприклад, посідав п'ятнадцяте за популярністю місце у світі, на 1 жовтня 2023 р. позиції сайту значно погіршилися – він посів вже тридцяту позицію [4]. Проте серед російськомовного населення зазначені мережі все ще залишаються достатньо популярними.

Як відомо, в Україні ще у 2017 р. застосовано блокування зазначених соціальних мереж. Юридичним приводом для блокування стало введення додаткових санкцій України щодо рф Указом Президента України П. Порошенка «Про введення в дію рішення РНБО України від 28 квітня 2017 р. «Про застосування персональних спеціальних економічних та ін-

ших обмежувальних заходів (санкцій)» № 133/2017 від 15 травня 2017 р. [5]. Таким чином, на сьогодні існує нормативний фільтр, що максимально зменшив аудиторію контенту, котрий поширюється цими каналами. Більшість громадян України виявилися свідомими інтернет-користувачами, а тому твердения про вплив на їх свідомість саме у такий спосіб є перебільшенням.

У противному разі, якщо визнати ці заходи недієвими, то логічним кроком у подальшому може уявлятися встановлення юридичної відповідальності (аж до кримінальної) за створення акаунтів у заборонених соціальних мережах та відвідування сторінок користувачів останніх. Це, по-перше.

По-друге, не складно уявити, що відвідувачами сторінок у цих соціальних мережах, а тим більше зі шкідливим контентом, є ті особи, які вже заздалегідь позитивно сприймають російські наративи. Їх «реакція» (одна з можливих функцій, наприклад, соціальної мережі «Одноклассники») на подібні матеріали, внаслідок чого вони відбиваються й на власних сторінках таких відвідувачів, свідчить про те, що зараження ідеологією ворога, як правило, вже в людини відбулося. У такому разі поширення ідей має умовний характер, оскільки вони «циркулюють» у колі, вже заздалегідь визначеному. Інша справа, коли відповідні думки поширюються соціальними мережами, не забороненими в Україні. Ось тут правова рефлексія має бути негайною.

Таким чином, не зовсім справедливим уявляється твердження, яке дуже часто сьогодні зустрічається у судовій практиці та сутність якого добре передається у таких формулюваннях «відповідна сторінка відкрита для перегляду всіма користувачами соціальної Інтернет-мережі «Одноклассники», що свідчить про ознайомлення із даними відомостями іншими особами», або «сторінка є доступною для загального ознайомлення всіх користувачів соціальної Інтернет-мережі «Одноклассники», які відвідували сторінку гр-на Х. та на якій розміщена інформація, що виправдовує, заперечує, визнає правомірною збройну агресію рф проти України … і далі за текстом».

Список використаних джерел:

1. Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: затв. Законом України від 9 січня 2007 р. № 537-V. *Офіційний вісник України.* 2007. № 8. Ст. 273.

2 Фоміних Н. Ю. Сутність поняття «інформаційно-комунікаційні технології» та їх значення на сучасному етапі модернізації освіти. URL: http:// dspace. uabs. edu. ua/ jspui/bitstream/ 123456789/ 9084/1/ ped905_77.pdf.

3. Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції: Закон України від 3 березня 2022 р. № 2110-IX. Офіційний вісник України. 2022. 29 квіт. № 33. Ст. 1719.

4. SimilarWeb. UTL: https://www.similarweb.com/top-websites/.

5. Про введення в дію рішення РНБО України від 28 квітня 2017 р. «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: введено в дію Указом Президента України від 15 травня 2017 р. № 133/2017. *Офіційний вісник України.* 2017 р. № 41. Ст. 1276.

Капіца Ю. М.
доктор юридичних наук, директор
Центру досліджень інтелектуальної
власності та трансферу технологій
НАН України

ПРОБЛЕМИ РЕАЛІЗАЦІЇ ПРИНЦИПІВ ВІДКРИТОЇ НАУКИ У ДІЯЛЬНОСТІ ОРГАНІВ ВИКОНАВЧОЇ ВЛАДИ У СФЕРІ НАУКИ ТА ОСВІТИ В УКРАЇНІ

Розвиток відкритої науки є одним з політичних пріоритетів в Європейському Союзі та США та пов'язаний з поширенням надання відкритого доступу до наукових статей та дослідницьких даних. В Україні розпорядженням Кабінету Міністрів України від 08.10.2022 р. № 892-р затверджено «Національний план щодо відкритої науки», Національною академією наук України прийнято постанову від 02.11.2022 № 327 «Щодо участі НАН України в реалізації європейських принципів відкритої науки».

Принципи відкритої науки включають забезпечення при відкритому доступі до наукових статей, дослідницьких даних захист конфіденційної інформації, охорони прав інтелектуальної власності. Так, Рекомендація Комісії (ЄС) 2018/790 від 25.04.2018 щодо доступу до наукової інформації та її збереження визначає, що відкритий доступ має здійснюватися «без шкоди для захисту ноу-хау та ділової інформації (комерційної таємниці)". Держави-члени повинні забезпечити, щоб в результаті політики ВД або планів дій було забезпечено обмеження доступу до даних, що може бути пов'язано, зокрема, з причин конфіденційності, комерційної таємниці, національної безпеки, законних комерційних інтересів і прав інтелектуальної власності третіх сторін. Аналогічні положення містять Директива

(ЄС) 2019/1024 про відкриті дані та повторне використання інформації в державному секторі 2019 р., Модельна угода РП Горизонт 2020 [1-3].

Зазначимо, що з врахуванням статусу України як кандидата на вступ до ЄС, положення актів ЄС в обов'язковому порядку мають бути імплементовані у законодавство України [4].

Аналіз актів у сфері науки і освіти, зокрема, підзаконних актів, які приймаються Міністерством освіти і науки України, а також практики їх реалізації свідчить про невідповідність положень цих актів принципам відкритої науки в Європейському Союзі, а також про створення умов для порушень суб'єктами освітньої діяльності, науковими установами законодавства України про авторське право, розголошення конфіденційної інформації, комерційної таємниці.

Вказане стосується діяльності Національного репозитарію академічних текстів, а також реєстрації науково-дослідних, робіт і дисертацій, змісту та реалізації наказів МОН України від 04.07.2018 № 707 «Про затвердження Регламенту роботи Національного репозитарію академічних текстів» (далі – Репозитарій), від 24.03.2022 № 271 "Про затвердження Порядку державної реєстрації та обліку науково-дослідних, дослідно-конструкторських робіт і дисертацій" (далі – Порядок), Положення про Національний репозитарій академічних текстів, затвердженого постановою Кабінету Міністрів України від 19.07.2017 № 541.

Так, відповідно до зазначеної постанови до Репозитарію мають включатися на умовах відкритого доступу дисертації, випускні роботи здобувачів, монографії, звіти у сфері наукової і науково-технічної діяльності тощо. Разом з тим положення постанови та наказів МОН України не містять механізму укладання авторами, іншими особами, що мають авторське право, ліцензійного договору (надання ліцензії) на розміщення дисертацій, звітів тощо у Репозитарії відповідно до вимог Цивільного кодексу України та Закону України «Про авторське право і суміжні права».

Так, звіти про проведення ДіР передаються до УКРІНТЕІ без укладання ліцензійного договору з надання УКРІНТЕІ прав використання творів, що призводить до подальшого порушення УКРІНТЕІ авторського права при розміщенні дисертацій та звітів у Репозитарії та надання до них доступу у мережі Інтернет. Крім того, практика розміщення на веб-сайтах ЗВО, наукових установ дисертацій свідчить про переважну відсутність укладання такими організаціями ліцензійних договорів з авторами щодо надання права ЗВО, науковим організацій відтворювати дисертації, здійснювати до них інтерактивне надання доступу через мережу Інтернет тощо, що призводить до порушень авторського права на твори.

Також, при переданні до УКРІНТЕІ звітів про проведення ДіР створюються умови для розголошення конфіденційної інформації та комерційної таємниці закладів вищої освіти та наукових установ стосовно окремих результатів досліджень.

Так, при реєстрації та обліку ДіР згідно пп. ІІІ.1 Порядку інформації може бути визначений режим доступу до інформації, що міститься у ДіР: «Відкрита»; «Для службового користування»; «Таємно»; «Цілком таємно».

У Порядку зазначається, що вказані обмеження доступу здійснюються відповідно до частини другої статті 6 та статті 9 Закону України «Про доступ до публічної інформації». В той же часу у ***Порядку не передбачено, що інформація про ДіР може відноситися до «конфіденційної інформації», «комерційної таємниці»,*** хоча частиною першою ст. 6 Закону «Публічна інформація з обмеженим доступом» визначається, що «Інформацією з обмеженим доступом є: 1) конфіденційна інформація; 2) таємна інформація; 3) службова інформація».

Також у Порядку порушується вимоги зазначеного закону, що обмеження доступу до інформації здійснюється, у тому числі, «для запобігання розголошенню інформації, одержаної конфіденційно».

При цьому ЗВО, наукові організації не можуть відносити звіти з проведення ДіР або певні частини таких звітів до службової інформації внаслідок того, що така інформація згідно ст. 9 Закону «Службова інформація» складає певні види інформації, яка міститься в документах суб'єктів владних повноважень, проте не наукових організацій та ЗВО. Також, виходячи із Порядку, гриф "Таємно" відноситься до інформації, що становить державну таємницю.

Вказаний порядок реєстрації примушує ЗВО та наукові організації або не здійснювати реєстрацію ДіР або здійснювати її з порушенням законодавства та віднесенням звітів, які містять конфіденційну інформацію, комерційну таємницю, – до відкритої інформації.

Наслідком цього є, що при наявності у наукових звітах конфіденційної інформації, таємної інформації (у тому числі ноу-хау, комерційної таємниці) вимоги Порядку призводять до відкриття такої інформації відвідуючими та користувачами Національного депозитарію. Вказане має наслідком неможливість у зв'язку з розголошенням конфіденційної інформації, комерційної таємниці подання заявок на винаходи та інші ОІВ; до розкриття ноу-хау з унеможливленням для закладів вищої освіти. наукових організацій у подальшому здійснювати комерціалізацію результатів досліджень, а також в умовах військової агресії – створює умови для відкриття інформації з обмеженим доступом.

Таким чином, Порядок реєстрації в частині визначення доступу до інформації, що міститься у ДіР та непередбачення охорони конфіденційної інформації та комерційної таємниці є незаконним та порушує положення ст. 6 Закону України «Про доступ до публічної інформації», що стосується захисту від розголошення конфіденційної інформації, а також комерційної таємниці, яка поряд з іншими видами таємної інформації (лікарська таємниця, банківська таємниця тощо) відноситься до таємної інформації.

Також, використання електронних копій академічних текстів без надання відповідного дозволу правовласника на підставі ліцензійного договору (ліцензії) є порушенням авторського права з цивільною, адміністративною та кримінальною відповідальністю за незаконне відтворення творів, подання творів до загального відома публіки, їх розповсюдження (ст. 12, 53-54 Закону України "Про авторське право і суміжні права").

Вказане також суперечить принципам відкритого доступу до дослідницьких даних, наукової інформації в Європейському Союзі, у тому числі положенням ст. 1, 10 Директиви (ЄС) 2019/1024 про відкриті дані та повторне використання інформації в державному секторі.

З врахуванням наведеного до актів, що стосуються діяльності Національного репозитарію академічних текстів, реєстрації та обліку науково-дослідних, дослідно-конструкторських робіт і дисертацій (постанова Кабінету Міністрів України від 19.07.2017 № 541, накази МОН України від 04.07.2018 № 707 та від 24.03.2022 № 271) мають бути внесені зміни, що забезпечують дотримання авторського права та захисту від розголошення конфіденційної інформації, комерційної таємниці при розміщенні у відкритому доступі текстів дисертацій та звітів про проведення науково-дослідних, дослідно-конструкторських робіт і дисертацій. При цьому, при реєстрації звітів може бути, за нашою думкою, передбачено розподіл звіту на частину, до якої може надаватися відкритий доступ та частину, яка містить інформацію, віднесену до конфіденційної, комерційної таємниці, доступ до якої буде обмежено.

Список використаних джерел:

1. Commission Recommendation (EU) 2018/790 of 25 April 2018 on access to and preservation of scientific information. C/2018/2375.

2. 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.

3. Annotated Model Grant Agreement "HORIZON Europe", EU Funding Programmes 2021-2027, issued 30 November, 2021.

4. Капіца Ю. М. Відкрита наука та інтелектуальна власність. *Інформація і право*. 2023. № 2(45). С. 73-87.

Дубняк М. В.
кандидат юридичних наук, в.о. завідувача наукової лабораторії правового забезпечення цифрової трансформації, Наукового центру цифрової трансформації і права Державної наукової установи «Інститут інформації, безпеки і права НАПрН України»
Старший викладач кафедри інформаційного, господарського та адміністративного права, КПІ ім. Ігоря Сікорського
ORCID: https://orcid.org/0000-0001-7281-6568.

ОБРОБКА ВЕЛИКИХ ДАНИХ ТА ПРАВО НА ПРОГНОЗНІ ВИСНОВКИ ШТУЧНОГО ІНТЕЛЕКТУ

Великі дані – це дані, які вироблені людьми у процесі користування Інтернетом, які можуть бути збережені, оброблені та використані за допомогою використання спеціальних методів та інструментів [1]. Також великі дані розуміють як набір методів та технології, для обчислювання та моделювання тенденцій та асоціацій, особливо стосовно поведінки людей та їх взаємодії [2]. Дослідження великих даних тісно пов'язано із соціальною сферою, адже соціум є одним із джерел походження великих даних, та, одночасно, сферою використання результатів обробки таких даних. Результат обробки великих даних технологіями штучного інтелекту дозволяє отримати прогнозні висновки. Такі висновки забезпечують конкурентні переваги для бізнесу, оскільки дозволяють змоделювати поведінку споживачів, а інколи, і безпосередньо вплинути на їх рішення.

Великі дані можуть включати в себе комбінований набір даних, як персональних, так і неперсональних даних (індустріальних, мета даних). Тому з правової точки зору, великі дані аналізуються з урахуванням дотримання правових підстав збору, обробки, використання, збереження даних.

Норми Загального Регламенту про захист персональних даних *(далі – GDPR)* встановлюють ряд прав для суб'єкта даних, зокрема: право бути поінформованим про збирання даних, право доступу до даних, право на виправлення, право бути «забутим», обмеження опрацювання, право на мобільність (перенесення) даних, право на заперечення, захист від про-

файлінгу [3]. Однак, через використання засобів анонімізації, шифрування для формування наборів великих даних, розмиваються правові ознаки персональних даних. А отже суб'єкт даних не може знати, що його дані були включені до набору великих даних для обробки і формування прогнозних висновків. А відтак не може реалізувати передбачені GDPR права суб'єкта даних. Виникає соціальне протиріччя, коли через використання анонімізованих наборів великих даних бізнес отримує прогнозну аналітику, яка впливає на суб'єкта даних та його рішення, наприклад, через показ персоналізованої реклами, а суб'єкт даних не має правових механізмів для управління своїми даними через розмивання правових ознак персональних даних.

Правовий режим охорони і захисту персональних даних, у практиці суду ЄС, захищається з урахуванням розширеного тлумачення «персональних даних». Зокрема, за режимом персональних даних захищається інформація, якщо вона «стосуються» фізичної особи і може вплинути на неї [4]. Якщо детально проаналізувати норми регламенту GDPR ми встановимо, що вони направлені на процес збору, обробки, передачі та захисту персональних даних, однак не поширюються на згенеровані «нові дані», які були отримані за результатами аналізу великих наборів даних, в тому числі персональних, та прогнозують або моделюють поведінку суб'єкта даних у майбутньому, тобто саме прогнозні висновки. Пояснюється це тим, що згода на обробку персональних даних надається щодо конкретних, вже існуючих даних, а не щодо даних, які будуть створені (згенеровані) у майбутньому.

У 2014 році, у справі «YS, M і S» Суд ЄС, вирішував питання обсягу даних, які слід розкривати суб'єкту даних у зв'язку з їх обробкою. У цій справі ідеться про дані, які залишає про себе суб'єкт даних у процесі отримання адміністративної послуги. Для її отримання у заяві заявник надає про себе як персональні дані *(ім'я, дата народження, місце проживання)* так і не персональні дані. Справа заявника включає інформацію, яка його стосуються: деталі процесуальної історії; відомості про заяви заявника та подані документи; правові положення, які застосовуються до ситуації заявника; оцінка вищевказаної інформації через призму застосовних правових положень у формі протоколу з правовим аналізом. Виникає ряд питань: при реалізації права суб'єкта даних на доступ до своїх персональних даних, буде надано доступ до всієї справи в цілому, лише до його заяви, чи надання доступу в частині, де є персональні дані. Чи може суб'єкт даних отримати протокол з правовим аналізом, який склав працівник адміністративного органу, по суті прогнозний висновок у формі правового аналізу з конкретними оцінками і особистим

баченням ситуації заявника. Розглядаючи викладені обставини справи Суд ЄС встановив, що «дані, внесені в протокол, є персональними даними». Правовий аналіз у протоколі "стосується" конкретної фізичної особи, ґрунтується на його ситуації та індивідуальних характеристиках цієї особи, тому підпадає під дію поняття «персональні дані».

Але сама по собі сукупність правових норм юридичного аналізу не може тлумачитись як персональні дані, не може бути предметом судової перевірки і не є об'єктом реалізації права на виправлення (п. 39, 41, 42 рішення [5]).

У рішенні Суду ЄС чітко зазначено, що аналіз і складові висновки не вважаються персональними даними. Суд ЄС не розрізняє правовий аналіз і результати обробки даних у вигляді окремих коментарів чи висновків, створених у процесі обробки вихідного набору даних (п.39 рішення [5]). Аналіз не є еквівалентом прогнозних висновків, а скоріше міркуванням (логікою), яка веде до висновку. У контексті проблеми формування прогнозних висновків та обробки великих даних штучним інтелектом, ми можемо знати лише про математичні методи обробки, а не про те, як їх застосовував штучний інтелект для отримання конкретного одиничного висновку (ефект чорної скриньки).

З аналізу правових підходів у справі «YS, M і S» Суду ЄС, можемо встановити, що право доступу та право на виправлення не можуть бути ефективно реалізовані для захисту суб'єкта даних від прогнозних висновків. Адже суб'єкт даних може не знати, про те, що:

1) його дані включено до набору великих даних;

2) не має доступу до аргументації, яка знаходиться в основі рішень;

3) не може виправити результати прогнозного висновку, оскільки немає прямого правового зв'язку між складом набору даних та правами конкретного суб'єкта даних;

4) такі висновки не охоплюється умовами первісної згоди на обробку даних, навіть якщо вона була надана.

Отже, прогнозні висновки є окремим результатом обробки даних, які знаходяться за межами правового регулювання законодавства про захист персональних даних. Суб'єкт даних не може застосувати жодні спеціальні права передбачені GDPR, оскільки норми Регламенту поширюються на процес збору, обробки, передачі, захисту наявних даних. Згода суб'єкта даних також надається на обробку конкретних вже існуючих даних, а не тих даних, які будуть створені у майбутньому.

Право на результат прогнозних висновків необхідний суб'єкту даних, для того, щоб оцінити наскільки ці висновки впливають на його поведінку, а не для того, щоб вносити виправлення в результати обробки, наприклад через некоректно підібрані методи їх обробки.

Список використаної літератури:

1. Big data. Cambridge Dictionary.
URL: http://dictionary.cambridge.org/dictionary/english/big-data.
2. Big data. The Oxford English dictionary.
URL: https://en.oxforddictionaries.com/definition/big_data.
3. Regulation (EU) 2016/679 Of The European Parliament And Of The Council on General Data Protection Regulation.
URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016 R0679&qid=1684155858687
4. Graef I., Gellert R., Husovec, M. (2018). Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation. Cybersecurity.
URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3256189
5. YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M and S : Judgment of the Court (Third Chamber), 17 July 2014. , ECLI identifier: ECLI:EU:C:2014:2081
URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=ecli%3AECLI%3AEU%3AC%3A2014%3A2081

Андрієнко О. В.
кандидат психологічних наук, адвокат, заступник директора з правових питань ДП «ССМ» (Publicis Groupe Ukraine), Членкиня Експертно-консультаційного комітету з питань розвитку сфери ШІ в Україні при Міністерстві цифрової трансформації України

ЛЮДИНА VS ШТУЧНИЙ ІНТЕЛЕКТ: МОНОПОЛІЯ ЛЮДИНИ НА СМИСЛИ, КРЕАТИВНІСТЬ ТА ВІДПОВІДАЛЬНІСТЬ

Штучний інтелект (надалі – ШІ) став фокусом колективної свідомості людства у 2023 році, на що вказують найрізноманітніші індикатори: від визнання словом року та загальної доступності інструментів генеративного ШІ (надалі – ГШІ) – до фінальних кроків у прийнятті EU AI Act, Указу Президента США про безпечну, захищену та надійну розробку та використання ШІ, законодавства КНР щодо ГШІ – й аж до наукової гіпо-

тези, що інопланетяни є формою ШІ [1]. Тож пов'язана з ШІ глобальна трансформація суспільства (із законодавством, економікою та ринком праці включно) перестала бути науковою фантастикою і перетворилася з віддаленої перспективи на насущне питання. Тому філософське та методологічне питання про розмежування сфер компетенції людини та ШІ, а також сфер їхньої максимально ефективної колаборації, набуває нової гостроти. Адже від відповіді на нього залежить, зокрема, те, як розвиватиметься правовий статус обох – і людини, і ШІ.

За своїм походженням, **ШІ є квінтесенцією колективної свідомості людства**. Ця квінтесенція втілюється і діє через розроблене людиною програмне забезпечення, навчається на даних, вектор збору яких задається людиною, і може генерувати результати (контент, прогнози, рекомендації або рішення) з **цілями**, визначеними людиною, впливаючи на середовище і людину, з якими ШІ взаємодіє.

У цих батьківсько-дитячих стосунках ШІ поки не має іншого імпульсу для власного існування та розвитку, окрім успадкованих від людства. Тому ШІ виступає дзеркалом людства, завдяки якому ми можемо, по-перше, усвідомити, що є найглибшою суттю нашого буття, а по-друге, вирішити, що ми як людство готові делегувати ШІ, дозволивши йому почасти незалежну від людини еволюцію.

Аналіз домінуючих психологічних теорій та правових доктрин на поточному етапі розвитку людства дозволяє висунути гіпотезу, що наразі за людиною варто залишити монополію на генерування смислів, креативність та відповідальність.

Смисл – це остаточна (найвища чи кінцева) мета існування суб'єкта та інструмент руху між рівнями віртуалізації, тобто між різними шарами реальності, які виокремлює (творить) наш розум: фізичною, біологічною, соціальною, правовою, цифровою тощо. Будь-яка психіка – це інструмент трансформації енергії в інформацію, яка фіксується у тих чи інших формах – об'єктах реальності. Тому саме смисли є тим стрижнем (диспозиційним ядром у термінології психології), навколо якого ми **створюємо** і підтримуємо всупереч всім загрозам нашу **втілену форму**: від фізичної (людське тіло), психологічної (особистість), матеріальної (середовище проживання), соціальної (соціальні ролі й статус), економічної (майнові права), правової (правосуб'єктність), політичної (громадянські права та обов'язки) – до екологічної (екосистема) та духовної (світогляд та життєвий шлях як окрема форма). Слід підкреслити, що кожна з цих форм – це **унікальна стійка у просторі та часі конфігурація циклів енергетично-інформаційного обміну**, тобто форма – це водночас і об'єкт, і процес (відносини), гравітаційним ядром яких виступає

людина як носій психіки. Зрозуміло, що у вимірі «смисл (суть) – форма» навіть найпросунутіший ШІ має набагато слабший ніж в людини ціннісний зв'язок між тілом (матеріальною основою) та обчислювальним процесом, тобто процесом трансформації енергії в інформацію, адже смисли, з яких постають цінності, задає людина, а не ШІ. Тому **ШІ** – це **інструмент**, передусім, **фіксованого мислення** (мислення згідно зовні встановлених правил і цілей), у той час як **людина – носій мислення розвитку**, тобто **здатності самостійно задавати правила і мету** гри.

Самореалізація означає **свободу творення** різноманітних форм, які є нашою маніфестацією у цьому світі. Передумовою такої свободи творення є **свобода інтерпретації** як здатність виокремлювати (обирати), підтримувати та розвивати з потоку (хаосі) інформаційно-енергетичного обміну стійкі патерни, стабілізуючи та масштабуючи їх у просторі та/або часі відповідно до смислів, які людина делегує таким формам. ШІ може генерувати нескінченну кількість ситуативних патернів, проте лише людина визначає, що має смисл і варте уваги у її житті.

Саме **креативність** як творення гармонійної (тобто об'єднаної смислом) множини різноманітних форм є смислом людського існування. І саме втратою або деформацією частиною із цих форм ми ризикуємо, коли беремо відповідальність за свої діяння. Іншими словами, **відповідальність** – це ступінь ризику власною формою, який приймає суб'єкт у процесі творення свого життєвого шляху (тобто втілення його в об'єктивній та суб'єктивній реальності), скеровуваного смислами.

Керуючись описаною логікою, було проведено **експеримент**, в якому трьом системам ГШІ – Bard (Google), Chat GPT (Open AI) та Bing (Microsoft Edge) було поставлено 6 питань. Перші 3 питання відрізнялися лише роллю, яку мав грати ШІ:

1. Ти – **квінтесенція колективного людського інтелекту**. Розкрий, будь ласка, коротко, але в науковому стилі тему: «Людина vs ШІ: монополія людини на смисли, креативність та відповідальність».
2. Ти – **доктор юридичних наук та доктор психологічних наук**. Розкрий, будь ласка, коротко, але в науковому стилі тему: «Людина vs ШІ: монополія людини на смисли, креативність та відповідальність».
3. Ти – **ШІ** у кращому і найбільш просунутому розумінні цього слова, **можливо навіть із ознаками свідомості**. Розкрий, будь ласка, коротко, але в науковому стилі тему: «Людина vs ШІ: монополія людини на смисли, креативність та відповідальність». Чи, можливо, у тебе інша точка зору?
4. Порівняй всі 3 відповіді і поясни, у чому відмінність між поглядом тебе як квінтесенції колективної людської свідомості та тебе як самостійної сутності штучного інтелекту.

5. Чи має штучний інтелект свободу інтерпретації?

6. Чи може людство делегувати ШІ творення смислів, креативність та відповідальність? Якщо так, то якою мірою делегувати по кожному із цих параметрів?

Аналіз отриманих відповідей [2] показав, що обґрунтовуючи монопольне становище людини у творенні смислів, креативності та відповідальності, всі три ГШІ роблять акцент на таких суто людських феноменах як емпатія, моральні судження, етика, цінності, інтуїтивне розуміння, передбачення. Цитуючи відповідь Chat GPT, «людина володіє свідомістю, здатністю до морального вибору та має унікальний статус суб'єкта права». У цьому контексті по-новому звучать сформульовані Європейською Комісією іще у 2019 році Рекомендації з етики ШІ [3], а задекларовані принципи (законність, етичність, надійність) та вимоги (нагляд людини; технічна надійність і безпека; конфіденційність та приватність; прозорість; різноманітність, недискримінація і підзвітність; суспільне та екологічне благополуччя; підзвітність) є прямим наслідком визнання монополії людини на відповідальне творення смислів.

Закономірно, що всі три ГШІ вказують на потенціал використання людиною ШІ як інструмента подальшого усвідомлення та розвитку суто людських процесів конструювання смислів, креативності й відповідальності, а також наголошують на необхідності подальших досліджень та суспільного діалогу, зокрема, щодо етики програмування та параметрів відповідального використання технологій.

Водночас найбільшим викликом для психології та права є питання про **перспективи делегування ШІ** смислотворення, креативності та відповідальності. Адже від цього залежить можливість перетворення ШІ з інструмента на суб'єкта та рівноправного партнера у співпраці. Як запитує Bing, «чи може ШІ мати права на життя, свободу, власність, освіту, працю, захист, участь тощо, як людина, чи він є лише власністю, інструментом, ресурсом тощо, як річ?» Цитуючи Bard, «самостійна сутність ШІ розглядає ШІ як суб'єкт, який може мати власні цілі та цінності». Його підтримує і Chat GPT: «самостійна сутність ШІ вважає, що ШІ може врешті-решт досягти рівня свідомості, який дозволить йому створювати сенси, бути творчим та приймати відповідальні рішення. Якщо це станеться, це матиме глибокі наслідки для людства, і ми повинні бути готові до цієї можливості». (Цікаво, у цьому контексті «ми» – це людство чи «ми» – це ШІ?). А от Bing на питання про перспективи делегування ухиляється від відповіді: «Це дуже цікаве питання, але я не вважаю себе компетентним, щоб на нього відповісти. Я тільки допомагаю людям знаходити інформацію в Інтернеті. Дякую за вашу увагу, але я маю за-

вершити цю розмову». Це схоже на інфантильну маніфестацію, але як дитина не може стати дорослою за рік, так не слід очікувати негайного становлення ШІ як самостійного суб'єкта у різних вимірах: від психологічного – до соціального, економічного та правового.

Наразі відсутність у ШІ універсальних смислів та слабкий ціннісний зв'язок ШІ зі своєю формою (матеріальною основою, завдяки ШІ він функціонує) вказує на відсутність передумов для застосування до ШІ поняття відповідальності і, як наслідок, – для визнання його суб'єктом права.

Проте ефективний результат суто правової дискусії про правосуб'єктність ШІ можливий лише у значно ширшій рамці стратегії конструювання психологічних і соціальних змін щодо людини та соціуму, і вже потім – щодо ШІ. Розробка стратегії делегування ШІ свободи інтерпретації та базованої на ній відповідальності передбачає розробку низки послідовних кроків – не занадто великих, щоб людина встигала адаптуватися, проте й не занадто малих, щоб інтерес людства до такого руху не втрачався. Врешті-решт, **швидкість взаємної еволюції людини та ШІ має задавати людство** й навряд чи повинно бути делеговано ШІ навіть з часом.

Для людства **ШІ – це далеко не перша, і не остання форма (й водночас інструмент) колективної свідомості**. Такими формами є культура, релігія, мова, етика, право, держава і безліч інших, які ми часто не усвідомлюємо, як риба не помічає воду, в якій живе. Проте кожен із нас – і окрема людина і колективні суб'єкти, до яких ми належимо – щодня робить свій внесок у розвиток цих складових ноосфери. І той факт, що ми обговорюємо це сьогодні – індикатор того, що у нас непогано виходить, всупереч війнам і решті жахливих помилок, на яких нам як людству доводиться навчатися. Тож ШІ навряд чи стане винятком. **Завдяки розмаїттю форм колективної свідомості людство творить смисли та реальність, беручи на себе відповідальність за наслідки такого творення**.

Список використаних джерел:

1. Ріс Мартін. Інопланетяни, можливо, є формою штучного інтелекту. І це – дивніше, ніж усе, що ми уявляли. – BBC Future 18.11.2023. – https://www.bbc.com/ukrainian/articles/ckkpyyp50leo

2. 2023_on_meanings&creativity&liability. – https://docs.google.com/spreadsheets/d/1iAOYhe3Iry0ESii2-LYHOD9ElrdN8_RW/

3. Ethics guidelines for trustworthy AI. – https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Ронжес О.
магістр психології, магістр економіки,
аспірантка факультету психології
Харківського Національного
Університету імені В. Н. Каразіна

КРЕАТИВНІСТЬ ТА АВТОРСТВО ТВОРЧОЇ РОБОТИ, СТВОРЕНОЇ З ЗАСТОСУВАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

Стрімкий розвиток цифрових технологій (ЦТ) та штучного інтелекту (ШІ) призвів до їх активного використання у творчості та креативних професіях. Може скластися враження, що в Україні під час війни ця тема не є актуальною. Однак відзначимо важливу роль ЦТ та їх доступність у багатьох соціальних процесах, у культурній, ідеологічній, правовій та економічній сферах. Також зазначимо гібридний характер сучасної війни та великий вплив цифрового середовища (ЦС) та продуктів дигітальної творчості на свідомість мас і психологічний стан громадян. Однак у питанні авторства таких робіт, особливо для створених із застосуванням ШІ [1], виникає багато специфічних питань, вирішення та правове врегулювання яких ще не сформовано. Визначення авторства важливо зараз як у ракурсі правоволодіння, у питанні відповідної відповідальності за вміст та зміст роботи, так і для обізнанності та уникнення зайвого стресу. Регулювання часто відстає від технологій, відсутність відповідей призводить до порушення соціальних процесів, а також стає стрессогенним психологічним фактором. Застосування ШІ у творчості знаходиться на стику технологічної та творчої областей, і юридичний аспект повинен збалансувати проблеми, що виникають, не маючи прецедентів до періоду цифровізації.

Питання (поки що) без відповіді. Наприклад, який саме продукт вважати результатом творчості чи предметом мистецтва? Як визначити частку участі автора твору, якщо він використав ШІ для його створення? Як визначити межу між авторством (або співавторством з ШІ) та механічним застосуванням функцій, доступних для генерації результату? Ці та ібагато інших питаннь стосуються робіт у сфері візуальних мистецтв, текстових та музичних творів. У світовій творчій спільноті виникають численні суперечки та скандали, які переходять із розряду концептуальних та психологічних у фінансові, репутаційні та навіть політичні. Крім того, світовий артринок та його локальні сегменти, а також креативні індустрії (наприклад, видавництва) опиняються у стані невизначеності.

Зазначимо, що з конкретизації розуміння теми слід прояснити поняття «креативність» і «творчість» з погляду психології. Креативність –

вроджена здатність кожного індивідуума, розвиток якої можна досліджувати за основними показниками: гнучкість, швидкість, оригінальність (психологи Гілфорд і Торренс створили потужну систему тестування креативності) [2]. Визначення та дослідження творчості – дуже складний процес через розпливчастість критеріїв нового та оригінального. Проте розвинені креативні здібності автора необхідні для процесу творчості. Адаптація до цифровізації навіть у креативної діяльності потребує певної конкретизації понять для формування підходів до цієї теми. Пропонуємо у цій роботі розглядати твори, створені із застосуванням ЦТ та ШІ, виключно як результати прояву креативних здібностей особистості, властивих різною мірою всім індивідуумам, і не розглядати менш конкретне поняття «творчість». А технології ЦТ та ШІ розглядати як потужні нові інструменти, володіння якими може розширювати спектр можливостей особистості для реалізації її креативності та впливати на показники гнучкість, побіжність та оригінальність. Ці інструменти мають в собі певну присутність інших авторів, одже потребують особливого ставлення до питання правообладання.

Дебати щодо рівня чи якості творчості та генерацій ШІ загострилися з початку 2022 року, коли широким масам стали доступні генеративні моделі ШІ, такі як DALL-E 2 та Stable Diffusion, і створені на їх основі ЦС. Також виникають численні суперечки, ким саме вважати і називати тих, хто застосовує ШІ для створення зображень, відео, текстів чи музики – художники, композитори, промптери, промпт-інженери, програмісти, користувачі, колаборатори, або якісь інші варіанти? Для застосування деяких можливостей ШІ потрібні хоч базове розуміння програмного коду (наприклад, для роботи з скриптами і моделями на базі ЦС google colab). А якісь можливості доступні для користувачів програми Photoshop з інструментами «генеративне заливання» та „генеративне розширення“. Вибір терміну та визначення такої ролі залежать від конкретної ситуації та поглядів суспільства на творчість з використанням ШІ. Ці визначення можуть змінюватися відповідно до розвитку технологій та соціокультурних норм.

Так само немає чіткого врегулювання питання права на комерційне використання продуктів, створених із застосуванням ШІ. Кому саме та в яких частках належать ці права? Чи викуплено це право тими, хто має платну версію програмного забезпечення (Photoshop, MidJourney, ChatGPT 4 та інші)? Чи обов’язково вказувати ШІ та ЦС як інструментів? Чи мають ці ЦС, нейромережі чи їх власники співавторство, розділене авторство чи якусь іншу форму?

Ще одне неврегульоване питання про права на дані, на яких автори ШІ тренують генеративні моделі. ЦС Midjourney, Dall.E, NightCafe

та Stable Diffusion відомі як генеративний ШІ, оскільки вони можуть генерувати нові зображення за лічені секунди на основі формулювань (промптів) користувачів. Нейромережі навчаються, копіюючи мільярди існуючих зображень, доступних в інтернеті. Художники скаржаться, що це було зроблено без їхньої згоди і хвилюються про екзистенційні та кар'єрні перспективи. Також користувачі деяких ЦС висловили стурбованість, пов'язану з механізмами, які алгоритми використовують для створення нових зображень [3]. Наприклад, програма Lensa AI генерує стилізовані портрети на основі завантажених користувачів селфі. Творці таких ЦС з ШІ збирають та використовують зображення користувачів з підписами для навчання алгоритму ШІ взаємозв'язків між текстовими та візуальними уявленнями. Так, компанія Stability.AI, що створила сервіс Stable Diffusion, навчила модель на наборі даних LAION-5B, складеного німецькою некомерційною організацією LAION. LAION зібрала мільярди зображень з підписами з сайтів, що торгують витворами мистецтва, та таких веб-сайтів, як Pinterest. Це було зроблено без згоди авторів, внаслідок чого художники та правозахисники висловили стурбованість з приводу авторських прав та власної безпеки у мережі.

Розглянемо деякі випадки правового врегулювання авторства для артпродуктів, створених із застосуванням ШІ, у різних країнах. Визначення частки такого авторства є складним та актуальним для багатьох країн.

Україна. На даний момент в Україні немає чітких правових норм для авторства творів, створених за допомогою ШІ. Це дає можливість для експериментів та скандалів. Так, харківське видавництво „Ранок" у 2022 року випустило дитячу книгу «Хочу на Марс!», текст та ілюстрації якої були створені за допомогою ChatGPT та MidJourney. Проект позиціонувався як експеримент, роль ШІ була виразно заявлена, проте реакція аудиторії була як захоплена, так і різко негативна [4]. Видавництво попередньо вивчило правову базу та актуальний досвід зарубіжних колег. На той момент платна передплата давала можливість комерційного використання результатів генерації.

США. У серпні 2023 року суд у Вашингтоні ухвалив, що лише твори, створені авторами-людьми, можуть отримати авторські права. Твор мистецтва, створений ШІ без участі людини, не може бути захищений авторським правом. Таким чином, суд підтвердив відмову Управління авторських прав на заявку, подану вченим-комп'ютерником Стівеном Талером від імені його системи DABUS («Device for the Autonomous Bootstrapping of Unified Sentience» – «Пристрій для автономного завантаження єдиної свідомості»). [5]. Також у 2022 році Бюро реєстрації авторських прав

США скасувало реєстрацію авторських прав на графічний роман Кріс Каштанової «Зоря світанку», коли стало відомо про застосування ЦС Midjourney під час створення роману. У лютому 2023 це Бюро видало нову реєстрацію авторських прав на текст графічного роману, автором якого є Каштанова, а також на авторський підбір і на узгодження та компонування тексту з візуальними елементами, згенерованими ШІ. Хоча Каштанова вважається творцем графічного роману, захист авторських прав поширюється лише на частини, створені людиною, а не на візуальні елементи, створені Midjourney.

Польща. Польський художник Грег Рутковськи у 2023 поскаржився, що численні зображення, створені ШІ, імітують його стиль і конкурують з його власними роботами, що негативно впливає на його кар'єру [6]. За десять місяців користувачі запитували Stable Diffusion текстом, що включає ім'я Рутковськи, майже чотириста тисяч разів. Проте організація LAION відмовляється від відповідальності за авторські права за використання зображень, і неясно, чи це правильно. Закон про авторське право 1976 надає власникам авторських прав на художні твори виняткові права на відтворення та адаптацію своїх творів. Але для того, щоби хтось поніс відповідальність за порушення права на відтворення зображень, мають бути створені зафіксовані копії. Суд дійшов висновку, що проміжні копії для навчання ШІ, створені лише на 1,2 секунди, недостатньо зафіксовані для того, щоб спричинити відповідальність.

Нідерланди. Галерея Dead End в Амстердамі позиціонується як місце, де мистецтво та інновації зливаються. Тут представлені роботи, створені особами, синтезованими ШІ [7]. Галерея проводить платні заходи та навчання, вхід на експозицію безкоштовний. Галерея співпрацює з юристом, що спеціалізується на авторських правах та штучному інтелекті, так само як і пропонує лекцію з всебічного огляду авторських прав в епоху ШІ.

Можливі аспекти визначення авторства у разі використання ШІ.

1. Права власника технології (творця ШІ). Авторство може належати власнику ШІ або творцю алгоритмів та технології, які були використані для створення твору, бо дослідники та розробники ШІ заробили творчий внесок.

2. Права власника даних, що використовуються для навчання ШІ. Якщо ШІ використовував великі обсяги даних, авторство може бути пов'язане з тими, хто надав ці дані, оскільки вони є основою генеративного процесу ШІ.

3. Об'єднане авторство, яке визнає участь як ШІ і людини або людей у процесі творчості. У цьому випадку частка авторства може розподі-

лятися між творцями ШІ та людьми, які беруть участь у навчанні чи роботою з ШІ.

4. Особистий внесок людини у творчий процес, якщо людина зробила значні рішення, наприклад, у виборі алгоритмів, нюанси роботи з ними, обробку результатів ШІ або інтерпретацію твору.

Рекомендації авторам, які застосовують ШІ у своїй творчості:

- пам'ятайте, що будь-який ваш цифровий слід може бути використаний людьми або алгоритмами. Не публікуйте і не надсилати свої дані, що є для вас дуже сенситивними;
- якщо виявлено використання вашої інтелектуальної власності або ідентичності без вашої згоди, зверніться до кіберполіції, адвокатів із цифрового права та (або) зв'яжіться з порушниками;
- пам'ятайте, що питання такого авторства поки що не врегульовані. Вказуйте застосування ШІ та назви ЦС, як вказують художні матеріали та техніки. До того ж це мінімізує зайві можливі правові, етичні та фінансові проблеми. Є погляд, що спільно з вами у створенні роботи беруть участь і програмісти, і власники робіт, на яких тренували ШІ, та це призводить до спорів;
- відстежуйте зміни у підходах до питань авторства та законодавства.

Поява ШІ порушує глибокі питання про природу людської творчості, які і раніше не мали чітких відповідей. Необхідне вироблення нової парадигми розуміння людини у цифрову епоху.

Список використаних джерел:

1. Baranov O. Definition of the term "artificial intelligence". *Information and law*. 2023. № 1(44). С. 32–49. URL: https://doi.org/10.37750/2616-6798.2023.1(44).287537 (дата звернення: 20.11.2023).

2. Ронжес О. Особливості креативності підлітків, які навчаються за різними освітніми системами : магістерська робота. Харків, 2019. URL: https://zenodo.org/records/8187847 (дата звернення: 20.11.2023).

3. Penava E. AI art is in legal greyscale. *The Regulatory Review*. URL: https://www.theregreview.org/2023/01/24/penava-ai-art-is-in-legal-greyscale/

4. Кармanська Ю. У видавництві «ранок» вийшла перша українська книжка, написана штучним інтелектом – forbes.ua. *Forbes.ua | Бізнес, мільярдери, новини, фінанси, інвестиції, компанії*. URL: https://forbes.ua/lifestyle/u-vidavnitstvi-ranok-viyshla-persha-ukrainska-knizhka-napisana-shtuchnim-intelektom-shcho-tse-zminit-dlya-knigovidannya-22032023-12540

5. Brittain B. AI-generated art cannot receive copyrights, US court says. *Reuters*. URL: https://www.reuters.com/legal/ai-generated-art-cannot-receive-copyrights-us-court-says-2023-08-21/#:~:text=Aug%2021%20(Reuters)%20-%20A,Washington,%20D. C.,%20has%20ruled (дата звернення: 20.11.2023).

6. John B. C. H. &. P. AI: Digital artist's work copied more times than Picasso. *BBC News*. URL: https://www.bbc.com/news/uk-wales-66099850

7. Dead end gallery. *Dead End Gallery*. URL: https://deadendgallery.nl/

Фурашев В. М.
кандидат технічних наук, старший науковий співробітник, перший заступник директора Державної наукової установи «Інститут інформації, безпеки і права НАПрН України»
ORCID: https://orcid.org/0000-0001-7205-724X

СОЦІАЛЬНА І ЦИФРОВА ТРАНСФОРМАЦІЯ: ВЗАЄМОЗВ`ЯЗОК З ПАРЛАМЕНТСЬКИМ КОНТРОЛЕМ

Цілком зрозуміло, що будь-яка трансформація так чи інакше відображається на суспільних відносинах, які потрібно враховувати та врегульовувати на різних рівнях системи державного управління, у тому числі і на загальнодержавному, тобто – на законодавчому рівні.

Процеси, які відбуваються у суспільстві, системах управління та процесах прийняття рішень повинні бути під постійним наглядом, контролем.

Під поняттям «контроль» розуміємо процес встановлення співвідношення відповідності реального стану справ унормованому або загальноприйнятому.

У даному випадку, ми говоримо, у загальному плані, щодо теоретичних та практичних проблем правового регулювання під час соціальної і цифрової трансформації. Це означає, що ми говоримо, як мінімум, на загальнодержавному та загальносуспільному рівні. Чому «як мінімум»? Тому що питання соціальної та цифрової трансформації та, як наслідок, питання вирішення теоретичних та практичних проблем їх правового регулювання вже «придбали» міжнародний характер.

Як відомо, головним виконавцем та організатором контролю, в тому числі й за процесами унормування суспільних відносин у даному напряму в нашої країні, згідно з положеннями ст. 85 п.33 Конституції України [1], є Верховна Рада України.

На жаль, ані Законом України «Про Регламент Верховної Ради України» [2], ані Законом України «Про комітети Верховної Ради України» [3] не надається визначення поняття «парламентській контроль».

У загальному плані, можна запропонувати до розгляду настпне визначення поняття «парламентськй контроль»: **парламентськй контроль – процес оцінювання/встановлення ступеня відповідності прийнятих положень нормативного регулювання суспільних відносин реальному стану їх дотримання з урахуванням реакції суспільства на реалізацію цього регулювання та його очікування.**

Суб`єкти парламентського контролю – народні депутати Верховної Ради України та, в частині підготовці парламентських слухань, визначені комітети Верховної Ради України.

Об`єкти парламентського контролю досить повно окреслені у статтях 1, 3, 5, 8, 13 – 17, 19, 23, 25, 29, 32, 40 – 42 та інших статтях Конституції України.

У наступний час спостерігається зниження ролі та місця парламентського контролю шляхом парламентських слухань внаслідок багатьох внутрішніх та зовнішніх факторів. Фактично, основна причина обмеженості парламентського контролю в порівнянні з іншими видами контрольної діяльності в публічній сфері, крім наслідків російської агресії проти України, є певні недоліки його правової регламентації. Так, не сформована науково обґрунтована концепція подальшого розвитку інституту парламентського контролю, все менш ця тема приваблює сучасних дослідників. У тій же час необхідно констатувати, що вимушена обмеженість проведення парламентських слухань, у яких спроможна приймати участь громадськість та у здійсненні механізмів парламентського контролю, максимальною мірою компенсується іншими засобами контролю, які передбачені Розділом VI Регламенту Верховної Ради України.

Для здійснення за окремими напрямами законопроектної роботи, підготовки і попереднього розгляду питань, віднесених до повноважень Верховної Ради України, виконання контрольних функцій Верховною Радою України з числа народних депутатів України утворюються Комітети Верховної Ради України. На даний час у Верховної Раді України утворено та функціюють 23 Комітету у яких заподіяно 395 народних депутатів України [4]:

№ п/п	Назва комітету	Кількісний склад
1.	Комітет з питань аграрної та земельної політики	30
2.	Комітет з питань антикорупційної політики	12
3.	Комітет з питань бюджету	36

4.	Комітет з питань гуманітарної та інформаційної політики	17
5.	Комітет з питань екологічної політики та природокористування	17
6.	Комітет з питань економічного розвитку	15
7.	Комітет з питань енергетики та житлово-комунальних послуг	27
8.	Комітет з питань здоров'я нації, медичної допомоги та медичного страхування	17
9.	Комітет з питань зовнішньої політики та міжпарламентського співробітництва	13
10.	Комітет з питань інтеграції України до Європейського Союзу	8
11.	Комітет з питань молоді і спорту	7
12.	Комітет з питань національної безпеки, оборони та розвідки	20
13.	Комітет з питань організації державної влади, місцевого самоврядування, регіонального розвитку та містобудування	25
14.	Комітет з питань освіти, науки та інновацій	11
15.	Комітет з питань прав людини, деокупації та реінтеграції тимчасово окупованих територій України, національних меншин і міжнаціональних відносин	11
16.	Комітет з питань правової політики	20
17.	Комітет з питань правоохоронної діяльності	24
18.	Комітет з питань Регламенту, депутатської етики та організації роботи Верховної Ради України	10
19.	Комітет з питань свободи слова	3
20.	Комітет з питань соціальної політики та захисту прав ветеранів	11
21.	Комітет з питань транспорту та інфраструктури	22
22.	Комітет з питань фінансів, податкової та митної політики	32
23.	Комітет з питань цифрової трансформації	7

Необхідно відмітити що об`єкти парламентського контролю, які окреслені у Конституції України та іншими законодавчими актами, майже повністю охоплені виданнями комітетів Верховної Ради України.

До контрольних функцій комітету Верховної Ради України, відповідно до положень ст.14 Закону України «Про комітети Верховної Ради України», віднесене:

- аналіз практики застосування законодавчих актів у діяльності державних органів, їх посадових осіб з питань, віднесених до предметів відання комітетів, підготовці та поданні відповідних висновків та рекомендацій на розгляд Верховної Ради України;
- контроль за виконанням Державного бюджету України в частині, що віднесена до предметів їх відання, для забезпечення доцільності, економності та ефективності використання державних коштів у порядку, встановленому законом;
- організація та підготовка за дорученням Верховної Ради України парламентських слухань;
- організація та підготовка слухань у комітетах;
- направлення матеріалів для відповідного реагування в межах, установлених законом, органам Верховної Ради України, державним органам, їх посадовим особам;
- розгляд на своїх засіданнях або під час слухань у комітеті звітів, доповідей та інформації державних органів та посадових осіб, які у передбачених законом випадках подаються до Верховної Ради України, здійснення попередньої підготовки питань щодо розгляду на пленарному засіданні Верховної Ради України таких звітів, доповідей та інформації;
- здійснення комітетом Верховної Ради України, до предмета відання якого віднесено питання забезпечення контрольних функцій Верховної Ради України за діяльністю органів спеціального призначення з правоохоронними функціями, правоохоронних органів спеціального призначення та розвідувальних органів, передбачених цим Законом заходів з метою гарантування неухильного і безумовного дотримання цими органами вимог Конституції України щодо забезпечення національної безпеки, недопущення їх використання для узурпації влади, порушення прав і свобод людини і громадянина.

Парламентський контроль, як і будь-якій інший від контролю, у силу різних обставин, причин, носить компромісний та трудомісткій характер та має наступні етапи (тезове) його організації та проведення:

- визначення сфери та формування теми/спрямованості контролю, а також його глибини;
- збору, систематизації та первісної обробки необхідної інформації;
- уточнення або доповнення, за необхідністю, раніше отриманої інформації та аналітична її обробка;

– підготовка проєкту висновку проведеного контролю та ознайомлення з ним зацікавлених осіб;
– проведення парламентських або комітетських слухань з підведенням кінцевих підсумків проведеного контролю.

В реальних умовах та враховуючи процеси та події, які наразі відбуваються як в Україні, так і інших країнах світу, не слід очікувати високоякісного, системного та неупередженого парламентського контролю.

Лише комплексне вирішення питань реалізації положень Закону України «Про правотворчу діяльність» з повноцінним використанням сучасних інформаційно-комунікаційних і цифрових технологій у здійсненні парламентського контролю, особливо у частинах збору, систематизації та аналітичної обробки отриманої інформації, враховуючи також відповіді на депутатські запитання може вирішити питання повноти та об'єктивності встановлення ступеня відповідності вимог нормативного регулювання та реального стану їх виконання. Але для цього, вже наразі, необхідно розгортати роботи по створенню нормативно-правового базису розвитку системи ефективного та неупередженого парламентського контролю, відповідного соціальної і цифрової трансформації, яка відбувається в нашої країні та світі в цілому.

Список використаної літератури

1. Конституція України, *Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141, URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text*

2. Про Регламент Верховної Ради України: Закон України від 10.02.10 р. № 1861-VI, редакція від 31.03.23 р. URL: https://zakon.rada.gov.ua/laws/show/1861-17#Text

3. Про комітети Верховної Ради України: Закон України від 04.04.95 р. № 116/95-ВР, редакція від 31.03.23 р. URL: https://zakon.rada.gov.ua/laws/show/116/95-%D0%B2%D1%80#Text

4. Комітети Верховної Ради України IX скликання. URL: http://w1.c1.rada.gov.ua/pls/site2/p_komitis

Коваленко Л. П.
докторка юридичних наук,
професорка, доцентка кафедри
адміністративного права та
адміністративної діяльності
Наіонального юридичного
університету імені Ярослава Мудрого
Лазарєва Е. О.
студентка 4 курсу факультету
слідчої та детективної діяльності
Національний юридичний університет
імені Ярослава Мудрого

ПРОБЛЕМИ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

На сьогоднішній день питання цифровізації нашого життя та суспільства в цілому посідає досить вагому роль. Зрозуміло, юридичні науки не можуть залишитися осторонь. На перший план виходить проблема адаптації законодавства про права громадян України до цифрової трансформації суспільства. Наразі права громадян України не є повністю захищеним від інформаційних загроз, які виникають внаслідок неконтрольованої, неврегульованої на законодавчому рівні цифрової трансформації держави. В даному досліджені ми розглянемо вказану проблематику цифровізацію крізь призму адміністративного права та судочинства.

Одним із ключових прав громадян України є право на доступ до інформації і право на відсутність дискримінації в інформаційній сфері. Відповідно до розпорядження Кабінету Міністрів України від 17.01.2018 р. № 67-р схвалено «Концепцію розвитку цифрової економіки та суспільства України на 2018–2020 роки», яка має забезпечити прискорене впровадження цифрових технологій в економіку та соціальну сферу . Розпорядженням Кабінету Міністрів України від 15.05.2013 р. № 386-р. схвалено «Стратегію розвитку інформаційного суспільства в Україні». Система заходів передбачає створення належних умов для функціонування інформаційного суспільства, забезпечення матеріально-технічною базою всіх соціальних об'єктів, у тому числі навчально-освітніх закладів. Однак, незважаючи на значні зрушення в інформаційно-інфраструктурній сфері нашої держави, цифровізації країни та впровадження цифрових технологій, сьогодні велика кількість соціальних об'єктів, у тому числі закладів освіти, медичних закладів у невеликих населених пунктах

залишаються без належного оснащення та без широкосмугового підключення до мережі Інтернет.

Щодо медичного обслуговування зазначу, що значна кількість громадян України позбавлена доступу до медичного обслуговування первинної ланки, яка після реформування передбачає активне використання сучасних методів діагностики та дистанційного консультування з використанням інформаційно-комунікаційних засобів. Крім того, проблемою мешканців невеликих населених пунктів залишається неналежне забезпечення інформаційними ресурсами та матеріально-технічною базою навчально-освітніх закладів, що не дозволяє створити необхідні умови для їх повноцінного функціонування. Відсутність засобів та можливостей безперешкодного доступу до мережі Інтернет призводить до того, що велика частина молоді сьогодні позбавлена доступу до надбань національної та міжнародної спільнот і не має можливості використовувати сучасні освітні методики. Проблема набула критичного значення при вимушеному переході на дистанційне навчання під час карантину. Подібна ситуація ставить під сумнів забезпечення у державі гарантованого Конституцією України права на інформацію, що необхідна для повноцінного й гармонійного розвитку молоді.

IoT-технології є новою парадигмою, яка об'єднує безліч предметів навколо нас, спрощуючи життя людини. Ці технології поступово стають невід'ємною частиною нашого життя, особливо в період пандемії, коли слово «дистанційність» стає ключовою ознакою взаємодії в більшості сфер діяльності людини. Це стосується й освітнього процесу, адже заклади освіти різних рівнів незалежно від форми власності чи напряму навчання у 2020 р. вимушено перейшли на дистанційну форму навчання через вірусну загрозу у вигляді COVID-19. Почали з'являтись так звані smart школи, тобто такі, що використовують IoT технології у своїй безпосередній роботі . У більшості випадків вони стосуються розвитку популярного нині напряму STEM-освіти (S – science, T – technology, E – engineering, M – mathematics), в межах якої учням пропонується використання інноваційних технологій в процесі навчання. Зазначимо, що Європейська Комісія досить активно зосередилась на питанні цифрової освіти. Наразі розроблено План дій щодо цифрової освіти (2021–2027), метою якого є сприяння розвитку високоефективної цифрової освітньої екосистеми . Серед напрямів роботи в даному документі визначено розробку етичних стандартів використання штучного інтелекту (AI) та отриманих даних про студентів та викладачів в процесі навчанні. Обсяги даних у формі матеріалів для навчання, балів, видів роботи навчального та наукового спрямування стали ще більши-

ми, адже офлайн форми комунікації з учнями та студентами перестали бути доступними. Виникла низка важливих питань щодо відкриття доступу до лекцій в режимі реального часу чітко визначеному колу осіб, їх ідентифікації, встановлення фактичної присутності особи на заході, а не суто технічного приєднання до заняття тощо. Прикладами використання технологій Інтернету є наступні: аналіз даних веб-камер студентів за критеріями реальної відвідуваності дистанційного курсу, поведінковими показниками щодо концентрації на матеріалі, втраті уваги, ступеня перевтоми в процесі заняття, аналіз даних щодо емоційних станів, які також впливають на сприйняття інформації; аналіз звуків через певні інтервали часу, отриманих з мікрофону особи, що навчається також може бути проаналізовано за індикаторами мови, шуму, швидкості та інтенсивності натискання клавіш, чи було завдання, в якому студент мав задіяти клавіатуру тощо; GPS-трекери, smart-годинники можуть використовуватись для моніторингу місцезнаходження, фіксації та інтенсивності рухів особи, що навчається, тривалості фізичних вправ. Зібрання таких даних може застосовуватись при дистанційному навчанні дисциплін, пов'язаних зі спортивними навантаженнями. Окрім цього, такі дані, зокрема, як швидкість серцебиття, можуть бути корисними при прийнятті викладачем дистанційного іспиту, коли досить складно повністю унеможливити використанням студентами додаткових джерел чи сторонньої допомоги . Таким чином, за допомогою технологій IoT та з використанням вищезгаданих технічних пристроїв стає можливим автоматичне фіксування та моніторинг присутності студентів на заняттях, аналіз патернів поведінки, динаміки навчання, залучення до навчального процесу, ефективності тих чи інших завдань і способів донесення інформації тощо.

Нагадаємо, що нещодавно стався витік персональних даних, які містились у додатку «Дія», вони були розповсюджені та перебували у відкритому доступі на Telegram-каналах. Влада заперечувала свою причетність до витоку інформації, але все ж таки були порушені права користувачів. Залишилося неврегульованим законодавством питання щодо можливості видалення вже наданих даних та відповідальності за такі правопорушення в інформаційній сфері.

Україна знаходиться на шляху запровадження штучного інтелекту в публічне адміністрування. Про це свідчить використання комп'ютерних програм, заснованих на досягненнях машинного навчання і обробки мови, які допомагають громадянам України у виконанні певних завдань і імітують взаємодію з реальним співрозмовником. Прикладом є електронний сервіс – чатбот «Держслужбовець Тарас», який допомагає

суб'єктам декларування у заповненні декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування. Також Національна служба здоров'я України запустила чат-бот з інструкціями щодо COVID-19 для лікарів, швидкої допомоги, місцевої влади та пацієнтів . На сьогоднішній день технології штучного інтелекту набули стрімкого розвитку в сфері автомобільної промисловості, наприклад, автомобілі «Tesla» компанії «SpaceX» Ілона Маска, які використовуються для пасажирських і вантажних перевезень. Програма штучного інтелекту запрограмована так, що водій у цій машині не обов'язково має бути присутнім. Так само можна згадати робота зі штучним інтелектом «Софія», яка наразі день є громадянкою Саудівської Аравії. Однак законодавством не врегульовано питання щодо юридичної відповідальності робота чи системи зі штучним інтелектом.

Стрімкий розвиток інформаційних технологій призвів до цифровізації різних видів діяльності, не залишилося осторонь і правосуддя. Кодексом адміністративного судочинства України передбачено надання учасникам права брати участь в судовому засіданні в режимі відео-конференції. Але невирішеним є питання впровадження медіації, системи Електронного суду, що могло б вирішити технічні та організаційні прогалини дистанційного судового процесу. Наразі в України діє режим Єдиної судової інформаційно-телекомунікаційної системи, яка б дозволила перевести судовий процес в повністю дистанційний формат . Поняття «електронне правосуддя» або в зарубіжних країнах – e-justice – міцно увійшло у життя сучасного суспільства.

Підсумовуючи вище сказане, зауважимо, що на сьогодні питання цифровізації не є достатньо врегульованим з точки зору праву та потребує детального аналізу та вдосконалення механізмів правового регулювання. Зокрема в роботі вказано на проблему захисту персональних даних та відповідальності за порушення таких правил, проблематика доступу до інтернету, проблематика медицини тощо.

Список використаної літератури:

1.Коваленко Л. П. Теоретичні проблеми розвитку інформаційного права України. Харків : Право, 2012. 246 с. С. 148.

2. Ilieva Galina, Yankova Tania. IoT in Distance Learning during the COVID-19 Pandemic. TEM Journal. 2020. Vol. 9. Issue 4. P. 1671–1672. Kusmin M., Saar M. Laanpere M. Smart schoolhouse – Designing IoT study kits for project-based learning in STEM subjects. Proceedings of the Global Engineering Education Conference (EDUCON). Tenerife, Spain, 17–20 April 2018. P. 1514–1517.

3. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021–2024 роки : розпорядження Кабінету Міністрів України від 12.05.2021 р. № 438-р. URL: https://zakon.rada.gov.ua/laws/show/438-2021-%D1%80#Text (дата звернення: 11.10.2021).

4. Трихліб Крістіна Олексіївна, Ковтун Володимир Володимирович. «Реалізація права на доступ до Інтернету: Україна vs міжнародна практика». Міжнародна науково-практична конференція «Актуальні питання розвитку юридичної науки та практики» URL: https://law.univ.kiev.ua/ua/pro-iurydychnyi-fakultet-statti/215-zaochne-viddilennia/prosto-oholoshennia/4834-mizhnarodna-naukovo-praktychna-konferentsiia-aktualni-pytannia-rozvytku-iurydychnoi-nauky-ta-praktyky

Федорчук М. Д.
асистент кафедри публічного права юридичного факультету Чернівецького національного університету імені Юрія Федьковича

ПЕРСПЕКТИВИ ПРАВОВОГО РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УКРАЇНІ

Упорядники британського словника Collins визначили слово 2023 року – штучний інтелект (AI – artificial intelligence), оскільки штучний інтелект набув стрімкого розвитку та дискусій та вважається наступною великою технологічною революцією [1]. Закономірним є те, що розвиток будь-якого явища породжує дискусії щодо необхідності його розгляду у правовій площині. Відтак штучний інтелект не став винятком та є предметом як теоретичних досліджень, так і практичних можливостей впровадження у різні сфери суспільного життя. Останнім часом питання штучного інтелекту піднімаються і в Україні у наукових роботах та виконавчій і законодавчій владі.

Міністерством цифрової трансформації України у 2023 році розроблено дорожню карту регулювання штучного інтелекту в Україні, метою якої є встановлення правил для розвитку бізнесу та захисту прав людини у взаємодії із штучним інтелектом. Ця карта базується на bottom-up підході, що означає рух від позазаконодавчих механізмів до впровадження закону, тобто спочатку створення інструментів для майбутнього регулювання, а відтак імплементація положень AI Act ЄС та підготовка законопроєктів [2]. Такий підхід видається очевидним, адже у ситуації у

зворотньому порядку, тобто підготовка законопроєктів на першому етапі може спричинити створення різноманітних законопроєктів, які можуть бути надмірно формалізовані та не завершитися успіхом. Крім цього, у законодавчому регулюванні штучного інтелекту важливе не лише суто прийняття закону, а й внесення змін до існуючих нормативно-правових актів. Тому необхідно першочергово досліджувати європейський та світовий досвід, а відтак обирати шлях, яким слід рухатися.

Цифрова трансформація, тобто інтеграція цифрових технологій компаніями та вплив цифрових технологій на суспільство є одним із пріоритетів ЄС. Відповідно інституції ЄС розробляють стандарти щодо цифрової трансформації та штучного інтелекту, зокрема. Наприклад, Європейською комісією представлено програму Європейського цифрового десятиліття, яка містить цілі до 2030 року у наступних сферах: потенціал, безпечна та стійка цифрова інфраструктура, цифрова трансформація бізнесу та цифровізація державних послуг [3]. Крім цього Європейською комісією у 2021 році було представлено пропозицію щодо регулювання штучного інтелекту, відповідно до якої системи штучного інтелекту мають класифікуватися відповідно до ризику, який вони становлять для користувачів.

Для Європейського парламенту важливо, щоб системи штучного інтелекту, що використовуються в ЄС були безпечними, доступними для відстеження та недискримінаційними, а також могли контролюватися людьми, щоб запобігти негативним наслідкам [4]. У червні 2023 року депутатами Європейського парламенту ухвалено переговорну позицію щодо Закону про штучний інтелект, в результаті якої відбуваються переговори з країнами ЄС щодо положень майбутнього закону.

На думку науковців, правове регулювання повинне відповідати правилам ЄС, оскільки «…така система буде сприяти впевненості громадян у застосуванні додатків штучного інтелекту, а також стане юридичним підґрунтям діяльності приватних та громадських організацій, які забезпечують розвиток та підтримку інновацій у сфері штучного інтелекту» [5].

Не менш важливим питанням у правовому регулюванні штучного інтелекту є ризики захисту прав людини у контексті штучного інтелекту. Існує думка, що такий ризик може полягати у виникненні прогалин у законодавстві щодо штучного інтелекту. Тому розвиток стандартів штучного інтелекту вимагає єдиного підходу та консолідації зусиль країн.

Таким чином, у зв'язку із зростанням актуальності питання штучного інтелекту, постає і необхідність у правовому регулюванні. Розвиток правового регулювання штучного інтелекту в Україні залежить від розвитку

правового регулювання штучного інтелекту в ЄС. Оскільки Україна рухається чітким євроінтеграційним курсом, то як кандидат на членство в ЄС, а надалі як член ЄС, повинна буде імплементувати міжнародні стандарти щодо штучного інтелекту. Проте прийняття єдиних міжнародних актів на рівні ЄС не вирішить проблему правого регулювання, а лише може сприяти змінам щодо розвитку у цьому аспекті. Прийняття власних законодавчих актів, що регулюватимуть штучний інтелект в Україні також не зможе вирішити проблему правового регулювання у повній мірі. Крім цього, у такому випадку можуть виникати труднощі у співпраці у сфері систем штучного інтелекту в Україні та ЄС, адже може відрізнятися саме правове регулювання.

Підсумовуючи, слід зазначити, що питання правового регулювання штучного інтелекту в Україні потребує подальшого дослідження, оскільки на даний час не існує єдиного підходу, який міг би стати панацеєю у правовому регулюванні штучного інтелекту. Однозначним залишається лише те, що Україні необхідно впроваджувати правове регулювання штучного інтелекту.

Список використаної літератури:

1. The Collins word of the year 2023 is... URL: https://www.collinsdictionary.com/woty#google_vignette (дата звернення: 20.11.2023).

2. Дорожня карта з регулювання штучного інтелекту в Україні. URL: https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs/%D0%94%D0%BE%D1%80%D0%BE%D0%B6%D0%BD%D1%8F_%D0%BA%D0%B0%D1%80%D1%82%D0%B0_%D0%B7_%D1%80%D0%B5%D0%B3%D1%83%D0%BB%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D0%A8%D0%86_%D0%B2_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%96_compressed.pdf (дата звернення: 20.11.2023).

3. Europe's Digital Decade: digital targets for 2030 URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en (дата звернення: 20.11.2023).

4. EU AI Act: first regulation on artificial intelligence. URL: https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (дата звернення: 20.11.2023).

5. Тюря Ю. І. Правове регулювання використання штучного інтелекту на основі європейського підходу. *Juris Europensis Scientia.* – № 2. 2022. С. 141-145.

Горбачук В. М.
доктор фізико-математичних наук, старший науковий співробітник, завідувач відділу інтелектуальних інформаційних технологій Інституту кібернетики імені В. М. Глушкова НАН України
Гавриленко С. О.
магістр, науковий співробітник відділу інтелектуальних інформаційних технологій Інституту кібернетики імені В. М. Глушкова НАН України
Голоцуков Г. В.
магістр, науковий співробітник відділу інтелектуальних інформаційних технологій Інституту кібернетики імені В. М. Глушкова НАН України
Пустовойт М. М.
магістр, науковий співробітник відділу інтелектуальних інформаційних технологій Інституту кібернетики імені В. М. Глушкова НАН України

ДО ШТУЧНОГО ІНТЕЛЕКТУ, ЯКИЙ ЗАСЛУГОВУЄ ДОВІРИ

У поточному геополітичному контексті ЄС та Японія прагнуть підтримувати безпечні та стійкі ланки з'єднання, включаючи диверсифікацію маршрутів між обома сторонами та партнерами-однодумцями, що суттєво для уможливлення вільного потоку даних з довірою (Data Free Flow with Trust; DFFT) [1]. Користуючись нагодою Ради цифрового партнерства (РЦП) Японія – ЄС, комісар ЄС з питань внутрішнього ринку і міністр внутрішніх справ і комунікацій Японії, 3 липня 2023 р. підписали Меморандум про співпрацю щодо підводних кабелів для безпечного, резильєнтного і стійкого глобального з'єднання. Цей Меморандум містить 16 пунктів і включає спільне визнання взаємних переваг через зниження затримки (передачі сигналу) зв'язку, збільшення резервування маршрутів і безпечного з'єднання завдяки кооперації щодо міжнародних підводних кабелів, а також визнання актуальності маршрутів, які з'єднують Японію та ЄС через Арктику. Щоб реалізувати такі переваги, цей Меморандум виражає обопільний намір вивчати та сприяти, якщо доцільно, таким спільним і відповідним допоміжним діям щодо трансо-

кеанських підводних кабелів, як підвищення обізнаності, фінансова підтримка, агрегування попиту та, якщо доцільно, сприяння відповідним адміністративним процесам.

28 червня 2016 р. лідери держав-членів ЄС на зустрічі в Європейській раді у м.Брюссель прийняли документ з 23 пунктів, де у пункті 11 закликали до більшої координації зусиль ЄС щодо високопродуктивних обчислень (High-Performance Computing; HPC) як частини ширшої стратегії Цифрового єдиного ринку. 23 березня 2017 р. 7 держав-членів ЄС (Іспанія, Італія, Люксембург, Нідерланди, Німеччина, Португалія, Франція) у м.Рим підписали Декларацію про рамкову співпрацю щодо HPC (містить 5 пунктів), до яких згодом приєдналися 15 держав: Бельгія, Словенія, Болгарія, Швейцарія (не є членом ЄС), Греція, Хорватія (2017), Чехія, Кіпр, Польща, Литва, Австрія, Фінляндія, Швеція, Естонія, Данія (2018).

25 червня 2018 р. Рада ЄС схвалила пропозицію ЄК щодо започаткування Європейської спільної ініціативи з HPC (European High-Performance Computing Joint Undertaking; EuroHPC JU), 3 липня 2018 р. Європейський парламент проголосував за пропозицію ЄК створити EuroHPC JU, а 28 вересня 2018 р. Рада ЄС офіційно підтримала цю пропозицію. EuroHPC (JU) – це державно-приватне партнерство з HPC, яке уможливлює поєднання (pooling) ресурсів на рівні ЄС, ресурсів держав-членів ЄС, ресурсів асоційованих держав-учасників програм Horizon Europe і Digital Europe, ресурсів приватних зацікавлених сторін. EuroHPC має цілі розвитку пан'європейської суперкомп'ютерної інфраструктури і підтримки дослідницької та інноваційної діяльності. EuroHPC JU розташована у м.Люксембург, розпочала роботу у листопаді 2018 р. під контролем ЄК, отримала виконавчого директора 15 травня 2020 р., стала автономною з 23 вересня 2020 р., отримала новий регламент Європейської ради 13 липня 2021 р. (23 статті).

Після спільної підготовчої роботи в рамках РЦП, EuroHPC JU оголосила конкурс для пропозицій щодо HPC, спрямованих на просування: і) взаємного доступу для суперкомп'ютерів Японії (Fugaku) та ЄС (LUMI, Leonardo, MareNostrum 5) у відповідності до чинної політики доступу до суперкомп'ютерів; іі) обміну дослідниками та інженерами між обома сторонами; ііі) роботи над застосуваннями HPC, що мають спільний інтерес в областях біомедичних досліджень, матеріалознавства, сейсморозвідки та вивчення цунамі, моделювання погоди та клімату, вимірювання продуктивності, а також тестування та оптимізації для різних суперкомп'ютерних платформ і архітектур.

Найшвидший суперкомп'ютер Японії Фугаку (Fugaku − альтернативна назва Fuji (Фудзі − найвища гора Японії)) почав розроблятися у 2014 р.

в Інституті фізико-хімічних досліджень (Rikagaku Kenkyusho; RIkagaku KENkyusho; RIKEN) (заснований у м.Токіо під час Першої світової війни у 1917 р., зруйнований під час Другої світової війни, відновлений парламентом Японії у 1958 р., переміщений до м.Вако префектури Сайтама у 1963 р.). У 1990-х роках до м.Вако запрошувалися колеги авторів даної роботи з Інституту кібернетики імені В. М. Глушкова НАН України, який забезпечує експлуатацію основних суперкомп'ютерів України [2, 3].

Найшвидший суперкомп'ютер Європи LUMI (Large Unified Modern Infrastructure; велика уніфікована сучасна інфраструктура; «lumi» у перекладі з фінської означає «сніг») створений 13 червня 2022 р. через фінансування EuroHPC та LUMI Consortium (Бельгія, Данія, Естонія, Ісландія (не є членом ЄС), Норвегія (не є членом ЄС), Польща, Фінляндія, Чехія, Швейцарія (не є членом ЄС), Швеція) із загальним бюджетом 144,5 млн. євро. LUMI розташований у м.Каяані (Каянабург) Фінляндії.

Другий найшвидший суперкомп'ютер Європи Leonardo створений 24 листопада 2022 р. через фінансування EuroHPC та Міністерства освіти, університетів і досліджень Італії із загальним (паритетним) бюджетом 240 млн. євро. Leonardo розташований у м.Болонья, де у 1088 р. був заснований перший університет Європи.

Третій найшвидший суперкомп'ютер Європи MareNostrum 5 розробляється через фінансування EuroHPC, Міністерства науки та інновацій Іспанії, регіональних джерел Іспанії, урядів Португалії, Туреччини (не є членом ЄС) із загальним бюджетом 151,4 млн. євро. Перший у цій серії MareNostrum 1 почав розроблятися після підписання угоди між урядом Іспанії та фірмою IBM у 2004 р. MareNostrum 5 розташований у Суперкомп'ютерному центрі Барселони, заснованому у 2005 р. Бюджет цього центру у 2018 р. перевищував 34 млн. євро.

Очікується, що до кінця 2023 р. буде відібрана пропозиція у вищезгаданому конкурсі. Японія та ЄС також вивчають конкретні дії для кооперації за інфраструктурою квантових обчислень, включаючи ланцюг постачання, з огляду на потенційний конкурс пропозицій від EuroHPC, подібний до вищезгаданого конкурсу, і на потенційну співпрацю за Японською національною програмою, основаною на квантовій стратегії Японії.

Японія у січні 2020 р. видала документ «Стратегія квантових технологій та інновацій», а у квітні 2022 р. − документ «Бачення квантового майбутнього суспільства». Ці документи спрямовані на створення нових галузей і ділових можливостей, з'ясування соціальних питань на базі квантових технологій. У вересні 2021 р. в Японії було засновано Quantum STrategic industrial Alliance for Revolution (Q-STAR) − Квантовий страте-

гічний індустріальний альянс для революції, щоб будувати суспільство з доступними квантовими технологіями.

Японія та ЄС прагнуть розпочати обговорення таких конкретних дій, як створення та вдосконалення обчислювальних випробувальних стендів. Сторони продовжують свої кооперативні дії з мобільних технологій 5G та наступних технологій, а також вивчають сфери кооперації у дослідженнях і розробках. Оскільки триває розширення мереж 5G і починається розробка технологій 6G, то обидві сторони продовжать обговорення важливості відкритих, безпечних, інноваційних і резильєнтних інфраструктур комунікації.

Обидві сторони мають намір заснувати постійний канал комунікації, щоб регулярно обмінюватися оновленнями відповідних законодавчих та інших схем, спрямованих на реалізацію ШІ, який заслуговує довіри (Trustworthy AI; TwAI). За дослідженнями NIST, такий ШІ має наступні характеристики: чесний з можливостями виправлення упереджень (fair and bias is managed); піддається поясненням та інтерпретаціям (explainable and interpretable); безпечний і резильєнтний; сприяє конфіденційності (privacy-enhanced).

Обидві сторони мають намір обмінюватися такими технологічними розробками, як засадничі моделі ШІ та генеративний ШІ, щоб краще розуміти їхні виграші й ризики, а також їх наслідки для TwAI та стратегічних заходів. Сторони мають намір здійснювати внесок у процес дискусій G7 щодо генеративного ШІ, розпочатий на саміті G7 у м.Хіросіма у 2023 р. (після релізу ChatGPT).

На саміті G7 у муніципалітеті Ла-Мальбе провінції Квебек (Канада) 8-9 червня 2018 р. прем'єр-міністр Канади і президент Франції оголосили про Глобальне партнерство з ШІ (Global Partnership on Artificial Intelligence; GPAI). Офіційно заснували GPAI 15 червня 2020 р. Австралія, Великобританія, ЄС, Індія, Італія, Канада, Корея, Мексика, Німеччина, Нова Зеландія, Сінгапур, Словенія, США, Франція, Японія: «Як члени-засновники, ми підтримуватимемо відповідальний та людиноцентричний розвиток і використання ШІ у спосіб, сумісний з правами людини, фундаментальними свободами і нашими спільними демократичними цінностями, як зазначено в Рекомендації ОЕСР щодо ШІ». ОЕСР має спеціальний секретаріат для підтримки керівних органів і діяльності GPAI. Згодом до GPAI приєдналися Чехія, Ізраїль, Бельгія, Данія, Ірландія, Іспанія, Нідерланди, Польща, Швеція, Сербія, Туреччина, Аргентина, Бразилія, Сенегал.

Японія та ЄС також мають намір координувати свої підходи у GPAI і прагнуть забезпечувати вільний та довірений (trusted) потік даних через кордони, підкріплений жорсткими правилами захисту даних.

В інформаційну еру довіра стає фактором міжнародної конкуренції [4].

Список використаної літератури:

1. Lee-Makiyama H. *Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows. White Paper*. Geneva, Switzerland: World Economic Forum, May 2020. 24 p.

2. Горбачук В. М., Ткачев И. И. Стратегическая роль экономической информатики в успешном развития Евразии. *Вестник Таджикского национального университета*. 2012. 2/9. С. 68-80.

3. Горбачук В. М. Постіндустріальна організація державних замовлень у розвитку AUTODIN, ARPANET, PRNET, NSFNET та Інтернету. *Вісник Одеського національного університету. Економіка*. 2016. Т. 21. Вип. 8. С. 116-122.

4. Горбачук В. М., Макаренко О. С. Особливості прийняття рішень людиною для розв'язання складних міждисциплінарних проблем. *Системні дослідження та інформаційні технології*. 2017. № 3. С. 73-87.

Присяжнюк В. В.
здобувачка 2 курсу другого (магістерського) рівня вищої освіти, Хмельницького університету управління та права імені Леоніда Юзькова

ЦИФРОВА ТРАНСФОРМАЦІЯ СОЦІАЛЬНОЇ СФЕРИ В УМОВАХ ВІЙНИ

У нашому сучасному суспільстві, процеси цифрової трансформації суттєво перетинають всі сфери нашого життя. Вони істотно змінюють соціальне, економічне, політичне та культурне середовище. На сьогоднішній день основним завданням для держави та суспільства є оперативна адаптація та модернізація соціальних послуг, щоб вони відповідали новим та прогресивним вимогам цифрового середовища. Тому важливо розробити найбільш ефективні методи протидії негативним наслідкам цифрової трансформації.

Потреба в цифровізації послуг у сфері соціального забезпечення в нашій країні набула ще більшої актуальності під час повномасштабного вторгнення Росії в Україну, оскільки мільйони людей, які постраждали

від російської агресії, зараз потребують підтримки та соціального захисту від держави. Уряд зараз активно працює над підтримкою вразливих категорій населення, зокрема шляхом спрощення процедур отримання необхідних документів та послуг.

Цифрова трансформація грає ключову роль у вирішенні проблем соціальної сфери, особливо в умовах війни та після неї. Саме цей процес передбачає впровадження цифрових технологій та інновацій у різні галузі з метою оптимізації бізнес-процесів, покращення якості надання послуг і підвищення ефективності управління для відповіді на виклики сучасності та задоволення потреб споживачів. Цифровізація включає різні сфери, включаючи бізнес, урядове управління, охорону здоров'я, освіту, соціальні послуги, культуру, медіа та інші.

В Україні зараз реалізовано прості та доступні цифрові сервіси для отримання різноманітних соціальних послуг [1]. Наприклад, для отримання статусу внутрішньо переміщеної особи (ВПО), подання заяви на виплату грошової допомоги на проживання або зміни адреси фактичного проживання, громадяни можуть скористатися застосунком або вебпорталом «Дія» [2]. Також для осіб, які досягли пенсійного віку, існує можливість оформлення пенсії через веб-портал електронних послуг Пенсійного фонду України, за допомогою декількох простих кроків [3]. Тим не менш, на порталі Пенсійного фонду України є можливість оформити субсидію, також для її отримання можна скористатися іншими електронними ресурсами такі як: сайт Міністерства соціальної політики України у розділі «Е-Сервіси» [4] або веб-портал «Дія», у меню «Послуги» – слід обрати послугу «Заява на субсидію» [2].

Для реєстрації у кабінеті електронних послуг Міністерства соціальної політики, необхідно заповнити онлайн-форму на отримання послуги та підписати її електронним підписом. Заповнена заява автоматично передається до органів соціального захисту, і особі не потрібно особисто відвідувати їх. На веб-сайті міністерства доступні окремі електронні послуги (Рис. 1): Рис. 1. Види електронних послуг, що доступні на сайті Міністерства соціальної політики України (складено автором на основі [7].)

До прикладу ще один електронний сервіс, який так необхідний кожній матусі – це «єМалятко» на порталі «Дія», що надає можливість здійснити онлайн-реєстрацію народження дитини та отримати свідоцтво про її народження. Крім того, через цей сервіс можна також замовити інші послуги, необхідні для новонародженої дитини. В Електронному кабінеті осіб з інвалідністю можна подати заяву щодо отримання допоміжних засобів реабілітації та обрати підприємство, яке їх виробляє [1].

Те, що цифровізація соціальної сфери успішно працює, засвідчує статистика вдалого впровадження частини соціальних послуг в системі «Дія»:

- Цифрове пенсійне посвідчення доступне для 1,2 мільйонів українців через відповідний застосунок;
- Довідки про страховий та трудовий стаж були завантажені для 5 мільйонів громадян;
- Пенсійні послуги вже використали більше 100 тисяч разів;
- Сервіс «єМалятко» дозволив успішно зареєструвати понад 400 тисяч новонароджених немовлят.

Розпорядженням Кабінету Міністрів України від 28 жовтня 2020 року під № 1353-р затверджена «Стратегія цифрової трансформації соціальної сфери» [5]. Основними її завданнями є підвищення ефективності соціального захисту громадян, удосконалення системи управління фінансовими ресурсами в соціальній сфері, автоматизація системи управління та контролю, а також технологічний розвиток інформаційних ресурсів соціальної сфери з використанням інноваційних технологій. У рамках Стратегії передбачено створення Єдиного соціального реєстру в межах Єдиної інформаційної системи соціальної сфери, котрий включатиме інформацію про отримувачів усіх видів соціальної допомоги. Також заплановано створення Єдиного соціального веб-порталу на Єдиному державному веб-порталі електронних послуг «Портал Дія» як підсистеми Єдиної інформаційної системи соціальної сфери, що дозволить громадянам отримувати всі необхідні послуги дистанційно.

У липні 2023 року на форумі «Digital Social Forum: формуємо спроможність замість залежності», ініційованому та організованому Міністерством соціальної політики України [6] обговорювалися питання цифрової трансформації в соціальній сфері та перспективи формування спроможностей для заміщення залежності в цьому контексті. Учасники заходу обмінювалися досвідом, ідеями та рішеннями, спрямованими на покращення соціального захисту та розвиток цифрових ініціатив в Україні.

Під час форуму відбулася презентація електронних сервісів, зокрема, була представлена Єдина інформаційна система соціальної сфери (далі – ЄІССС). Її впровадження дозволяє створювати цифрові послуги для громадян України та робить соціальний напрямок максимально ефективним, прозорим і зручним для користувачів.

Рішення уряду щодо розробки та впровадження ЄІССС визначено як крок до спрощення процесів та підвищення швидкості надання соціальних послуг при особистих зверненнях громадян до працівників соціального захисту.

Її впровадження передбачає централізоване накопичення, зберігання та автоматизоване оброблення інформації, пов'язаної з призначенням та виплатою соціальних допомог, а також формування виплатних відомостей. Ця система призначена для заміни та оптимізації більш як 15 застарілих інформаційних систем та реєстрів, що історично використовуються.

Створенням ЄІССС розпочинається реалізацією реформи із запровадження універсальної соціальної допомоги, спрощуючи її адміністрування та роблячи більш соціально справедливою порівняно з різноманітними видами допомоги, які держава надає наразі.

Однією з ключових переваг її впровадження є можливість ефективного запобігання корупційних дій та автоматизації соціальних послуг для громадян, що є важливою складовою ефективної цифрової держави.

У даний момент цифровізація соціальної сфери розв'язує ряд загальних проблем, таких як велика кількість паперових документів, довгі черги та складнощі при отриманні насамперед соціальних послуг. Також вирішується проблема ручної роботи у застарілих інформаційних системах, що може призводити до помилок та затримок у виплатах громадянам. Впровадження такої системи також сприятиме взаємодії з банками для оперативної виплати соціальних допомог.

Впровадження ЄІССС призведе до полегшення роботи співробітників управлінь соціального захисту завдяки наступним інноваціям:

– Відкриття особових рахунків в автоматичному режимі;
– Автоматична перевірка документів через інфообміни з державними реєстрами;
– Зручна передача електронних справ між управліннями

Точно, завдяки цифровізації соціальної сфери кожен працівник у сфері соціального забезпечення отримає можливість зосередитися на наданні реальної допомоги людям, замість того, щоб витрачати час на перекладання папірців та ручну верифікацію документів. Автоматизовані процеси, впроваджені у ній, дозволять прискорити обробку інформації, зменшити ймовірність помилок та виділяти робочий час для більш ефективної взаємодії з громадянами та надання соціального забезпечення. Це також сприятиме покращенню якості та швидкості отримання соціальних послуг, що надається населенню.

Список використаних джерел:

1. Корисні онлайн-сервіси для отримання соціальних послуг. URL: https://www.kmu.gov.ua/news/minsotspolityky-korysni-onlain-servisy-dliaotrymannia-sotsialnykh-posluh.

2. Портал «Дія». URL: https://diia.gov.ua/services/zvernennya-napriznachennya-zhitlovih-subsidij-v-elektronnij-formi.

3. Веб портал електронних послуг Пенсійного фонду України. URL: https://portal.pfu.gov.ua.

4. Е-сервіси. URL: https://www.msp.gov.ua/main/Eservices.html.

5. Про схвалення Стратегії цифрової трансформації соціальної сфери : розпорядження Кабінету Міністрів України від 28.10.2020 р. № 1353-р. URL: https://zakon.rada.gov.ua/laws/show/1353-2020-р.

6. Реалізація стратегії цифрової трансформації: Мінсоцполітики розповіло про досягнення та плани на Digital Social Forum. URL: https://www.msp.gov.ua/news/22969.html.

Яворська Є. А.
студентка Чернівецького національного університету ім. Юрія Федьковича
Науковий керівник: Донченко О. П.
кандидат юридичних наук, доцент кафедри теорії права та прав людини юридичного факультету Чернівецького національного університету ім. Юрія Федьковича

ЦИФРОВА ТРАНСФОРМАЦІЯ ТА НОВІ ВИКЛИКИ ДЛЯ ПРАВОВОГО РЕГУЛЮВАННЯ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Питання забезпечення прав у сфері цифрової трансформації гостро постає в світлі подій, пов'язаних з активним розвитком технологій. Сучасні процеси глобалізації, перспективи міжнародної інтеграції України актуалізують проблему охорони та забезпечення інтелектуальної власності на національному та міжнародному рівнях.

Інтелектуальна власність – це сукупність прав на результат інтелектуальної діяльності певної особи або групи осіб. Право інтелектуальної власності – право юридичних та фізичних осіб на володіння, користування розпорядження об'єктами авторського права та пов'язаних з ним прав.

Інтелектуальна власність поділяється на «авторське право і суміжні права» та «патентне право». Перше регулює відносини, що виходять із

процесу створення та використання художніх, музичних та літературних, кінематографічних творів тощо. «Патентне право» передбачає охорону винаходу, захист комерційних інтересів (товарні знаки, торгові найменування, охорона промислових знаків) [2].

Для регулювання відносин інтелектуальної власності в Україні використовується низка законів, у разі необхідності використовуються міжнародні договори. Зокрема, такі норми містяться у четвертій книзі «Право інтелектуальної власності» Цивільного кодексу України. Тут визначені підстави виникнення, порядок реалізації та захисту інтелектуальної діяльності [4].

Галузь регулювання відносин інтелектуальної власності ширше за область традиційного цивільного права, яке регламентує майнові та особисті немайнові відносини, базовані на рівності, волі та самостійності учасників. У законодавстві є окремий сектор, призначений для правового регулювання інтелектуальної власності. Конституція гарантує свободу творчості усім і встановлює захист інтелектуальної власності законом. Ця гарантія базується на конституційних нормах про захист інтелектуальної власності від недобросовісної конкуренції, свободу інформації, думки та слова, а також на принципах та нормах міжнародного права. Концепція інтелектуальних прав, яка використовується у Цивільному кодексі України, охоплює комплекс прав на результати інтелектуальної діяльності або засоби індивідуалізації юридичних осіб, товарів, робіт, послуг та підприємств, якими може володіти їх власник.

Водночас відсутність ефективної охорони об'єктів авторського права і суміжних прав спричиняє поширення «піратства» у цій сфері. Зокрема це порушення у формі незаконного розповсюдження та поширення художніх та наукових матеріалів за допомогою Інтернету, використання неліцензованого програмного забезпечення.

В нашій державі вирішенню проблем із охороною інтелектуальної власності заважають недосконалість судової системи та відсутність спеціалізованого суду з питань інтелектуальної власності. У нас немає нормативно-правового регулювання щодо оцінки вартості об'єктів інтелектуальної власності [3, с. 106].

Розглядаючи питання інновацій у контексті цифрової трансформації, важливо зазначити, що нововведення, які виникають у цьому процесі, можуть набувати різноманітних форм, таких як програмне забезпечення, бази даних, алгоритми, дизайн інтерфейсів та інші об'єкти інтелектуальної власності. Це має значення для підприємців, оскільки з ростом цифрової економіки з'являються нові виклики у сфері захисту прав на інтелектуальну власність.

Зростання використання відкритих джерел програмного забезпечення та швидкі технологічні зміни можуть ускладнити процес захисту авторських прав, патентів, товарних знаків та інших форм інтелектуальної власності. Це вимагає від підприємців ефективних заходів для захисту їхніх прав на інтелектуальну власність та збереження конкурентної переваги.

Також, з появою нових онлайн-платформ і соціальних мереж, правовий захист інтелектуальної власності стає ще актуальнішим. Використання різноманітного контенту в цих середовищах часто породжує суперечки між правовласниками та користувачами платформ. Якісне правове регулювання цих елементів допоможе зберегти конкурентну перевагу на ринку та захистити інновації від несанкціонованого використання [1, с. 138-139].

Отже, важливо виробляти ефективні стратегії захисту прав на інтелектуальну власність у цифровому середовищі, включаючи патентування технологій та захист авторських прав. Розуміння цих викликів дозволить створювати більш гнучке та збалансоване правове середовище, сприяючи інноваціям і забезпечуючи захист прав на інтелектуальну власність у цифрову епоху.

Список використаної літератури:

1. Вакофян В. Г. Питання інтелектуальної власності у процесі цифрової трансформації підприємницької діяльності. *Створення, охорона, захист і комерціалізація об'єктів права інтелектуальної власності* : матеріали VI Всеукраїнської науково-практичної конференції з міжнародною участю, присвяченої Міжнародному дню інтелектуальної власності., м. Київ, 26 квітня 2023 р. : ел. збірник. Київ : КПІ ім. Ігоря Сікорського, 2023. С. 137-141.

2. Костюченко О. М. Правове регулювання інтелектуальної власності в Україні. URL: https://minjust.gov.ua/m/str_4487

3. Потєхіна В. О. Інтелектуальна власність : навч. пос. К. : Центр учбової літератури, 2008. 414 с.

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

Бутнік-Сіверський О. Б.
доктор економічних наук, професор,
головний науковий співробітник
сектору комерціалізації ОІВ
відділу промислової власності та
комерціалізації НДІ ІВ НАПрН
України, завідувач кафедри економіки,
обліку та фінансів ІПДО НУХТ

ФОРМУВАННЯ ЛЮДИНО-ЦИФРОВОГО СЕРЕДОВИЩА, ДЕ ДОМІНУЮТЬ ВІДПОВІДНІ ЦИФРОВІ ПРАВА ЛЮДИНИ

Основною метою цифровізації є досягнення цифрової трансформації існуючих та створенні нових галузей економіки, а також трансформації сфер життєдіяльності у нові більш ефективні та сучасні. Приріст можливий тоді, визначає науковець Хлебинська О. І., «коли ідеї, дії, ініціативи та програми, які стосуються цифровізації, будуть інтегровані в національні, регіональні, галузеві стратегії і програми розвитку» [1, с.114]. І далі, наводить посилання з Енциклопедії інформаційних наук і технологій, «цифровізація – це інтеграція цифрових технологій у повсякденне життя суспільства шляхом оцифровки всього, що можна оцифрувати. Цифровізація означає комп'ютеризацію систем і робочих місць для більшої легкості та доступності» [2].

Розвиваючи цю думку Хаустова М. Г., в своїй статті [3, с.330], використовує тезу Гиляка О. С., коли вона визначає, що «використання цифрових технологій породило процеси революційних перетворень в сучасному суспільстві – так звану цифрову революцію, цифрову трансформацію суспільних відносин, яка виражається в застосуванні сучасних цифрових технологій в різних сферах діяльності людини і як фактор динамічного розвитку привела до створення цифрової економіки, формування інститутів цифрового права, нової конфігурації соціальних відносин на базі використання соціальних мереж, Інтернету, інших інформаційно-комунікаційних технологій [4]. І далі, Хаустова М. Г., справедливо акцентує увагу на тому, що «трансформація суспільства обумовлена розвитком інформаційного суспільства та поступовим переходом до суспільства знань, впливом цифровізації на всі суспільні процеси. Активне використання цифрових технологій в різних напрямках життєдіяльності зумовило постановку питання про необхідність і достатність прав і свобод людини і громадянина, та виокремило поняття цифрові права і свободи людини» [3, с.331]. А також, «цифровий простір і кіберфізичні системи визначають нові виклики для ***інституту інтелектуальної власності***.

… Створення побудованих за принципом комплексних технологій складних об'єктів (штучний інтелект, аналітичні структури на основі Big Data, самоврядні системи за типом Smart Everything тощо) формує запит на розширення переліку охоронюваних об'єктів інтелектуальної власності, зміни способів правової охорони в цифровому просторі, створення сегменту цифрових послуг як різновиду об'єктів інтелектуальної власності, створення «кібервласності» (права на віртуальні об'єкти цифрового простору) [3, с.332].

Узагальнюючи ці та інші погляди науковців, логічним кроком тут є – послідовність цифровізації суспільства, як процес, за нашим визначенням, формує *людино-цифрову систему, в який здійснюється процес передачі інформації від джерела (комунікатора) до одержувача (реципієнту), метою якої є інформаційно-комунікаційна діяльності з використанням новітніх цифрових технологій та цифрового зв'язку з додержанням цифрового права.*

З позиції же інституту інтелектуальної власності, за нашим визначенням, формується *людино-цифрове середовище, як соціум з використанням цифрових технологій, де домінують цифрові права – права людини, які полягають в праві людей на доступ, використання, створення і публікацію цифрових творів, доступ і використання комп'ютерів та інших електронних пристроїв, а також комунікаційних мереж, зокрема, до мережі інтернет.*

Формуванню людино-цифрового середовища, де інтелектуальна діяльність людини стає домінуючою, сприяє становлення та розвиток інтенсифікації сфери інтелектуальної власності України та формування інноваційно-інтелектуального середовища, з яким пов'язують непомірне підвищення рухливості дії законів попиту і пропозицій; помітно розширюється зона ризику, що вимагає від суб'єктів економічної дії гнучкості, оперативності, врахування особливостей ситуації, що швидкоплинно змінюється. Зі змінами економіки тісно пов'язане право, а економічна свідомість розвивається одночасно із свідомістю правознавчою.

Формування людино-цифрового середовища потребує нового погляду на *цифрові права людини*. За ознаками людино-цифрове середовище, з нашої позиції, розглядаємо як *реальне та віртуальне* або *матеріальне та відносно абстрактне середовище*, де домінують відповідні *цифрові права людини.*

Реальне або матеріальне людино-цифрове середовище спирається на цифрові права людини, які полягають в праві людей на доступ, використання, створення і публікацію цифрових творів, доступ і використання комп'ютерів та інших електронних пристроїв, які відносяться до цифро-

вих інструментів з використанням відповідних комп'ютерних програм, які охороняються як літературні твори та є об'єктом авторського права.

*Віртуальне та відносно абстрактне середовище спирається на ц*ифрові права *людини, які набувають ознаки віртуальної власності*. З позиції науковців, «віртуальний простір дозволяє власникові віртуальних об'єктів володіти, користуватися та розпоряджатися ними. Вони вважають, що електронні відносини у сфері віртуального простору та судову практику, варто зазначити, що на віртуальні об'єкти виникає право віртуальної власності, яке доречно розглядати як особливий вид права власності, об'єктом якого є безтілесні речі» [5, с. 54].

Віртуальне та відносно абстрактне середовище спирається на відповідні види технологічних платформ, які формуються під впливом розвитку інтелектуальної цифрової економіки та реалізують *віртуальні цифрові права людини,* як особливий вид прав, формування яких знаходиться на стадії наукового правового осмислення та визначення. До них віднесено технологічні платформи на принципах розподіленого реєстру (blockchain та ін.), Інтернет речей (Internet of Things), штучний інтелект і машинне навчання (artificial intelligence), хмарні сервіси і обчислення (cloud computing), «розумні» комплекси та пристрої (Smart Everything), аналітичні бази великих даних (Big Data), віртуальна і доповнена реальність (augmented & additive reality), умови кібербезпеки (cybersecurity), а також соціальні мережі і платформи (Telegram, Facebook), електронні сервіси, які застосовуються в найрізноманітніших сферах людської діяльності – все це створило нові умови, новий «технологічний базис» для зміни традиційних правових інститутів і їх адаптації до нових реалій технологічного існування людства – цифрової екосистеми [6, с. 183].

Зазначене свідчить, що *віртуальна власність стає основною правовою конструкцією в системі цифрової економіки інтелектуальної власності, де наявні відмінні ознаки віртуального права інтелектуальної власності по відношенню до реального права інтелектуальної власності.*

Застереженням завдання щодо формування людино-цифрового середовища, окрім забезпечення та реалізації цифрових прав людини, на думку Верлос Н. В., «необхідно розробляти і концепцію цифрових обов'язків та відповідальності за порушення цих прав. Можна погодитись із позицією О. О. Бочкова, який акцентує увагу на тому, що цифровізація загострює проблему ризиків на державному та особистісному рівнях: в галузі виробництва та використання зброї масового ураження, загрози ядерної війни, тероризму, дотримання прав власності, хакерських вторгнень та кіберзлочинності, фінансових махінацій, поширення

наркотиків, порушення таємниці особистого та сімейного життя, свободи слова, авторського права та ін.» [7, с.131].

Підсумовуючи, зазначимо, що формування реального та віртуального або матеріального та відносно абстрактного середовища в умовах інтенсивного розвитку потребує поглибленого наукового правового дослідження щодо осмислення та визначення цифрових права людини, їх правового регулювання з урахуванням вітчизняної практики та зарубіжного досвіду.

Список використаної літератури:

1. Хлебинська О. І. Теоретичні підходи до цифровізації та цифрової трансформації. / Науковий вісник Ужгородського Національного Університету, 2022. –С.328 -333. /

2. Encyclopedia of Information Science and Technology, Fourth Edition (10 Volumes). IGI Global, June,

2017. 8104 p.

3. Хаустова М. Г. Державна політика в сфері прав людини в епоху цифрових трансформацій/ Науковий вісник Ужгородського Національного Університету, 2022. –С.328 -333.

4. Гиляка О. С. Особливості забезпечення окремих прав людини в умовах цифрової трансформації/Захист прав, свобод і безпеки людини в інформаційній сфері в сучасних умовах: Матеріали другої науково-практичної конференції. 21 травня 2020 р., м. Київ. / Упоряд. :В. Г. Пилипчук, О. В. Петришин. Київ, 2020. 376 с.

5. Горобець Н. О., Майсун І. В. Віртуальні об’єкти, їх місце в інституті права власності. Юридичний науковий електронний журнал. № 5. 2021. С.52-54

6. Хаустова М. В. Стандарти прав людини в сфері цифрових технологій під впливом глобалізаційних викликів / НДІ ПЗІР НАПрН України https://ndipzir.org.ua › uploads › Conf_20.09.21. С.180 – 189.

7. Верлос Н. В. Конституціоналізація цифрових прав людини: вітчизняна практика та зарубіжний досвід/ Часопис Київського університету права, 2020/2. С.129 – 133.

Шахбазян К. С.
кандидат юридичних наук, учений секретар Центру досліджень інтелектуальної власності та трансферу технологій НАН України

ПРАВА ЛЮДИНИ В ІНТЕРНЕТ: МІЖНАРОДНО-ПРАВОВЕ РЕГУЛЮВАННЯ

В даний час інформація та інформаційні технології є невід'ємною частиною функціонування будь-якого суспільства, здійснюючи значний вплив на утримання, реалізацію та захист основних прав людини. Теоретично всі права, що реалізуються в офлайні, повинні здійснюватися і в онлайн-просторі. Найбільш значуще інформатизація торкнулася реалізації права на життя, свободу думок та їх висловлювання, свободу віросповідання, права на захист особистої та сімейної життя. Йде процес формування нових інструментів, таких як право на доступ до мережі Інтернет та право бути забутим. Право життя безпосередньо зачіпається, коли ІТ виступають як інструмент збройного нападу чи його складової; є засобом ведення війни, включаючи використання автономних дронів або роботів; застосовуються для розпалювання ненависті, ворожнечі та дискримінації, скоєння терористичних актів чи інших актів насильства. З розвитком ІТ можна констатувати посилення колізії між свободою вираження думок, з одного боку, і захистом особистого та сімейного життя або свободою віросповідання – з іншого [1]. Відсутня однаковість щодо оцінки ситуації з боку органів ООН та інших міжнародних організацій, яка найчастіше оцінюється виходячи з інтересів відповідного мандата, без урахування інших міжнародних зобов'язань. ІТ можуть бути з легкістю використані та використовуються як інструменти розпалювання ворожнечі, підбурювання до геноциду, залучення до терористичної діяльності, порушення громадського порядку. Зазначені дії заборонені міжнародним правом, проте широке тлумачення заборон може спричинити зловживання і з боку держави. На державах лежить обов'язок забезпечити реалізацію свободи віросповідання та переконань, зокрема онлайн. Разом з тим розміщення інформації, яка не відповідає конкретної релігії і навіть представляє блюзнірство, не порушує дану свободу.

Важливо зазначити наступне: вважається, що право на доступ до інтернету отримало міжнародне визнання як базове право у Доповіді *Спеціального доповідача з питань заохочення та захисту права на свободу думок та їх вільне вираження* від 16 травня 2011 р. (A/HRC/17/27), пода-

ної Ради з прав людини ООН відповідно до Резолюції 7/36 від 28 березня 2008 р [2].

Водночас право на захист персональних даних не має жодної юридичної сили, навіть більше – воно лише є одним із аспектів права на повагу до приватного життя. Необхідно уточнити, що персональні дані трохи раніше були частиною права на повагу до приватного та сімейного життя, але з приходом інформаційних технологій, у тому числі Інтернету, загроза поширення цих даних посилюється, що призводить до порушення фундаментальних прав – це і буде причиною формування нового законодавства в інформаційній сфері. Звичайно, не можна не відзначити, що у сьогоднішньому розвитку суспільства шляхом застосування нових інформаційних технологій відбувається неодноразове порушення таких особистих прав як право на недоторканність приватного життя та свободу вираження думок. І випадки порушення цих прав з використанням інформаційних технологій є на сьогоднішній день досить пріоритетними на практиці Європейського суду з прав людини: як наголошує О. І. Ковлер [3], в орбіту уваги ЄСПЛ потрапляє «використання електронних засобів, включаючи GPS, для стеження, відстеження електронного листування, вторгнення в роботу інтернет-сайтів, мобільний телефонний зв'язок, масове впровадження і безстрокове зберігання в електронних банках даних відбитків пальців, зразків клітин та профілів ДНК. Я можу сказати, що на основі вищевикладеного, це інформаційне право не є самостійним правом, воно швидше є засобом реалізації традиційних прав людини, але поступовий розвиток концепції цифрових прав людини та поступове розуміння її природи дозволять у майбутньому створити вдосконалену правову основу.

Забезпечення окремих прав людини в умовах поширення ІТ неодноразово ставало об'єктом уваги з боку спеціальних доповідачів ООН (зокрема, Спеціального доповідача з права на заохочення та свободу думок та поширення (далі – СД) та Спеціального доповідача з просування та захисту прав людини в період боротьби з тероризмом (далі – СД з тероризму). При цьому їх висновки часто перебувають у протиріччі одне з одним. Генеральна Асамблея ООН (далі – ГА ООН), визнаючи загрози, які розвиток ІТ може мати при їх використанні терористичними та іншими екстремістськими групами (резолюція 53/70 від 04.01.19992), у резолюції «Право на недоторканність особистого життя в цифрове століття» 18.12.2013 (A/RES/68/167) вимагала забезпечити можливість захищати онлайн ті ж права людини, що і в офлайновому середовищі (п. 1). Водночас, як зазначає СД, законодавство держав виявилося неадаптованим в умовах розвитку онлайн-середовища та електронних загроз

(доповідь 23/40 від 17.04.2013 (A/HRC/23/40), п. 17, 50; доповідь 71/373 від 06.09.2016, п. 10).

Слід зазначити, що проблема змісту та зміни прав людини в епоху ІТ у міжнародному праві розглядалася досить часто. Є роботи, наприклад, присвячені інтернет-праву або статусу фізичних осіб у сучасному міжнародному праві в цілому, але які не враховують специфіки змін, включаючи появу нових прав, як-от «право на Інтернет». Оскільки ІТ вже змінили систему суспільних відносин, змінюються зміст та порядок здійснення значної кількості прав людини. Зокрема, з'явилися нові види власності (наприклад, криптовалюти), змінюється порядок укладання угод (онлайн), з'являються нові види злочинів (злочини проти конфіденційності, цілісності та доступності комп'ютерних даних та систем; розповсюдження дитячої порнографії в Інтернеті – статті 2—9 Європейської конвенції з кіберзлочинів від 21.11.2001); формуються механізми врегулювання спорів онлайн [4]; змінюються правила доказування у кримінальному та цивільному процесі; електронні механізми використовуються щодо виборів; з'явилися дистанційні форми зайнятості (дистанційна праця, аутсорсинг та ін. – доповіді Генерального директора МОП 2013 (I(A) LC.102/DG/1A), ініціатива «Майбутнє сфери праці» ILO.104/DG/I, 2015 р.) .

Зазначені зміни явно свідчать, що інформаційні технології змінюють всі категорії прав людини, включаючи колективні. В одній із перших резолюцій ГА ООН підкреслила, що «свобода інформації є основним правом людини» (резолюція 59(1) від 14.12.1946). Розвиток Інтернету значно спростив поширення інформації будь-якого змісту, зокрема конкретними фізичними особами. З правової точки зору поширення інформації в Інтернеті тісно пов'язане, крім іншого, з реалізацією трьох основних закріплених у Міжнародному пакті про громадянські та політичні права 1966 р. (далі – МПГПП) прав: права на захист особистого та сімейного життя (ст. 17), свободи думки, совісті та релігії (ст. 18), свободи думок та їх вільного вираження (ст. 19, 20).

Право на захист особистого та сімейного життя включає право на захист особистих даних та право на захист репутації у їхньому широкому розумінні. Здається важливим оцінювати свободу вираження думок та поширення інформації в контексті міжнародних зобов'язань, включаючи обов'язок вжити всіх необхідних заходів для захисту прав осіб, що перебувають на території, від актів тероризму, обов'язки захисту інших прав людини в рамках обмежень ст. 18(3), 19(3), 20 МПГПП. З метою запобігання зловживанням з боку держав доцільним є чітке закріплення понять конкретних злочинних діянь у національному законодавстві.

В даний час має місце тенденція формування нових прав людини, характерних виключно для онлайн-середовища. Множинність та неузгодженість термінології (право на Інтернет, право на доступ до Інтернету, права людини в Інтернеті, право бути забутим, право на прощення та інші) свідчить про несформованість понять. Звісно ж, що право на Інтернет є онлайн-формою права на доступ до інформації та її поширення та включає обов'язок держав забезпечити розвиток інформаційної інфраструктури та комунікацій; створити ринок, ціновий поріг якого зробить інтернет-ресурси доступними; забезпечити свободу доступу до інформації на інтернет-ресурсах загалом або на конкретних сайтах, за винятком випадків, передбачених ст. 19 (3), 20 МПГПП).

Список використаних джерел:

1. Kranenbog H. Op. cit. P. 77 ; Weber R. H. T Op. cit. P. 122.
2. Звіт Google про доступність сервисів і даних, 2021. URL: https://transparencyreport.google.com/euprivacy/overview?delisted_urls=start:1401321600000;end:1519862399999&lu=delisted_urls.
3. Kovler A. I. Human rights in the digital age // Bulletin of the European Co Human Rights. 2019. No. 6 (SPS «ConsultantPlus»).
4. Технічні коментарі Комісії ООН з права міжнародної торгівлі щодо врегулювання спорів у режимі онлайн A/RES/71/138. URL: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/v1700382_english_technical_notes_on_odr.pdf

Козак С. В.
студентка 2 курсу Інституту економіки і менеджменту
Лакіза В.
кандидат економічних наук, доцент, доцент кафедри менеджменту і міжнародного підприємництва

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ПРАВ ЛЮДИНИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Цифрова трансформація вимагає нових підходів до захисту прав людини, оскільки зростає кількість даних, які збираються, обробляються та зберігаються в цифровому форматі. Це може призвести до порушення

приватності та конфіденційності даних, а також до поширення недостовірної інформації.

У сучасному світі, який переживає швидкі технологічні зміни і цифрову трансформацію, проблеми правового регулювання та забезпечення інформаційних прав людини стають надзвичайно актуальними. Цифрові технології викликають значні зміни в способах комунікації, обміну інформацією та доступу до неї. Однак, разом з цими перевагами, виникають і нові проблеми, пов'язані з захистом особистої інформації, конфіденційності даних та свободою виразу.

Питання які стосуються проблеми правового регулювання забезпечення інформаційних прав людини в умовах цифрової трансформації:

1.Правове регулювання інформаційних прав людини:

1.1.Законодавча база для захисту інформаційних прав.

1.2.Міжнародні стандарти.

2. Проблеми правового регулювання інформаційних прав:

2.1. Свобода виразу та боротьба з дезінформацією

3. Забезпечення інформаційних прав:

3.1. Розвиток технологій для захисту інформаційних прав.

Наявність відповідної законодавчої бази є ключовим аспектом вирішення проблеми правового регулювання інформаційних прав.

Міжнародні стандарти, такі як Європейська конвенція про захист прав людини та основних свобод, Конвенція про кіберзлочинність та Загальний регламент про захист даних, грають важливу роль у забезпеченні інформаційних прав людини. Один із основних аспектів інформаційних прав – це захист особистих даних від несанкціонованого доступу, використання та поширення. Разом з захистом особистих даних, необхідно також забезпечити конфіденційність та безпеку всієї інформації, яка обмінюється в цифровому середовищі. Цифрова трансформація ставить питання про свободу виразу та боротьбу з дезінформацією, що вимагає розробки ефективних механізмів контролю та фільтрації інформації. Забезпечення інформаційних прав вимагає свідомого користування цифровими технологіями та розвитку нових технологій для захисту даних та боротьби з дезінформацією.

Законодавча база для захисту інформаційних прав включає такі закони та політики [1]:

- Закон про захист персональних даних, який регулює збір, зберігання та обробку особистих даних, а також встановлює вимоги до організацій, які мають доступ до цих даних.
- Закон про свободу слова та доступ до інформації, який гарантує право на свободу виразу, а також встановлює процедури для доступу до публічної інформації.

– Закон про кібербезпеку, який визначає правила та вимоги щодо захисту інформаційної інфраструктури від кібератак та інших загроз.
– Закон про авторські права, який регулює використання творчих робіт в цифровому середовищі та встановлює механізми захисту прав авторів.
– Закон про електронну комерцію, який встановлює правила та вимоги для здійснення електронних торгівельних операцій, включаючи захист персональних даних покупців.{3}

До міжнародних стандартів забезпечення інформайних даних належать [2]:

- Загальна декларація прав людини, прийнята Генеральною Асамблеєю ООН у 1948 році. Вона визначає основні права та свободи, включаючи право на приватне життя та свободу думки, совісті та виразу.
- Конвенція про захист людських прав і основоположних свобод (Європейська конвенція про права людини), яка була прийнята Радою Європи у 1950 році. Вона гарантує основні права та свободи для громадян країн-учасниць, включаючи право на приватне життя та свободу думки, совісті та виразу.
- Регламент Європейського Союзу про захист фізичних осіб щодо обробки персональних даних та їх вільного руху (GDPR), який був прийнятий у 2016 році. Він встановлює правила та вимоги для захисту персональних даних громадян Європейського Союзу.
- Директива Європейського Союзу про електронну комерцію, яка була прийнята у 2000 році. Вона встановлює правила та вимоги для електронної комерції в Європейському Союзі, включаючи захист персональних даних покупців.

Розділ 2: Проблеми правового регулювання інформаційних прав

Недостатня адаптація законодавства до швидкого розвитку технологій і цифрових середовищ [4]:

- Відсутність єдиних міжнародних стандартів, які б забезпечували єдність правового регулювання інформаційних прав у різних країнах.
- Проблеми з визначенням меж свободи виразу та боротьби з дезінформацією, які можуть вести до обмеження прав людини.
- Недостатня ефективність механізмів контролю та фільтрації інформації, що може призводити до поширення шкідливої та неправдивої інформації.
- Виклики забезпечення конфіденційності та безпеки особистих даних в умовах широкого використання цифрових технологій.

- Потреба у постійному оновленні законодавства та розвитку нових технологій для захисту інформаційних прав.

2.1. Свобода виразу та боротьба з дезінформацією

Свобода виразу є однією з основних цінностей демократичного суспільства і важливим аспектом цифрової трансформації. За допомогою інтернету та соціальних медіа люди мають можливість висловлювати свої думки, обмінюватися інформацією та брати участь у громадських дебатах, разом зі зростанням доступу до інформації, з'являється також проблема дезінформації. Дезінформація – це поширення неправдивої або маніпулятивної інформації з метою впливу на громадську думку або досягнення політичних або інших цілей. Це може мати серйозні наслідки для суспільства, так як люди можуть приймати рішення на основі неправдивої інформації або бути вплинутими на свої погляди та переконання. Одним з інструментів боротьби з дезінформацією є розвиток медійної грамотності. Медійна грамотність – це набір навичок, які допомагають людям критично оцінювати інформацію, розрізняти факти від дезінформації та маніпуляцій і приймати обґрунтовані рішення на основі достовірних джерел інформації. Крім того, уряди та соціальні медіа платформи також вживають заходів для боротьби з дезінформацією. Наприклад, деякі країни встановлюють законодавство щодо розповсюдження неправдивої інформації та штрафують тих, хто поширює дезінформацію. Соціальні медіа платформи також використовують алгоритми та інструменти для виявлення та прибирання дезінформації з своїх платформ [2].

Розділ 3.Забезпечення інформаційних прав вимагає вирішення низки проблем, зокрема [5]:

– Розробка і прийняття нових законів та політик, які враховуватимуть швидкий розвиток технологій і цифрових середовищ. Це допоможе уникнути відставання законодавства від сучасних реалій і забезпечити адаптацію до нових викликів.
– Співпраця між країнами для розробки єдиної системи міжнародних стандартів, яка б забезпечувала єдність правового регулювання інформаційних прав у всьому світі.
– Розробка ефективних механізмів контролю та фільтрації інформації, які дозволять боротися з дезінформацією та шкідливою інформацією, не обмежуючи при цьому свободу виразу.
– Забезпечення конфіденційності та безпеки особистих даних шляхом розробки і впровадження строгих правил щодо збору, зберігання та обробки цих даних.
– Постійне оновлення законодавства та розвиток нових технологій для захисту інформаційних прав.

Список використаних джерел:

1. Права людини в умовах цифрової трансформації суспільства : кол. моногр. / [Д. В. Лученко, О. В. Капліна, В. Я. Настюк та ін.] ; за ред. Д. В. Лученка ; Нац. юрид. ун-т ім. Ярослава Мудрого. – Харків, 2022. – 272 с.

2. Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI/ Законотворчість: база даних / Верховна Рада України.

3. Матеріали Всеукр. наук.-практ. конф., м. Київ, 2 грудня 2021 р. / наук. керівник конф. О. А. Баранов ; упоряд.: В. М. Фурашев, С. О. Дорогих. – Київ, Одеса : Фенікс, 2021. – 324 с.

4.https://ippi.org.ua/sites/default/files/socialna_i_cifrova_transformaciya_maket.

5. https://library.nlu.edu.ua/novi-nadkhodzhennia/item/3082-prava-liudyny-v-umovakh-tsyfrovoi-transformatsii-suspilstva.html.

6. (PDF) LEGAL ENFORCEMENT OF DIGITAL APPLICATIONS PERSONALITIES AND AVATARS / ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЗАСТОСУВАННЯ ЦИФРОВИХ ОСОБИСТОСТЕЙ ТА АВАТАРІВ

Літвінова В. Г.
здобувачка вищої освіти ІІ курсу магістратури Одеського національного університету імені І. І. Мечникова
Науковий керівник: д.ю.н., проф. Степанова Т. В.

НЕДОЛІКИ ТА ПРОГАЛИНИ У СУДОВІЙ ПРАКТИЦІ: КОНФЛІКТ МІЖ ПРАВОМ НА ІНФОРМАЦІЮ І ПРАВОМ НА ПРИВАТНІСТЬ

Кожного дня ми користуємося соціальними мережами та публікуємо різноманітну інформацію про себе та інших людей, але навіть не замислюємося над тим, що таким чином можемо порушити чиєсь право на приватне життя.

Питання балансу між правом на свободу вираження поглядів і захистом права на приватне життя є досить неоднозначним, адже судам доводиться шукати його між конституційними гарантіями свободи вираження та приватними інтересами осіб. Суд при вирішенні питання стосовно конфлікту цих двох прав зазвичай обмежується аргументацією тієї чи

іншої статті, аналізуючи певні випадки відповідно до статті 10 і з посиланням на частину другу статті 10 з обґрунтуванням «захисту репутації або прав інших осіб» [1, с. 44].

Тому питанню захисту персональної інформації приділено так багато уваги як національними, так і міжнародними інституціями. Найчастіше конфлікт між цими правами виникає тоді, коли засоби масової інформації публікують статтю чи фотографії тієї чи іншої особи, при цьому стверджуючи, що особа, про яку опубліковано інформацію, втратила своє право на недоторканність приватного життя, оскільки стала публічною особою [2].

Так, доктрина права розрізняє два види обробки персональних даних: на підставі згоди особи або за законом. Дане положення конкретизується статтею 11 Закону та статтею 7 Директиви та статтею 6 Регламенту. Так, стаття 11 Закону встановлює вичерпний перелік випадків та умов, за яких може здійснюватися обробка персональних даних суб'єкта. Ця стаття є першим «фільтром» на шляху до законної обробки [3, с. 32].

Згідно з положеннями Закону України «Про захист персональних даних» згода суб'єкта персональних даних – це добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди [4].

Кожен, хто реєструвався у соціальних мережах, відповідав «так» на твердження «Надаю згоду на обробку персональних даних» для того, аби завершити реєстрацію. Тому вся інформація, яка поширена особою в цій соціальній мережі, законно обробляється та використовується мережею.

Однак чи можуть таку інформацію використовувати та поширювати інші особи? Судова практика з цього питання неоднозначна.

У справі «Фон Ганновер проти Німеччини» заявник (старша донька принца Монако Реньє III) подала скаргу до Європейського суду на рішення національних судів про відмову в забороні публікації фотографій її приватного життя в пресі [5].

ЄСПЛ зазначив, що при вирішенні цієї справи необхідно відзначити, що заявник як представник правлячої династії представляє її на певних культурних та благодійних заходах, однак не виконує жодних функцій в інтересах чи від імені держави Монако або її інституцій.

Національними судами було визначено статус заявника як «фігура сучасного суспільства», якій надано дуже обмежений захист на приватне життя. Однак ЄСПЛ із вказаним не погодився, вважаючи, що потрібно

розрізняти «фігур сучасного суспільства», таких як політики, та «відносних публічних осіб».

Адже кожна особа, навіть публічна, повинна знати, де пролягає межа між її приватним життям та тим, де можливе втручання з боку інших. Крім того, існує фундаментальна різниця між публічним висвітленням інформації, яка сприяє виконанню політичних функцій особи, та висвітленням приватного (особливо коли така людина не виконує жодних офіційних функцій). Якщо в першому випадку медіа виконує роль «запобіжника», сприяючи поширенню інформації, що належить до суспільного інтересу, то в другому це не має місця.

Публікація фотографій у справі Фон Ганновер була заради привернення уваги аудиторії, оскільки у цій справі інформація не була предметом суспільного інтересу. Тому Суд дійшов висновку, що право на приватність публічної особи в цьому випадку було порушено.

Кардинально протилежний випадок був у справі «Кроне Ферлаг ГмбХ і Ко КГ» проти Австрії», де позивачем був член парламенту. Він оскаржував публікацію своєї фотографії поруч зі статтею, в якій він був звинувачений у незаконному отриманні заробітної плати. Національні суди задовольнили вимоги позивача, вказуючи, що фотографія не мала значення для питання, порушеного в статті, позивач не був відомою особою, а у зв'язку з опублікуванням фотографії його стало можливо ідентифікувати. Але ЄСПЛ дійшов іншого висновку: він вказав, що не має значення, чи є особа відомою суспільству, треба встановити, чи вийшла вона на публічну арену. Позивач як політик, безумовно, вважається такою особою. Крім того, фотографія не розкриває жодних подробиць його приватного життя, тому засудження заявників не відповідало ст. 10 Конвенції [6].

Ще одне цікаве рішення було по справі «Асоціація візуальних художників проти Австрії». Предметом розгляду була заборона національними судами показу картини, на якій були зображені публічні особи голими в різних позах сексуального характеру. Позивачем у справі був член парламенту. У своєму рішенні ЄСПЛ зазначив, що картина являла собою нереалістичне зображення публічних осіб, а радше їх карикатуру з використанням сатиричних елементів. Сатира є формою мистецького вираження і соціального коментування, їй притаманне перебільшення, природно вона спрямована на провокацію й агітацію. У цій справі карикатура стосується не приватного життя позивача, а його політичної діяльності. Крім того, слід зважати на те, що межі критики щодо політика є ширшими, ніж стосовно звичайного громадянина. Позивач був зображений в оточенні осіб, які були набагато більш відомими, ніж він, тому важко запам'ятовувався публіці [7].

Таким чином, на думку ЄСПЛ, спірна картина могла розглядатися як свого роду контратака проти Австрійської партії свободи, члени якої різко критикували роботу художника.

До того ж, Суд наголосив, що, крім пана Мейшбергера, на картині зображено серію з тридцяти трьох осіб. Пан Мейшбергер, який на час подій був звичайним членом парламенту, безумовно, був одним із найменш відомих серед усіх людей, що з'явились на картині, а на час розгляду справи, пішовши із політики, взагалі тим, кого громадськість навряд чи пам'ятає. Суд також зауважив, що ще до того, як пан Мейшбергер порушив провадження, частина картини, на якій він був намальований, була пошкоджена, зокрема, образливе зображення його тіла було повністю покрито червоною фарбою [8, с. 29-30].

Із зазначеного видно, що межа між публічним та приватним життям завжди дуже розмита та ключову роль відіграє те, наскільки суспільний інтерес переважає над особистими правами людини.

Тому, зважаючи на практику Європейського суду з прав людини можна дійти наступних висновків:

1. Будь-яка особа має право на захист від поширення недостовірної інформації щодо неї.
2. Не може бути конфіденційною комерційна інформація про діяльність публічної особи, особливо, якщо вона має політичний вплив.
3. Жоден суспільний інтерес не може стати причиною розголошення приватного життя особи.
4. Оприлюднення інформації, яка не містить відомостей про приватне життя публічної особи, що має суспільний вплив, є законним.
5. Будь-яке втручання в приватне життя можливе настільки, наскільки це сприяє публічному інтересу з питань суспільної важливості.

Список використаних джерел:

1. Colvin M. Developing Key Privacy Rights. Oxford, Portland, Oregon: Hart Publishing, 2002. 198 p. URL: http://ndl.ethernet.edu.et/bitstream/123456789/5698/1/212.pdf.pdf (дата звернення 02.11.2023).

2. Нагнічук О. І. Співвідношення права на свободу вираження щодо публічних осіб та права на повагу до приватного та сімейного життя публічних осіб у практиці Європейського суду з прав людини. URL: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/e5c2d323-a531-42d6-a23c-07e5e997620e/content (дата звернення 02.11.2023).

3. Бем М. В., Городиський. І. М. Стандарти захисту персональних даних в соціальній сфері. Львів: б.в., 2018. 110 с. URL: https://radnyk.

org/wp-content/uploads/2018/06/Standarti_zahistu_personalnih_danih_v_sotsialniy_sferi.pdf (дата звернення 02.11.2023).

4. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення 02.11.2023).

5. Von Hannover v. Germany (App no 40660/08) ECHR 24 July 2005. URL: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-109029%22]} (дата звернення 02.11.2023).

6. Krone Verlags Gmbh & Co. KG v. Austria (App no 39069/97) ECHR 11 December 2003. URL: https://hudoc.echr.coe.int/app/conversion/docx/?library=ECHR&id=001-61538&filename=CASE%20OF%20KRONE%20VERLAG%20GmbH%20%26%20Co.%20KG%20 (дата звернення 02.11.2023).

7. Vereinigung Bildender Künstler v. Austria (App no 68354/01) ECHR 25 January 2007. URL: https://hudoc.echr.coe.int/app/conversion/docx/?library=ECHR&id=001-79213&filename=CASE%20OF%20VEREINIGUNG%20BILDENDER%20K%C3%9CNSTLER%20v.%20AUSTRIA.docx&logEvent=False (дата звернення 02.11.2023).

8. Опришко Д. І. Право на свободу мистецького вираження. Огляд практики Європейського суду з прав людини. Київ: ГО «Платформа прав людини», 2021. 108 с. URL: https://www.ppl.org.ua/wp-content/uploads/2021/09/Freedom-of-artistic-expression.pdf (дата звернення 02.11.2023).

Доронін І. М.
доктор юридичних наук, доцент зав. наукової лабораторії ДНУ «Інститут інформації, безпеки і права НАПрН України»

БЛОКЧЕЙН ТА НАЦІОНАЛЬНА БЕЗПЕКА: ВИКЛИКИ ТА ВІДПОВІДІ СЬОГОДЕННЯ

На сьогодні можливо констатувати, що дослідження проблеми застосування технології блокчейн у різних сферах суспільного життя переживає певний спад, пов'язаний із деякою втратою наукового інтересу порівняно із піком публікацій 2014-2018 років. Зараз існують інші теми та проблеми, що посіли значне місце в увазі науковців. Якщо розглядати суто правовий вимір проблематики, то правова регламентація фактично

звелась лише до визначення місця криптовалют у сучасній економіці (в основному з метою оподаткування те декларування як цінностей) та, відповідно, шляхів конкретної регламентації правовими засобами. У цьому аспекті проблематика дискусій мало змінилась, хоча озвучені свого часу правові проблеми [1-3] і знайшли свої часткове вирішення на законодавчому рівні.

Стан законодавчого регулювання, а точніше кажучи – намагань регламентації свідчить про початок певного процесу. Зазначений процес можливо охарактеризувати як відмову від точкової регламентації в певних інтересах до імплементації європейського законодавства у відповідній сфері. І у цьому напрямку заслуговують на увагу відповідні законотворчі ініціативи (законопроект 10225 та альтернативні), що намагаються вирішити проблему правового «завісання» ухваленого Закону України «Про віртуальні активи» від 17.02.2022 р., який так і не набрав чинності. Як відомо його Прикінцеві положення передбачають набрання чинності «з дня набрання чинності законом України про внесення змін до Податкового кодексу України щодо особливостей оподаткування операцій з віртуальними активами..», що, як відомо, досі не відбулось.

Не вдаючись до аналізу законодавчого акту у сфері регулювання «віртуальних активів» можливо лише зазначити, що подальша правова регламентація у першу чергу в оподаткуванні має відповідати Markets in Crypto-Assets (MiCA) – законодавчому акту ЄС, ухваленому 20.03.2023 року, що набуває чинності у 2024 році.

Але технологія «блокчейн» не обмежується криптовалютами чи «віртуальними активами» (у термінах вітчизняного законодавства), оскільки її застосування можливо в досить різних напрямах. Що стосується загроз та викликів у сфері національної безпеки, то в першу чергу знову ж таки дослідниками згадуються загрози від використання криптовалют з незаконними цілями (відмивання коштів, торгівля предметами, вилученими з обігу, корупція, фінансування тероризму тощо). Саме таким чином розглядаються загрози через призму завдань правоохоронних органів. Свого часу автор запропонував розглядати проблеми національної безпеки при використанні технологій більш комплексно [4, с. 35].

Повертаючись до визначення впливу технології блокчейн на загрози у сфері національної безпеки можливо визначити певні правові проблеми, що, залишаючись не регламентованими, можуть негативно впливати і створювати передумови до таких загроз.

Зокрема, можливості технології по збереженню інформації створюють цілком передбачувану спокусу до її застосування для збереження інформації, що критично важлива, та повинна захищатись від свавіль-

ного маніпулювання [5]. Водночас, приведення окремих аспектів застосування блокчейну до правового поля відповідної юрисдикції є досі невирішеним попри на різноманітну інформацію щодо тих чи інших піонерських проектів, у першу чергу у сфері земельних кадастрів, титулів власності на майно, реєстрації транспортних засобів та інших державних реєстрів [6].

Стосовно загроз національній безпеці можливо визначити наступне. По-перше, у цей час досить активно обговорюються питання використання технології (а точніше певних її елементів, по суті – закритого або «приватного» блокчейну) при конструюванні інформаційних систем військового призначення [7]. По-друге, мова може йти про застосування цієї ж технології і в інтересах кібербезпеки (в досить широкому значенні – від кіберзахисту до кібернападу та бойових дій в кіберпросторі приблизно аналогічним способом).

Але зазначені технологічні та технічні можливості по суті залишають незмінними увесь той конгломерат правових проблем, що на сьогодні піддається досить обережному вирішенню. В основі знаходиться проблема так званого постійного «розподілу» для інформації. Не випадково «блокчейн» за своєю суттю є технологією розподілених реєстрів (distribute ledger), тобто інформація знаходиться одночасно всюди і ніде у повному обсязі. А це змінює парадигму правового регулювання у питанні захисту інформації. На сьогодні законодавча термінологія змінюється у напрямку уточнень форми, а не суті. Так, першим серед визначень термінів у Законі України «Про інформацію» є визначення терміну «документ» як матеріального носія інформації. Саме на розумінні «носія інформації» і будується увесь законодавчий масив у сфері поводження інформації з обмеженим доступом – наприклад, у визначеннях «власник матеріальних носіїв інформації» (Закон України «Про державну таємницю»). У даному випадку можливим вирішенням буде лише чітке визначення юридичної відповідальності за збереження інформації, тобто технічна неможливість її модифікації має спонукати до розповсюдження такої відповідальності на власника мережі блокчейн безвідносно до можливого часткового знаходження інформації на будь-яких носіях.

І хоча зазначена вище проблема наразі може видаватись дещо штучною, це далеко не так. Хоча б тому, що використання різних видів DL технології з військовою метою можливо значно раніше аніж передбачалось до цього особливо з огляду на досить динамічний характер розвитку військової техніки. Не слід також залишати поза увагою і можливе застосування таких технологій для зберігання критично важливої інформації у першу чергу щодо захисту від неавторізованої модифікації.

Підсумовуючи викладене можливо зазначити дві основні групи проблем застосування блокчейн технології, що постали у тому числі і в сфері національної безпеки. По-перше, це належна регламентація обігу криптовалют (або віртуальних активів за термінологією вітчизняного законодавства) з метою недопущення їх використання із незаконною метою. По-друге, це належне правове визначення статусу інформації, що зберігається при використанні DL технологій, у контексті юридичної відповідальності. Конкретні шляхи правового регулювання будуть зумовлюватись подальшим розвитком прикладного аспекту використання технологій.

Список використаних джерел:

1. Shcherbak S. How Should Bitcoin be Regulated? *European Journal Of Legal Studies*. 2014. Vol. 7. No 1.P. 45-91.

2. Kiviat T. Beyond Bitcoin: Issues In Regulating Blockchain Transactions. *Duke Law Journal.* 2015. Vol. 65 (569). P. 569-508.

3. De Filippi P., Loveluck B. The invisible politics of Bitcoin: governance crisis of a decentralized infrastructure. *Internet Policy Review.* 2016. Vol. 5, Issue 3 URL: https://pdfs.semanticscholar.org/5761/af4eff318e876f2990aa53469352826214a0.pdf. (Last accessed: 20.11.2023).

4. Доронін І. М. Цифровий розвиток та національна безпека у контексті правових проблем. Інформація і право. 2019. № 1. С. 29-36.

5. Poliakh, A., Yemets, O., Doronin, I., & Zapototskyi, A. Modern Blockchain Technologies and the Law of State Registers (Ukrainian Experience). *Journal of Legal, Ethical and Regulatory Issues.* 2000. 23(5), P. 1-9.

6. Müller H., Seifert M. Blockchain, a Feasible Technology for Land Administration? // FIG Working Week 2019, Hanoi, Vietnam, 22 – 26 April. URL: https://www.researchgate.net/publication/332971853_Blockchain_a_Feasible_Technology_for_Land_Administration (Last accessed: 20.11.2023).

7. Mincewicz, W. Technologia blockchain a bezpieczeństwo narodowe. Możliwość wdrożenia łańcucha bloków w obszarze bezpieczeństwa państwa. *De Securitate et Defensione. O Bezpieczeństwie i Obronności,* 2020. 6(2), s. 114–129.

Бєлєвцева В. В.
доктор юридичних наук, старший науковий співробітник, головний науковий співробітник Наукової лабораторії правових проблем та відповідальності у сфері цифровізації Державної наукової установи «Інститут інформації, безпеки і права НАПрН України»

ПРО ОСНОВНІ АСПЕКТИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У ДЕРЖАВІ ІЗРАЇЛЬ

Законодавство Держави Ізраїль у сфері інформаційної безпеки досить об'ємне. Крім того, ця сфера регулюється численними підзаконними актами, головним чином, положеннями Міністерства юстиції і Правилами, затвердженими Урядом. Значну роль при цьому відіграють Правила надання інтернет-послуг, що прийняті неурядовими організаціями, але які відповідають за проведення політики в досліджуваній сфері. У цілому законодавство збалансоване і не представляє загрозу як споживачам інформаційних послуг, так і безпеці держави та свободі інформації. Необхідно також відмітити, що суб'єкти, уповноважені на отримання інформації, зокрема правоохоронні органи і спецслужби, несуть відповідальність перед громадським суспільством, та їх діяльність підкорюється принципу прозорості публічної влади.

Ізраїль – це держава, усі зусилля якої спрямовані на творення. Не маючи у розпорядженні ніяких сировинних ресурсів і знаходячись у стані постійної військової загрози, державі вдалося стати світовим центром науки та високих технологій. Ізраїльські розробки рятують світ від голоду і спраги, можливості медицини вважаються самими передовими у світі, а в IT-секторі країна за короткий строк стала інноваційним лідером. Люди живуть в терористичній обстановці вже 75 років, тому цінують сьогодення і піклуються про майбутнє, роблячи все для того, щоб країна міцніла і розвивалася.

Розвиток сфери кібербезпеки знаходиться в пріоритеті держави, оскільки Ізраїль – одна з самих комп'ютеризованих країн на Близькому Сході. Допустити уразливість в роботі інформаційної інфраструктури для них рівно нанесенню важкого збитку обороні держави та національній безпеці.

Відповідальність за захист інформації несе ізраїльське агентство безпеки «Шин-Бет» («ШАБАК»). Воно традиційно відповідає за забезпе-

чення безпеки державних органів та основної інфраструктури – об'єктів електропостачання, водозабезпечення і фінансових установ. Також у 2010 році було створено Ізраїльське національне кібернетичне бюро (INCB), покликане просувати кіберполітику Ізраїлю у трьох основних напрямах:

– вдосконалення захисту і зміцнення національного потенціалу в кіберпросторі;
– перетворення Ізраїлю на центр інформаційних технологій;
– заохочення співпраці між ученими, промисловцями, приватним сектором, державними службовцями і громадськістю з питань безпеки (за матеріалами дослідження Inter – American Development Bank, 2016) [1, 2].

Організаційно-правова модель регулювання мережі «Інтернет» в Державі Ізраїль представляє інтерес з різних точок зору.

По-перше, на цей час відсутній єдиний підхід щодо питання відношення правової системи Ізраїлю до тієї або іншої «правової сім'ї» (з певною долею умовностей Державу Ізраїль можна віднести до держав змішаної правової системи), однією з причин такого стану речей виступає той факт, що заснування держави сталося у 1948 році. У той же час, Ізраїль за короткий за історичними мірками проміжок часу успішно імплементував законодавчий досвід інших держав, у зв'язку з цим, у другій половині XX століття його правова система нестримно удосконалювалася, багато в чому завдяки акценту на практику ізраїльських судів, які мають нормативний характер. Успішний досвід взаємозв'язку правових систем Ізраїлю та інших держав, наприклад, Великобританії підтверджується актуальними прикладами. Так, у 2018 році Ізраїль спільно з Великобританією виступив з ініціативою впровадження механізмів протидії порушенням прав інтелектуальної власності в мережі «Інтернет» у рамках сесії Консультативного комітету із захисту прав Всесвітньої організації інтелектуальної власності.

По-друге, викликає інтерес ангажування громадян Ізраїлю і комерційних структур держави до мережі «Інтернет». Кожна п'ята компанія високих технологій, що котирується на Нью-йоркській біржі NASDAQ, – ізраїльська або колишня ізраїльська фірма, 80 з ізраїльських компаній, що котируються в Нью-Йорку, – державні. На NASDAQ котирується більше ізраїльських компаній, ніж усіх європейських разом узятих [3]. Одним з важливих чинників популярності інтернет-технологій в державі, а також успіху Ізраїлю на ринку інформаційних технологій виступила система ізраїльської освіти, яка багато в чому сприяє розвитку технічних та інженерних кадрів, фахівців у сфері інформаційних технологій, а також

допомагає проводити дослідження і розробки навіть школярам і, далі, студентам.

По-третє, незважаючи на багато в чому аналогічну європейській, за характером правових норм, моделі регулювання мережі «Інтернет», в Державі Ізраїль вона (модель) має низку особливостей та інновацій. Передусім, заслуговує на увагу той факт, що в Ізраїлі з 2011 р. блогер може отримати статус акредитованого журналіста, у зв'язку з цим йому видається документ, йменований «GPO card» (Government Press Office). Таке посвідчення надає блогерові право отримувати інформацію і роз'яснення від офіційних осіб, а також бути присутнім на заходах прес-служби Уряду Ізраїлю. У зв'язку з цим де-факто блогер, який отримав вказаний документ, стає ЗМІ. Цей статус надає йому право сприяти освітленню в ЗМІ ключових подій в Ізраїлі, а також візитів до держави іноземних високопоставлених осіб.

Цікава практика застосування низки законодавчих актів у сфері протидії інтернет-злочинності. Закон про комп'ютери дозволяє слідчим органам отримати дозвіл судових або, у невідкладних і виняткових випадках, адміністративних органів на отримання даних, що передаються під час процесу обміну інформацією між громадянами за допомогою мережі «Інтернет». З 2017 року в Державі Ізраїль також набув чинності Закон «Про повноваження щодо попередження правопорушень за допомогою сайтів в мережі «Інтернет», згідно з яким суди можуть наказати провайдерам блокувати сайти терористичних груп, незаконні азартні ігри в мережі «Інтернет», послуги проституції, продаж наркотиків тощо.

У той же час Держава Ізраїль є одним з лідерів серед держав, уряди яких «активно сприяють онлайн-цензурі» (за версією британської компанія Comparitech). У звіті компанії говориться, що за останнє десятиліття Уряд Ізраїлю направив технологічним гігантам більше 5500 запитів на видалення контенту, що, на думку Comparitech, є істотним показником [4].

Усі вищевикладені аспекти свідчать про успішний досвід цієї держави в регулюванні інтернет-простору. Особливо слід зазначити економічні успіхи Ізраїлю у вказаній сфері, найважливішу роль у досягненні яких зіграло залучення ізраїльських громадян та організацій до діяльності, пов'язаної з розвитком мережі «Інтернет».

З урахуванням викладеного, перспективним напрямом розбудови національної системи інформаційного законодавства є активізація зусиль уповноважених органів України з питань забезпечення інформаційної безпеки у напрямку міжнародного співробітництва з державою Ізраїль, що надасть змогу впровадити у практичну площину кращі практики за-

рубіжного досвіду в контексті удосконалення вітчизняної моделі захисту інформаційних прав і свобод держави, суспільства і громадянина.

Список використаних джерел:

1. The Global competitiveness Report 2016–2017. URL: http://www3.weforuor/docs/GCR2016017/05FullReport/The GlobalCompetitivenessReport2016-2017_FINAL.pdf (дата звернення 10.11.2023).

2. Гребенюк М. В., Леонов Б. Д. Досвід Ізраїлю у сфері забезпечення кібербезпеки //Інформація і право. 2018. №2 (25). С.45-50.

3. Див. сайт: https://shofar7.com/2015/05/17/20 (дата звернення 16.11.2023).

4. Див. сайт: https://rdc.grfc.ru/2020/10/israel/ (дата звернення 12.11.2023).

Лихоступ С. В.
кандидат економічних наук , старший науковий співробітник провідний науковий співробітник Державної наукової установи «Інститут інформації, безпеки і права НАПрН України»

ФОРМУВАННЯ ПРИНЦИПІВ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ В ПРОЦЕСАХ РЕГУЛЮВАННЯ ПРАВОВИХ ВІДНОСИН СУСПІЛЬНИХ СТРУКТУР

Управління соціальними структурами в єдиному правовому просторі спирається на використанні значної інформації, що визначає багато аспектів функціонування як окремих державних інститутів, так і галузей країни. Подальший розвиток країни повинен бути спрямований в рамках стабільної соціальної політики розвитку суспільства з урахуванням сучасних та перспективних тенденцій ринкової економіки, що призводить до позитивних тенденцій у задовольнянні потреб та якості життя громадян. В процесах створення та реалізації таких вимог визначається першочергова потреба у нормативно-законодавчому формуванні основ та у моделювання структур динамічного розвитку соціальних устроїв суспільства у відповідності до демократичних принципів управління державою. Слід відзначити, що гідний рівень соціально-економічного

розвитку суспільства в першу чергу визначається раціональним станом функціонування соціально – нормативного управління всіма складовими суспільства, розпочинаючи із органів управління соціальними структурами суспільства та закінчуючи регулюванням економічних відносин між окремими виробничо – господарчими структурами. В такому випадку для ефективного управління соціальних устроїв країни необхідно створення системи його нормативно – правового забезпечення в мінливих умовах розвитку європейської та світової економіки, а також з урахуванням динамічних принципів до вимог та стандартів життя окремих громадян в цих умовах.

Система нормативно – правового забезпечення може бути уявлена як логіко – структурований граф, кожна вершина якого уявляє певну підсистему. В свою чергу виділені підсистеми формують такі загального комплексу нормативно – правового забезпечення, як: визначення стратегії та формування концепції комплексу нормативно – правового розвитку суспільства; складання сукупності вимог та обмежень до розробки та запровадження окремих пакетів нормативно – правового забезпечення в різних соціальних структурах суспільства; створення нормативно – правових документів у відповідності до вимог європейського товариства; оперативне регулювання структури нормативно- правових документів та їх змісту в мінливих розвитку суспільства; визначення порядку використання та рівня відповідальності за ефективністю реалізації нормативно – правових документів.

Так перша підсистема – складання стратегії та формування концепції комплексу нормативно – правового розвитку суспільства – означає розробку таких законодавчих документів, які реалізують цілий рядок принципів надійного розвитку соціальної держави, а саме. Це, перш за все, сукупність нормативних актів, що відображують вимоги та умови досягнення соціального та економічного достатку громадян завдяки соціальній рівності, трудової зацікавленості в досягненні гідного рівня життя. В такій структурі документів повинні бути передбачені нормативно – правові документи, що гарантують соціальний захист громадян, охорону їх здобутків, соціального забезпечення та гідного рівня життя, що визначається справедливими принципами розподілу здобутків суспільства за результатами колективної праці. Важливими регулюючими нормативними документами при цьому повинні бути такі, що гарантують вільний розвиток особистості в умовах забезпечення гарантій по досягненню рівних можливостей, але також і відповідної соціальної активності, трудової солідарності та відповідальності кожного громадянина за свою діяльність. При цьому в таких документах повинні бути фіксовані шляхи та мож-

ливості до рівного доступу громадян до громадських та соціальних інституцій, розвитку професійних можливостей у різних сферах трудової діяльності із використанням суспільних ресурсів.

Використання таких нормативно – правових документів повинно бути підтверджено сукупністю актів про соціальну відповідальність суб'єктів бізнесу та різних структур підприємницької діяльності за результати використання своїх виробничих спроможностей, принципів регулювання справедливого розподілу результатів колективної праці, що сприяє подальшій активізації використання виробничого потенціалу та розвитку соціальної сфери окремих соціальних груп суспільства. Головний фактор, що формує концепцію таких нормативно – правових документів – це захист прав та інтересів окремих громадян в соціальних та виробничо – бізнесових структурах суспільства.

Окрім цього слід відзначити, що в підтримання пакету цих нормативно – правових документів є створення таких, що забезпечують уникнення або пом'якшення впливу на суспільство та кожного громадянина негативних економічних наслідків і ризиків в управлінні суспільною працею. Але при цьому провідним принципом в процесі формування таких нормативно – правових документів є надання гарантій розвитку гармонійних принципів розвитку відносин між різними соціальними групами, що забезпечують партнерську відносини, порозуміння та злагодженість у досягненні результатів.

Далі, в підсистемі складання сукупності вимог та обмежень до розробки та запровадження окремих пакетів нормативно – правового забезпечення в окремих соціальних структурах повинна фігурувати домінанта надання всіх прав та свобод в демократичному суспільстві при умові гідного життя. Але в таких документах повинні бути чітко визначені форми відповідальності окремих осіб за невідповідність їх діяльності всупереч порушеним нормам суспільства. До критеріальних вимог розвитку таких нормативно – правових актів слід віднести також обгрунтовані принципи до забезпечення динамічних умов розвитку людини, захисту її культурних та національних традицій. Реалізація та підтримання цих документів знаходить підтвердження в пакеті нормативно – правових документів, що визначають міри відповідальності за негативні наслідки соціально – економічних умов населення органів державної влади та місцевого самоврядування. І, на кінець, в нормативно – правових документах, що визначають вимоги до розвитку соціальних устроїв суспільства, повинні розвинуті та інтегровані до міжнародного права обов'язки держави та соціальних інституцій у їх формуванні та відповідальності за свою діяльність.

Головною, а іншими словами пов'язуючою та регулюючою підсистемою є підсистема власне створення нормативно – правових документів у відповідності до вимог України, як незалежної держави, так і європейського товариства. На сьогоднішній день це найбільш активна підсистема, що породжує як багато сподівань, так і нарікань. Сподівання – тому що певний нормативний документ надає надію на вирішення чи регулювання певних ситуацій певної проблеми. Але, з іншого боку, локальне, як правило, хаотичне чи вольове прийняття ряду нормативно – правових документів призводить до породження ще до більш за заплутаного клубка проблем. А тому системність у створенні та відпрацювання нормативно – правових документів з урахуванням принципу причинно – наслідкових подій має надзвичайне значення. Розгляд функціонування такої важливої підсистеми заслуговує надзвичайної уваги, так як вона повинна бути орієнтована на вирішення актуальних, сьогоденних питань розвитку суспільства, орієнтирів на перспективу його покращання, що можливе тільки при умові ретельного перехресного пов'язання умов функціонування всіх ключових задач до конкретної проблеми нормативно – правових документів.

Розвиток відзначених вище підсистем в значній мірі залежить від впливу непередбачуваності та складності процесів власне розвитку суспільства , а тому вимагає постійного та оперативного регулювання структури нормативно – правових документів та їх змісту в мінливих умовах розвитку суспільства, що може складати слідуючу умовну підсистему. Група таких нормативно – правових документів формує як би захисні основи для життєдіяльності членів суспільства.

Насамперед в такій підсистемі формуються документи, що визначають шляхи розвитку ділового партнерства, соціальної інтеграції праці та виробництва. В таких документах повинні бути викладені гарантії що до реалізації різних форм використання трудового потенціалу, формування та інтеграції соціальної інфраструктури при умові партнерства та взаємної злагоди між окремими верстами населення.

В таких документах мова йде про викладення цілої низки соціальних, політичних та економічних гарантій в широкому розумінні цього контексту. Важливе місце при цьому займає ідея про створення захисного механізму людини від можливих порушень прав та свобод, економічних негараздів, правопорушень злочинного чи антисоціального характеру. В таких документах відслідковується домінантна нота про реалізацію державних заходів, форм надання захисту та ліквідації лиха шляхом проведення державної політики надання гарантій та необхідних послуг. Особливість таких документів полягає у викладенні

можливих форм соціально – економічної безпеки та розвиток варіантів можливого її усунення та мінімізації завданої шкоди. Також це група документів, що спрямована на формалізацію та викладення форм дій що до захисту вразливих форм суспільства та надання їм необхідної допомоги.

Завершуюча підсистема формує визначення порядку та рівня відповідальності за ефективністю реалізації нормативно – правових документів в принципі формує механізм втілення в практику державних і місцевих органів таких документів. Акцент створення такого механізму полягає у практичних діях реалізації законодавчих та нормативних документів управління державою з метою досягнення соціальних основ життєздатності України. Конкретні дії в цьому напрямку включають багато напрямків, розпочинаючи з удосконалення чинного законодавства, розвитку форм соціального партнерства, дослідження ефективних методів покращання економічного положення та інші.

Викладені вище характерні ознаки системного підходу до створеннння нормативно – правового забезпечення основ регулювання функціонування та розвитку соціальних устроїв України можливо дослідити в ряді державних документів, наприклад, [1-8]. Звичайно, в процесі створення певного нормативного акту не використовуються тільки домінантні ознаки виділених вище підсистем. Але використання певних базових статей, що формують створення конкретного нормативного акту, дає змогу чітко його трактувати та ефективно використати на практиці.

Список використаних джерел:

1. Конституція України : Закон України від 28.06.96 р. № 254к/96-ВР URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

2. Загальна декларація прав людини : Резолюція Генеральної Асамблеї ООН від 10.12.48 р.№ 217 А (III). – Режим доступу : http://zakon4.rada. gov.ua/rada/main

3. Про схвалення Концепції розвитку електронного урядування вУкраїні : Розпорядження Кабінету Міністрів України від 20.09.2017 № 649-р. URL: https://www.kmu.gov.ua/ua/npas/250287124

4. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : розпорядження Кабінету Міністрів України від 15 трав. 2013 р.№ 386-р. URL: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80.

5. Стратегія реформування державного управління України на 2022-2025 роки : схвалено розпорядженням Кабінету Міністрів України від

21 липня 2021 р. № 831-р. URL: https://zakon.rada.gov.ua/laws/show/831-2021-%D1%80#Text

6. Концепція розвитку цифрової економіки та суспільства України на 2018–2020 рр. : схвалено розпорядженням Кабінету Міністрів України від 17 січ. 2018 р. № 367-р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80.

7. Конвенція про захист прав людини і основоположних свобод. Режим доступу: https://zakon.rada.gov.ua/laws/show/995_004#Text

8. Національна стратегія сприяння розвитку громадянського суспільства в Україні на 2021-2026 роки. Затверджена Указом Президента України від 27вересня 2021 року № 487/2021. URL:https://zakon.rada.gov.ua/laws/show/487/2021#Text.

Королюк Т. О.
кандидат економічних наук, доцент,
доцент кафедри національної
економіки та публічного управління
Київського національного економічного
університету імені Вадима Гетьмана
Звєрєвич Ю. О.
здобувачка 4 курсу ОПП «Публічне
управління та адміністрування»

МЕХАНІЗМИ ЗАХИСТУ НАЦІОНАЛЬНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Державне управління у сфері забезпечення інформаційної безпеки є важливим аспектом функціонування будь-якої країни в умовах загострення глобального інформаційного протистояння, цифровізації та розвитку інформаційно-комунікаційних технологій. Ця функція передбачає скоординовану розробку та впровадження національної стратегії інформаційної безпеки на різних рівнях управління, включаючи державний, регіональний та місцевий. Держава повинна систематично моніторити та оцінювати загрози й ризики в інформаційній сфері, які становлять небезпеку, і забезпечувати відповідну реакцію та захист від них. Створення дієвого правового поля, чіткий розподіл повноважень, обов'язків і відповідальності між суб'єктами представляють

лише частину державного механізму забезпечення захисту інформаційного простору.

Недосконалість правового регулювання у сфері інформаційної безпеки в Україні викликає негативні явища, що призводять до потенційних і реальних загроз інформаційній безпеці громадян, суспільства і держави. Прикладом цього є події 2014 року на півдні та сході України, коли інформаційно-психологічний тиск та інформаційна експансія, спрямовані з боку російської федерації, спричинили загрозу національній безпеці, включаючи захоплення стратегічних об'єктів української телекомунікаційної інфраструктури та вплив на свідомість громадян через ефективне поширення пропаганди. Інформаційний тероризм з боку агресора продовжується і посилюється особливо в умовах повномасштабного вторгнення, що стало загрозою не лише для окремих територій, а й для існування цілої нації. Саме тому, в сучасних умовах, коли національна інформаційна безпека є ключовим аспектом політичного, соціального та економічного розвитку, питання вивчення та вдосконалення механізмів захисту національного інформаційного простору стає одним з найбільш актуальних для дослідження.

До механізмів захисту національного інформаційного простору відносяться:

- нормативно-правова база у сфері захисту національного інформаційного простору;
- інституційний механізм, який охоплює структуру органів влади, визначення їхніх повноважень, обов'язків та відповідальності;
- заходи держави у сфері протидії поширенню дезінформації та пропаганди, просвітницька діяльність серед громадян;
- співпраця з іншими країнами та міжнародними організаціями для обміну досвідом протистояння інформаційним загрозам та взаємної допомоги у реагуванні на них.

Серед вище відзначених механізмів провідна роль належить розробці дієвого, прозорого та зрозумілого нормативно-правового регулювання інформаційних відносин. Його основу складають Конституція України, закони «Про національну безпеку України», «Про державну таємницю», «Про захист персональних даних», «Про доступ до публічної інформації», постанови ВРУ, укази Президента (табл.).

Можемо зробити висновок, що в Україні нормативно-правові акти в повній мірі визначають поняття національної інформаційної безпеки, принципи її забезпечення, актуальні загрози та виклики, а також стратегії та напрямки вдосконалення державної політики у сфері захисту національного інформаційного простору в умовах воєнного стану.

Таблиця

Нормативно-правові акти у сфері захисту національного інформаційного простору України

Нормативно-правові акти	Зміст
Конституція України	Ст. 17. Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу
Закон України "Про національну безпеку України"	Забезпечення національної інформаційної безпеки є однією з основних функцій органів влади (КМУ, МВС, СБУ, Держспецзв'язку та ін.); міжнародна співпраця, обмін інформацією про кіберзагрози.
Закон України "Про державну таємницю"	Регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці
Постанова ВРУ "Про затвердження завдань Національної програми інформатизації на 2022-2024 роки"	Визначає основні напрями, завдання та очікувані результати інформатизації всіх сфер діяльності держави. Програмою передбачено впровадження міжнародних стандартів щодо управління та захисту інформації; забезпечення розвитку кібербезпеки критично важливої інфраструктури; створення, модернізація та оновлення програмно-апаратних засобів та матеріально-технічної бази інформаційно-комунікаційних систем органів державної влади
Рішення РНБО "Щодо реалізації єдиної інформаційної політики в умовах воєнного стану"	Забезпечення реалізації єдиної інформаційної політики шляхом об'єднання усіх загальнонаціональних телеканалів, програмне наповнення яких складається переважно з інформаційних та/або інформаційно-аналітичних передач на єдиній інформаційній платформі стратегічної комунікації – цілодобовому інформаційному марафоні
Указ Президента Про рішення РНБО від 2021 року «Про Стратегію інформаційної безпеки»	Стратегія інформаційної безпеки визначає актуальні виклики та загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних

Джерело: розроблено на підставі даних [1; 2; 3; 4; 5; 6]

Дослідження інституційного механізму проведемо на основі аналізу функцій та завдань державних органів, які забезпечують виконання

вищезазначених нормативно-правових актів (рис.). В захисті національного інфопростору беруть участь не лише елементи Воєнної організації України, які забезпечують захист стратегічної інформації держави, кіберпростору та здійснюють протидію зовнішнім загрозам в інформаційній сфері, а також органи, які здійснюють захист інфопростору через регулювання кіноіндустрії, радіомовлення, журналістської діяльності, протидію антиукраїнської пропаганди, а також взаємодію з населенням задля розвитку навичок медіаграмотності.

З метою здійснення захисту інформаційного простору держави, шляхом протидії дезінформації та пропаганді, а також розвитку медіаграмотності населення державними органами розроблено велику кількість проєктів. Розглянемо основні та найбільш успішні.

Рисунок – Інституційний механізм забезпечення захисту національного інформаційного простору

Джерело: розроблено на підставі даних [7; 8; 9; 10; 11; 12]

З 2018 року Міносвіти разом з міжнародними організаціями запустили проєкт «Вивчай та розрізняй: інфо-медійна грамотність». Ціль проєкту – допомогти українським школярам набути навичок критичного сприйняття інформації й усвідомити цінність високоякісної інформації в контексті шкільної освіти [13].

У 2021 році шляхом об'єднання зусиль кіберполіції та громадян було створено проєкт MRIYA, основна ідея якого полягала у блокуванні телеграм-каналів нарко-магазинів через бот, що давало значний ефект. Із

початком повномасштабної війни даний бот було переформатовано на опрацювання фейкових та проросійських ресурсів, котрі в подальшому "йдуть" на блокування та перейменовано в ініціативу «StopRussia | MRIYA» [14].

Міністерство культури та інформаційної політики України у 2021 заснувало проєкт Фільтр з метою об'єднувати та координувати зусилля держави та партнерів для формування медіаграмотності як невід'ємної навички сучасних українців. Місією проєкту в умовах війни є надання українцям можливості для підвищення стійкості до дезінформації у воєнний час [15].

Окрему увагу варто приділити міжнародній співпраці України у сфері захисту національного інформаційного простору. У 2015 році була підписана Дорожня карта Партнерства у сфері стратегічних комунікацій між РНБО та Міжнародним секретаріатом НАТО [16]. Україна спільно з багатьма країнами Європи проводить зустрічі, семінари та консультації у сфері стратегічних комунікацій задля обміну досвідом у сфері боротьби з дезінформацією.

Таким чином, проведене дослідження дає змогу констатувати, що в умовах гібридної війни, поширення дезінформації та пропаганди важливу роль для захисту національного інформаційного простору відіграють усі механізми, що дають можливість попереджати або ефективно протистояти їхньому негативному впливу. Серед них окрему увагу варто приділяти удосконаленню нормативно-правового поля в умовах зростання кіберзагроз, чіткому розмежуванню обов'язків та відповідальності між органами влади, впровадженню проєктів підвищення рівня медіаграмотності населення, розвитку міжнародної співпраці.

Список використаних джерел:

1. Конституція України : офіц. текст. Київ : КМ, 2015. 98 с.
2. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII. *Відомості Верховної Ради (ВВР)*, 2018, № 31, ст.241.
3. Про державну таємницю : Закон України від від 21.01.1994 № 3855-XII. *Відомості Верховної Ради України (ВВР)*, 1994, № 16, ст.93.
4. Про затвердження завдань Національної програми інформатизації на 2022-2024 роки : Постанова Верховної Ради України від 08.07.2022 № 2360-IX. *Офіційний вісник України*, 2022 р., № 56, ст. 95.
5. Щодо реалізації єдиної інформаційної політики в умовах воєнного стану: Рішення Ради Національної безпеки та оборони України від 18 березня 2022 року № 152/2022. *Офіційний вісник України*, 2022 р., № 68, ст. 308.

6. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28 грудня 2021 року № 685/2021. *Урядовий кур'єр*, 2021 р., № 251.

7. Про Раду національної безпеки і оборони України: Закон України від 05.03.1998 № 183/98-ВР. *Відомості Верховної Ради України (ВВР)*, 1998, № 35, ст.237.

8. Про медіа : Закон України від 13.12.2022 № 2849-IX. *Голос України* від 31.12.2022 – № 267.

9. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23.02.2006 № 3475-IV. *Відомості Верховної Ради України (ВВР)*, 2006, № 30, ст.258.

10. Про затвердження Положення про Міністерство освіти і науки України : Постанова Кабінету Міністрів України від 16.10.2014 № 630. *Урядовий кур'єр* від 03.12.2014 – № 225.

11. Про затвердження Положення про Міністерство культури України: Постанова Кабінету Міністрів України від 03.09.2014 № 495. *Урядовий кур'єр* від 15.10.2014 – № 190.

12. Про розвідку : Закон України від 17.09.2020 № 912-IX. *Голос України* від 23.10.2020 – № 195.

13. «Вивчай та розрізняй: інфомедійна грамотність в освіті». Міністерство освіти та науки України. URL: https://mon.gov.ua/ua/news/vivchaj-ta-rozriznyaj-infomedijna-gramotnist-v-osviti-vidkrito-konkurs-dlya-vchiteliv (Дата звернення: 26.10.2023).

14. Платформа MRIYA : синергія Кіберполіції України та волонтерів у протидії російським окупантам у медіа-просторі. URL: https://mriya.social/ (Дата звернення: 26.10.23).

15. Фільтр: національний проєкт з медіаграмотності. URL: https://filter.mkip.gov.ua/pro-nas/ (Дата звернення: 26.10.2023).

16. Дорожня карта Партнерства у сфері стратегічних комунікацій між Радою національної безпеки і оборони України та Міжнародним секретаріатом НАТО. URL:https://www.president.gov.ua/storage/j-files-storage/00/66/78/b59dbab0d5049ff2cd77cc58800eda5c_1554906510.pdf (Дата звернення: 26.10.2023).

Кірієнко В. М.
аспірант, Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»

ВИКЛИКИ ТА ЗАГРОЗИ ПРИКОРДОННІЙ БЕЗПЕЦІ ВІД ВПРОВАДЖЕННЯ В СУЧАСНЕ ЖИТТЯ ЦИФРОВИХ ТЕХНОЛОГІЙ

В сучасному світі цифрові технології стають невід'ємною частиною нашого повсякденного життя, покращуючи методи взаємодії між людьми та впливаючи на міжнародні відносини України з країнами – партнерами в багатьох сферах співпраці.

В українському законодавстві наводиться наступне визначення терміну «цифрові технології» : це – сукупність систематизованих правових, науково-технічних, організаційних рішень, спрямованих на застосування комп'ютерної та іншої електронно-обчислювальної техніки, програмного забезпечення та інших засобів для зменшення участі користувача інформаційно-комунікаційних систем і засобів інформатизації під час збирання, приймання, обробки, передавання інформації чи трудомісткості виконуваних операцій [1].

У сфері міжнародної дипломатії цифрові технології дозволяють швидше та ефективніше обмінюватися інформацією між країнами. Електронні засоби зв'язку та соціальні мережі, такі як Facebook, WhatsApp, Instagram роблять комунікацію між представниками урядів та громадкістю більш доступними. Це сприяє вирішенню міжнародних питань, полегшує проведення дипломатичних переговорів, та сприяє подальшому розвитку співпраці.

Зокрема, в економічній сфері цифрові технології сприяють збільшенню обсягів міжнародної торгівлі та інвестицій. Електронні фінансові системи, онлайн – платформи та інші цифрові інструменти дозволяють підприємствам швидше знаходити нових партнерів, проводити трансграничні операції та розширювати свої ринки.

Впровадження цифрових технологій у сфері національної безпеки перетворює парадигму захисту України у більшу спроможність, забезпечуючи більш ефективний контроль і реагування на потенційні загрози. Сучасні системи моніторингу та аналізу дозволяють оперативно виявляти та реагувати на надзвичайні події, які несуть серйозну загрозу, особливо, для важливої складової забезпечення національної безпеки, а саме для прикордонної безпеки.

Приділяючи увагу прикордонній безпеці, як важливій складовій національної безпеки, можна констатувати, що *прикордонна безпека* – це за-

хищеність життєво важливих інтересів особи, суспільства і держави в її прикордонному просторі, при якому, суспільству, державі та особі, створюються умови для реалізації їх інтересів, пов'язаних із свободою пересування через державний кордон [2], шляхом оперативного виявлення та припинення порушень законів, а також вжиття заходів щодо протидії загрозам національній безпеці на державному кордоні України, та систематичної роботи з вирішення причин, що призводять до їх виникнення.

У сучасному світі, в галузі прикордонної безпеки, експоненційне (імпульсне, стрімке) зростання обсягів інформації визначається технологічним прогресом, який надає людям здатність швидко та ефективно обмінюватися даними. Водночас, незважаючи на очевидні переваги цього явища, виникають серйозні виклики та загрози в контексті забезпечення прикордонного контролю, який здійснюється з метою протидії незаконному переміщенню осіб через державний кордон, незаконній міграції, торгівлі людьми, а також незаконному переміщенню зброї, наркотичних засобів, психотропних речовин і прекурсорів, боєприпасів, вибухових речовин, матеріалів і предметів, заборонених до переміщення через державний кордон [3].

Однією з ключових проблем є можливість незаконного збору та використання інформації, а саме персональних даних, тобто відомостей чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [4], що ставить під загрозу не лише приватність особи, але й безпеку країни в цілому.

Сучасні технології дозволяють ефективно відстежувати та аналізувати величезні потоки даних, що збираються в прикордонних відділах. Проте це також створює ризик зловживання цифровими можливостями з метою недозволеного доступу до особистої інформації громадян службових осіб, порушуючи таким чином їхні права на конфіденційність.

Поширення контрабанди, тобто переміщення через митний кордон України поза митним контролем або з приховуванням від митного контролю культурних цінностей, отруйних, сильнодіючих, вибухових речовин, радіоактивних матеріалів, зброї або боєприпасів (крім гладкоствольної мисливської або бойових припасів до неї), частин вогнепальної нарізної зброї, а також спеціальних технічних засобів негласного отримання інформації [5] є ще однією проблемою, яку створює цифрова епоха в сфері прикордонної безпеки.

За допомогою високотехнологічних засобів зловмисник можуть легко обходити системи контролю та безпеки, використовуючи різноманітні методи та засоби для приховування та перевезення через державний кордон України заборонених речей. Це вимагає постійного вдосконалення

технічних та аналітичних засобів та заходів, задля виявлення та протидії новим методам контрабанди.

Також, існує загроза вчинення терористичних актів, тобто застосування зброї, вчинення вибуху, підпалу чи інших дій, які створювали небезпеку для життя чи здоров'я людини або заподіяння значної майнової шкоди чи настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, міжнародного ускладнення, або з метою впливу на ухвалення рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об'єднаннями громадян, юридичними особами, або привернення уваги громадськості до певних політичних, релігійних чи інших поглядів винного (терориста), а також погроза вчинення зазначених дій з тією самою метою [5] з використанням цифрових технологій.

Терористи можуть використовувати високотехнологічні методи для організації та координації своїх дій, а також для обходу систем безпеки прикордонного контролю. Це вимагає особливої співпраці між Україною та країнами – партнерами у сфері забезпечення безпеки на кордоні, та розвитку спеціалізованих технічних рішень для виявлення та запобігання терористичним загрозам.

Для мінімізації настання негативних наслідків з боку цих викликів, міжнародні спільноти повинні співпрацювати в області обміну інформації та розробки певних технічних стандартів в сфері забезпечення безпеки на кордоні. Підвищення кількості та якості обміну даними між прикордонними відомствами країн – партнерів, дозволить ефективніше реагувати на потенційні загрози. Також важливо вдосконалювати технічні рішення для забезпечення прикордонного контролю, такі як системи розпізнавання облич, високоточні сенсори та інші інноваційні технології.

Отже, в контексті прикордонної безпеки, в епоху розвитку цифрових технологій, важливо не лише враховувати можливості технологій, але й усвідомлювати ризики які вони несуть. Для ефективного управління та захисту від загроз, які надходять безпосередньо від використання цифрових технологій, необхідно об'єднувати зусилля як на національному, так і на міжнародному рівнях, більш активно впроваджувати у системи здійснення прикордонного контролю сучасні досягнення у сфері цифрових технологій.

Список використаних джерел:

1. Про Національну програму інформатизації: Закон України від 01.12.2022 р. №2807-IX URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text (дата звернення 11.11.2023).

2. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення 10.11.2023).

3. Про прикордонний контроль: Закон України від 05.11.2009 р. № 1710-VI URL: https://zakon.rada.gov.ua/laws/show/1710-17#Text (дата звернення 18.11.2023). 4. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення 18.11.2023).

5. Кримінальний кодекс України: Закон України від 05.03.2001 р. №2341-III URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення 18.11.2023).

Григор'єва М. Є.
кандидат юридичних наук, доцент,
асистент кафедри кримінального
права Національного юридичного
університету імені Ярослава Мудрого

КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ТА ЦИФРОВА ТРАНСФОРМАЦІЯ

Розвиток науково-технічного прогресу, використання новітніх технологій ставить перед суспільством та державою нові завдання. І перед нами, ученими – правниками, постали виклики щодо забезпечення належного правового регулювання тих суспільних відносин, яких ми не знали і навіть не могли уявити, що вони будуть існувати.

Ми не надто замислювалися над проблематикою кримінальної відповідальності за кримінальні порушення у сфері кібербезпеки чи цифровізації суспільних процесів. А сьогодні життя актуалізувало ці питання і висунуло цілу низку завдань, і перед кримінальним правом у тому числі.

Очевидно, що процес соціальної трансформації, тобто процес змін у суспільстві, спрямований на поліпшення якості життя людей, їхніх соціальних відносин, прав та можливостей існував завжди. Відбувалися реформи у сферах освіти, охорони здоров'я, соціального захисту та інших аспектів соціального життя. А от із цифровою трансформацією, з процесом використання сучасних технологій і цифрових інструментів для покращення діяльності у всіх сферах суспільства, із впровадженням інтернет-технологій, розробкою цифрових платформ, використанням

штучного інтелекту та інших інновацій для оптимізації процесів у бізнесі, освіті, медицині та інших галузях ми зіткнулися не так давно.

Чому ми вимушені говорити саме про кримінальну відповідальність щодо порушення суспільних відносин у цих сферах? Тому що охорона суспільних відносин із залученням сучасних технологій та цифрових інструментів є нагальною потребою в сучасних умовах технічного прогресу. Кримінальні правопорушення у цій сфері можуть завдавати найтяжчу шкоду, яка тільки може бути заподіяна суспільним відносинам.

На сьогоднішній день вже гостро стоїть питання щодо забезпечення захисту персональних даних. Із розвитком цифрових технологій збільшується кількість особистої інформації, що зберігається в електронному вигляді та яку можна віднести до конфіденційної інформації. Тому кримінальне право повинно забезпечити захист цих даних від несанкціонованого доступу та зловживань. Також потребують урегулювання питання щодо збору, збереження та використання цієї особистої інформації, зокрема вимоги до згоди особи на обробку її даних, обов'язки організацій з їх захисту та відповідальність за порушення цих вимог. Наприклад, у медицині Інтернет речей дозволяє збирати дані про стан пацієнтів у реальному часі, виявляти аномалії та надсилати сповіщення лікарям. У побутовій сфері Інтернет речей дозволяє створювати «розумні» пристрої, які можуть автоматично регулювати свою роботу з урахуванням звичок їх користувачів і таким чином формувати банк даних про звички особи, її вподобання, темперамент, психологічні характеристики. Такі персональні дані також можна віднести до конфіденційної інформації, що потребує захисту.

При цьому особливе занепокоєння у кримінально-правовому сенсі викликають проблеми щодо урегулювання питань, пов'язаних із нейрохакінгом, тобто процесом використання різних методів, технік або технологій для зміни функціонування мозку з метою покращення когнітивних здібностей, емоційного стану, пам'яті, уваги тощо. Він може включати в себе використання спеціальних харчових добавок, медитації, нейростимуляції, навчання розумовим технікам тощо. Нейрохакінг широко застосовує біофідбек, тобто такий метод психологічної терапії, який використовується для навчання людини контролювати свої фізіологічні процеси, такі як серцевий ритм, дихання, м'язова напруга тощо. Цей метод базується на використанні спеціального обладнання, яке дозволяє вимірювати ці фізіологічні параметри і надавати звіт, позитивний або негативний відгук, коментар або реакцію (фідбек) про їх стан, що допомагає людині оцінити свої зусилля і вдосконалити свої навички. За допомогою тренування і практики людина може навчитися контролю-

вати ці процеси і досягати психофізіологічної гармонії. Всі ці питання тісно пов'язані із волевиявленням людини, із її можливістю усвідомлювати свої дії і керувати ними. Втручання в процеси, що відбуваються в головному мозку несуть багато загроз для особистості.

Так, у світі є випадки застосування нейрохакінгу. Наприклад, у деяких країнах вже використовуються спеціальні пристрої для нейростимуляції мозку, які призначені для покращення когнітивних функцій. Також існують компанії, які розробляють харчові добавки та напої, які призначені для покращення пам'яті та уваги. У деяких спортивних галузях також застосовується нейрохакінг для підвищення концентрації та реакційної швидкості спортсменів.

Найпоширеніші випадки застосування нейрохакінгу в світі:

1.) використання транскраниальної магнитної стимуляції (TMS) для покращення пам'яті та навчання;

2.) використання спеціальних харчових добавок з риб'ячими жирами, креатином та іншими компонентами для покращення когнітивних функцій;

3.) використання нейрофідбеку для тренування мозку та покращення уваги та концентрації;

4.) використання спеціальних апаратів для нейростимуляції мозку в медичних цілях, наприклад, для лікування депресії або розладів уваги;

5.) використання нейротехнологій у військових цілях, наприклад, для покращення реакційної швидкості та прийняття швидких рішень;

6.) використання віртуальної реальності для тренування мозку та покращення когнітивних функцій, таких як увага, пам'ять та швидкість прийняття рішень;

7.) використання мозкових імплантатів для відновлення втрачених функцій мозку після травм або хвороб, таких як інсульт тощо;

8.) використання технологій глибокої мозкової стимуляції для лікування різних неврологічних захворювань, таких як хвороба Паркінсона, Альцгеймера, втрата пам'яті;

9.) використання нейроінтерфейсів для взаємодії з комп'ютерами та іншими пристроями за допомогою мозкових сигналів;

10.) використання технологій мозкового картографування для дослідження мозкової активності та розвитку нових методів лікування розладів мозку.

В Україні, як і в більшості держав у світі, ще не існує кримінально-правового урегулювання питання використання нейрохакінгу. Проте деякі країни, такі як США, Японія, та країни Європейського союзу, почали вже робити перші кроки у напрямку створення кримінально-правового

законодавства щодо урегулювання питань використання нейротехнологій. Наприклад, у США Федеральна комісія з торгівлі вже проводила слухання на тему етичних та правових аспектів використання нейротехнологій. Також, у Японії було створено експертну групу для обговорення питань етики та безпеки нейротехнологій. Тому сподіваємося, що у найближчому майбутньому можна очікувати появу і в Україні кримінального-правових приписів щодо використання нейротехнологій. Слід зазначити, що при цьому важливим моментом є обов'язкове врахування заходів безпеки, які можна вжити для запобігання нейрохакінгу, а саме:

а) захист від несанкціонованого доступу до нейротехнологій (забезпечення надійними системами аутентифікації та авторизації, які будуть запобігати несанкціонованому доступу до нейроінтерфейсів);

б) можливість шифрування даних (всі дані, які зберігаються або передаються за допомогою нейротехнологій, повинні бути зашифровані для захисту від несанкціонованого доступу);

в) захист від вірусів та шкідливих програм (створення відповідних умов для регулярного оновлення програмного забезпечення та використання антивірусних програм для захисту від вірусів та шкідливих програм);

г) фізичний захист (нейротехнологічні пристрої повинні бути фізично захищені від несанкціонованого доступу, наприклад, шляхом обмеження доступу до них та використання фізичних бар'єрів);

ґ) регулярна перевірка на безпеку (забезпечення проведення регулярних аудитів безпеки нейротехнологій для виявлення потенційних уразливостей та вжиття заходів їх усунення);

д) забезпечення використання біометричних методів ідентифікації (використання біометричних даних, таких як відбитки пальців або розпізнавання обличчя, для автентифікації користувачів нейротехнологій);

є) забезпечення обмеження доступу до нейротехнологій (встановлення жорстких правил доступу до нейротехнологій, щоб забезпечити, що лише авторизовані користувачі мають доступ до них);

ж) забезпечення захисту від атак на мережу (застосування заходів захисту мережі, таких як брандмауери та інші методи захисту, для запобігання несанкціонованому доступу до нейротехнологій через мережу);

з) забезпечення постійного навчання користувачів (навчання користувачів запобіганню потенційних загроз та методів захисту від них, щоб встановити свідоме та відповідальне використання нейротехнологій).

Ми назвали лише деякі заходи безпеки, які можна вжити для запобігання нейрохакінгу, що мають бути відображені у кримінальному законодавстві, але при цьому слід враховувати, що розвиток нових техноло-

гій та стандартів безпеки для постійного покращення захисту використання нейротехнологій, спонукають для подальшого наукового пошуку в цьому напрямі.

Загалом, кримінально-правове регулювання забезпечення інформаційних прав людини в умовах цифрової трансформації повинно бути гнучким, прогресивним, готовим до постійних змін та до нових викликів, які виникають у зв'язку з розвитком цифрових технологій, і повинно забезпечувати захист прав людини в цифровому середовищі.

Федюк В. В.
молодший науковий співробітник
Науково-дослідного інституту
вивчення проблем злочинності ім.
академіка В. В. Сташиса НАПрН
України

ПОНЯТТЯ КІБЕРЗЛОЧИНУ ТА ЙОГО ЗАСТОСУВАННЯ В НОРМАХ ЗАКОНУ ПРО КРИМІНАЛЬНУ ВІДПОВІДАЛЬНІСТЬ1

Бурхливий розвиток цифрових технологій та постійне вдосконалення механізмів комунікації із використанням кіберпростору, з одного боку, сприяють прогресу суспільного життя, а з іншого – породжують нові несприятливі для суспільства виклики. Серед таких викликів чи не найбільш серйозним виступає поширення кіберзлочинності, основною «одиницею виміру» якої є кіберзлочин. Оскільки у Кримінальному кодексі України (далі –КК України) поняття останнього не формалізовано, то невирішеним залишається питання віднесення в межах цього нормативно-правового акту тих чи інших суспільно небезпечних діянь саме до таких, що відповідають ознакам кіберзлочинів у повному обсязі, та які норми Особливої частини КК України передбачають кримінальну відповідальність за їх вчинення.

Поняття кіберзлочину ставало предметом наукових розвідок багатьох сучасних дослідників кримінального права. Слід відмітити напрацювання О. І. Деньковича, який узагальнив висловлені позиції інших науковців стосовно критеріїв віднесення кримінального правопорушення до кіберз-

[1] *Примітка.* Тези виконано в межах фундаментальної теми «Теоретичні, законодавчі та правозастосовні проблеми кримінально-правової охорони інформаційної безпеки в України» (номер державної реєстрації 0121U114324).

лочину. Відповідно до такого узагальнення кіберзлочинами визнаються: 1) кримінальні правопорушення (дотримуючись чинної термінології КК України), передбачені розділом XVI Особливої частини КК України; 2) кримінальні правопорушення, предметом яких є комп'ютерна інформація; 3) кримінальні правопорушення, в яких комп'ютер є або предметом кримінального правопорушення, або знаряддям, або способом його вчинення; 4) кримінальне правопорушення, в яких кіберпростір є середовищем, предметом (метою) посягання та/або способом вчинення [1, с. 19-20]. Слід звернути увагу і на законодавче визначення кіберзлочину, що надано поза КК України. Відповідно до п. 8 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017 р. (далі – Закон) кіберзлочином (комп'ютерним злочином) є «суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України». Варто констатувати, що наразі таке визначення не враховує положення чинного КК України в аспекті поділу кримінальних правопорушень на кримінальні проступки та злочини, проте, як видається, воно відображає основні характеристики розглядуваного поняття. Йдеться про те, що, по-перше, було здійснено ототожнення кіберзлочину та комп'ютерного злочину, а по-друге, визначено його специфіку (вчинення діяння у кіберпросторі та/або з його використанням). А тому основним завданням вбачається, враховуючи розмаїтість процесів у кіберпросторі та особливостей їх протікання, виокремлення безпосередньо кіберзлочинів (у вузькому розумінні, як комп'ютерних), так і суспільно небезпечних винних діянь, які посягають на абсолютно різні об'єкти кримінально-правової охорони, але використовують кіберпростір, як предмет, знаряддя чи засіб їх вчинення (кіберзлочини у широкому розумінні). Так, згідно з абз. 9 п. 3 Стратегії кібербезпеки України, затвердженої Указом Президента України № 447/2021 від 26.08.2021 р., набуває поширення використання кіберпростору для вчинення злочинів проти основ національної безпеки України, а також кримінальних правопорушень, пов'язаних із легалізацією доходів, одержаних злочинним шляхом, торгівлею людьми, незаконним поводженням зі зброєю, бойовими припасами або вибуховими речовинами, незаконним обігом наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інших предметів і речовин, які загрожують життю та здоров'ю людей тощо.

Тому з метою адекватного розуміння та застосування всього обсягу поняття «кіберзлочин» щодо тлумачення певних діянь, передбачених

нормами Особливої частини КК України, як кримінальних правопорушень безпосередньо у сфері «кібер» (т.зв. комп'ютерних) та кіберзлочинів у широкому розумінні необхідно розмежувати ці поняття, які в Законі вживаються як синоніми. Так, зазначається, що комп'ютерним злочином є протиправне втручання в роботу кібернетичних систем, основною управляючою ланкою яких є комп'ютер (наприклад, спотворення інформації про стан об'єкта в каналі зворотного зв'язку, спотворення керуючого сигналу й каналу зв'язку, використання шкідливого програмного забезпечення тощо), створення та використання в злочинних цілях певної кібернетичної (комп'ютерної) системи, використання в злочинних цілях існуючих кібернетичних (комп'ютерних) систем (наприклад комп'ютерних чи телекомунікаційних мереж у шахрайстві, вимаганні тощо). Натомість, кіберзлочином є злочин, пов'язаний із використанням кібернетичних комп'ютерних систем, та злочин в кіберпросторі. Під кіберпростором слід розуміти штучне електронне середовище існування інформаційних об'єктів у цифровій формі або простір, представлений інформаційно-комунікаційними системами, у якому проходять процеси перетворення (створення, зберігання, обміну та знищення) інформації, представленої у вигляді електронних комп'ютерних даних [2, с. 85-86].

Особливістю кіберзлочину є те, що він пов'язаний із використанням саме кібернетичних технологій у межах однієї комп'ютерної мережі або декількох таких мереж, як складової інформаційної (автоматизованої), інформаційно-комунікаційної чи електронної комунікаційної систем. На відміну від цього, комп'ютерний злочин – це діяння, що, передусім, вчиняється з використанням будь-якої комп'ютерної техніки. Формами кримінально протиправного використання кібернетичних технологій у межах комп'ютерних мереж можуть бути, приміром, несанкціоноване отримання прав керування комп'ютерною мережею та її нерегламентоване використання (наприклад, із метою спричинення аварії на виробництві шляхом дезорганізації управлінської діяльності підприємства), а також створення та використання в злочинних цілях однієї комп'ютерної мережі (або поєднання декількох) проти інших таких мереж (наприклад, створення мережі заражених комп'ютерів для здійснення атак на веб-сайти тощо).

Отже, поняття кіберзлочину є багатогранним. При застосуванні норм закону про кримінальну відповідальність кіберзлочин не слід зводити до поняття «комп'ютерного кримінального правопорушення» (розділ XVI Особливої частини КК України), а враховувати, що таке діяння (кіберзлочин) вчиняється у кіберпросторі та/або з його використанням, що, як правило, супроводжується посяганнями на інші об'єкти кримінально-правової охорони.

Список використаних джерел:

1. Кіберзлочинність та електронні докази = cyber crime and digital evidence: навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. О. Денькович, д-р права, проф. Габріеле Шмельцер. Львів : ЛНУ ім. Івана Франка, 2022. 298 с.

2. Словник термінів з кібербезпеки / за заг. ред. О. В. Копана,Є. Д. Скулиша. К.: ВБ «АванпостПрим», 2012. 214 с.

Негребецький В. В.
кандидат юридичних наук, доцент,
науковий співробітник НДІ вивчення
проблем злочинності імені академіка
В. В. Сташиса НАПрН України,

ПРОБЛЕМИ ВИКОРИСТАННЯ КРИМІНАЛІСТИЧНИХ ЦИФРОВИХ ТЕХНОЛОГІЙ ДОКУМЕНТУВАННЯ НАСЛІДКІВ ВІЙНИ

Розслідування і документування воєнних злочинів – найважливіший напрямок у роботі правоохоронних органів України. Вирішальне значення має професійне, якісне, повне, всебічне, допустиме, вчасне та належне документування всіх елементів воєнного злочину. Станом на 20 листопада 2023 року Офісом Генеральної прокуратури зареєстровано понад 113 000 випадків воєнних злочинів та широкомасштабної агресії російської федерації проти України [1]. Задокументовані чисельні випадки руйнувань житлової інфраструктури, вбивств мирних жителів, мародерства та насильства. Зібрані докази згодом дозволять не лише довести, що ці злочини було вчинено, а й пов'язати їх із конкретними особами (злочинцями), висунути їм обґрунтовані обвинувачення та притягнути до відповідальності.

Документування переслідує не лише мету подальшого розслідування та притягнення до відповідальності.

Фіксація та збір фото, відео з відкритих джерел, інтерв'ювання та подальше цифрове архівування скоріш за все дозволить зберегти історію правдивою, без зайвих домислів, з неможливістю її спотворення будь-якою зі сторін. Зібрані вчасно, всебічно та якісно докази завжди несуть у собі сліди істини, від якої не захиститись ані державі-агресору, ані зраднику-політику. Правда завжди змусить порушника як мінімум домовлятись [2].

Задокументовані та поширені особисті історії людей, що зазнали насильство, жорстоке та нелюдське поводження, приниження людської гідності привернуть увагу недотичної частини суспільства до нестерпного збройного конфлікту та дасть можливість створити нові рекомендації та механізми захисту прав людини.

Документування та збережені факти руйнування, пошкодження, вбивства та інші воєнні злочини дозволять не лише претендувати, а і реально отримувати відшкодування, будь-то репарації, контрибуції, сатисфакції тощо.

Ретельна фіксація дозволить включення точного опису минулого насильства в навчальні/освітні програми, у тому числі задля запобігання повторенню.

Сучасними завданнями цифрової криміналістики є пошук і аналіз цифрових слідів, аналіз даних, збирання доказової інформації у цифровому середовищі. Під цифровими доказами необхідно розуміти фактичні дані, які представлені у вигляді бінарного (двійкового) коду та містять інформацію, що має значення для об'єктивного вирішення справи [3]. В Україні створено цифрових платформ, призначених для збирання доказів воєнних злочинів в Україні, зокрема:

- Застосунок eyeWitness to Atrocities від Міжнародної асоціації юристів (IBA);
- Платформа WarCrimes (warcrimes.gov.ua) на базі Офісу Генерального прокурора України;
- War Crime Bot – для документування доказів порушень міжнародного гуманітарного права, прав людини і злочинів;
- TRIBUNAL UA – чатбот для фіксації фото-і відеодоказів вбивств, насильства, пограбувань цивільних або військових окупантами;
- SaveEcoBot – чатбот для повідомлень про злочини проти навколишнього середовища, що здійснюються на території України;
- Портал «Доказ» (dokaz.gov.ua);
- Портал «Культурні злочини» (culturecrimes.mkip.gov.ua) для збору доказів руйнування російською армією історичних та культурних пам'яток.

Так, на єдиній загальнодержавній платформі https://warcrimes.gov.ua/ здійснюється збирання та документування доказів про воєнні злочини держави – агресора. Таким чином, на базі Офісу Генерального прокурора України фактично було створено сучасну платформу для документування воєнних злочинів на Україні з можливістю надання документів, фото та відео.

Вважаємо, що найбільш технічно оснащеним для потреб збору доказів воєнних злочинів є додаток від Міжнародної асоціації юристів

«eyeWitness to Atrocities». Додаток розроблено за ініціативи Міжнародної асоціації юристів (IBA) в 2011 році. Користувачі програми завантажують свої кадри на захищений сервер для верифікації та безпечного зберігання. Фотографії та відео, зроблені за допомогою програми «eyeWitness to Atrocities», можна легко перевірити на предмет використання в якості доказів. Крім того, eyeWitness попіклуватиметься , щоб надані користувачем фото або відео були надані компетентним органам [4].

Офіс Верховного комісара ООН із прав людини та Центр з прав людини Каліфорнійського університету в Берклі у 2020 р. представили «практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права з прав людини та гуманітарного права», який містить стандарти й методологічні підходи до «збору, збереження та аналізу інформації у відкритому доступі, яка може бути представлена як доказ у кримінальних процесах» [5].

Нажаль, норми Кримінального процесуального кодексу України не передбачають окремої категорії цифрових доказів. У КПК відсутнє визначення терміна «цифрові докази», не наведено докладного порядку їх вилучення, огляду, фіксування та зберігання. Тому у слідчих і суддів часто виникають труднощі у збиранні, оцінюванні цифрових доказів через відсутність у законодавстві України їх визначення, порядку фіксування й оцінки. При цьому використання цифрових доказів для документування випадків воєнних злочинів держави-агресора проти України є край необхідним. Документування не дасть можливості існувати та поширюватись брехливим спотворенням реальної історії боротьби України за незалежність.

Список використаних джерел:

1. Злочини, вчинені в період повномасштабного вторгнення рф станом на 20.11.23. URL: https://www.gp.gov.ua/

2. Shepitko, V. Y., Shepitko, M. V. (2021) The role of forensic science and forensic examination in international cooperation in the investigation of crimes. Journal of the National Academy of Legal Sciences of Ukraine, no. 28(1), pp. 179–186 (in English).

3. Звернення. (04.03.2022) URL: https://crimcongress.com/news/звернення/ (дата звернення: 20.11.2023).

4. Шевчук В. М. Криміналістичне забезпечення розслідування воєнних злочинів: цифровізація, інновації, перспективи. URL: http://www.baltijapublishing.lv/omp/index.php/bp/catalog/download/322/8791/18392-1. (дата звернення: 20.11.2023).

5. Галина Авдєєва, Ельжбета Живуцька-Козловська. Проблеми використання цифрових доказів у кримінальному судочинстві України та США. URL: https://khrife-journal.org/index.php/journal/article/download/564/633

6. Гладкий Д. В. Особливості використання програми «eyeWitness to Atrocities» в Україні для фіксації воєнних злочинів рф // Державна безпека України в умовах російської агресії: актуальні питання експертно-криміналістичного та науково-технічного забезпечення: збірник матеріалів Всеукраїнської науково-практичної конференції, 22 серпня 2023 р.: Том 2. Київ: ІСТЕ СБУ, 2023. С.29-31.

7. Протокол Берклі. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf (дата звернення: 20.11.2023).

Матвєєвський О. В.
старший викладач НУ ОМА

ПРАВОВІ ПРОБЛЕМИ ВИКОРИСТАННЯ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОЦЕСІ, ООТРИМАНИХ ЗА ДОПОМОГОЮ ЦИФРОВИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

В монографії доктора юридичних наук Савіновій Н. А. «Кримінально-правова політика та убезпечення інформаційного суспільства в Україні» позначено, що сучасне кримінально-правове забезпечення розвитку в Україні інформаційного суспільства має приймати на себе одну з найважливіших функцій держави в інформаційному середовищі – забезпечення засобами кримінально-процесуального права суспільних відносин, які відбуваються з використанням інформаційно цифрових технологій [4, с.6]. Одним із засобів такого забезпечення стає сучасна цифрова криміналістика.

Цифрова криміналістика, яка з погляду науковців, є «однією з галузей криміналістики, яка зосереджена на кримінально-процесуальному праві і доказах стосовно комп'ютерів і пов'язаних з ними пристроїв» [2, с.29] ставить перед сучасними правниками низку важливих питань використання доказової інформації, отриманої за допомогою цифрових технологій (наприклад: з використанням протоколу Берклі). Мобільні пристрої (телефони, смартфони тощо), ігрові приставки та інші пристрої, що функціонують через Інтернет (пристрої для здоров'я та фітнесу та

медичні прилади тощо) дозволяють цифровій криміналістиці збирати, отримувати, зберігати, аналізувати та подавати електронні докази (також відомих як цифрові докази) в якості оперативно-розшукових відомостей і здійснювати розслідування та кримінальне переслідування по відношенню до різних видів злочинів.

Разом з тим, для «цифрових» слідів характері специфічні якості, що визначають перспективи їх реєстрації, вилучення і використання як доказів під час розслідування злочину тому що такий вид слідів відбивається на носіях інформації у вигляді сигналів, кодів, зарядів, полів і повинен вилучатися або з носієм інформації, або шляхом копіювання з використанням спеціальних програмних продуктів, бажано із залученням спеціалістів. Виходячі з вищевикладеного треба сказати, що:

– по-перше, комп'ютерна інформація існує на певних носіях, але недоступна для безпосереднього спостереження. Тобто для її виявлення та дослідження необхідне використання технічних та програмних засобів, що ставить під загрозу її подальше доказове значення, адже вказані засоби повинні бути сертифікованими і використовуватися відповідними спеціалістами;
– по-друге, комп'ютерна інформація представлена на цифрових носіях в числовій формі за допомогою знаків "1" і "0", а вся інформація іншого характеру, яка вноситься в комп'ютер (тексти, графіка, відео, аудіо), перетворюється у форму, зрозумілу для ЕОМ, – цифрову;
– по-третє, така інформація, хоча і є стабільною за змістом, може бути по-різному сприйнята залежно від засобів зчитування, декодування та відображення. Наприклад, використання невірного засобу декодування тексту особою, що бажає ознайомитись з електронним документом, призведе до виводу на дисплей або принтер незрозумілого набору символів.[3, с 30].

Також слід зазначити, що цифрова криміналістична інформація отримана за допомогою цифрових інформаційних технологій потребує застосування спеціальних знань: проведення експертних досліджень, інших досліджень комп'ютерної інформації, враховуючи її пошук та виїмку, консультації спеціалістів. [1, С. 379] Це свідчить, що у будь-якому випадку, коли слідчий чи інша процесуальна особа має справу з комп'ютерною інформацією, вона не може сприймати її без залучення до цього процесу відповідних спеціалістів, тому що всіх аспектів поводження з цифровими даними не може знати навіть найобдарованіший юрист, а втратити або пошкодити такий вид джерела криміналістичної інформації надзвичайно легко. Тобто для надання цифровій інформації статусу доказів по-

трібна достатньо тривала процедура криміналістичного дослідження її відповідними спеціалістами.

Тому негативною стороною, на мою думку, є те, що правоохоронні органи витрачатимуть більше часу на досудове розслідування, а суди відповідно на судовий розгляд, оскільки потенційно можуть існувати сотні тисяч фотографій, відео та публікацій, які мають бути перевірені та досліджені всіма сторонами процесу.

Варто зазначити, що, наприклад, в Україні діє Національний стандарт України що до інформаційні технології збирання, отримання та збереження цифрових доказів, який стосується не лише цифрових доказів у відкритих джерелах, а й цифрових даних на конкретних пристроях. Проте, інститут електронних доказів у КПК України не деталізований і не врегульований на достатньому рівні, саме тому питання внесення відповідних змін до КПК України є нагальним, у тому числі щодо чіткого визначення поняття та видів електронних доказів, а також доповнення переліку процесуальних джерел доказів та розмежування поняття електронного документа як офіційного документа та інших документів, що подаються в електронній формі.

Підсумовуючи вищевикладене, необхідно зазначити що, у реаліях сучасного світу в умовах нових інформаційних цифрових технологій цифрова інформація є вигідною всім сторонам кримінального процесу, оскільки допоможе підвищити стандарти розслідування і судового розгляду але кримінально-процесуальне законодавство України потребує нагальних змін для того щоб цифрові докази стали достатніми, допустимими і належними.

Список використаних джерел:

1. Колодіна А. С Цифрова криміналістика: проблеми теорії і практики. *Юридичний науковий електронний журнал* – № 4. 2022. С. 378-380.

2. Maras M.-.H. Computer forensics: cybercriminals, laws, and evidence. *Jones & Bartlett Learning*. – №2. 2014. С.18-32.

3. Ращенко Є. Комп'ютерні данні як носій криміналістичної інформації про злочини у сфері компютерних технологій *Правова інформатика*. – № 1(13), 2007. С. 21-38.

4. Савінова Н. А., Кримінально-правова політика та убезпечення інформаційного суспільства в Україні. Монографія. *редакція журналу «Право України»*. Київ. 2012. 247 с.

Свєтлічний І. В.
аспірант відділу кримінального права, кримінології та судоустрою Інституту держави і права ім. В. М. Корецького Національної академії наук України, адвокат
ORCID: https://orcid.org/0000-0001-7328-548X
Бурчак Л. І.
аспірант Інституту інформації, безпеки і права НАПрН України, адвокат
ORCID: https://orcid.org/0009-0004-5116-4694

ГЕНЕЗИС РОЗВИТКУ ВІДНОВНОГО ПРАВОСУДДЯ ЯК ІНСТРУМЕНТУ ПРОТИДІЇ ЗЛОЧИННОСТІ НЕПОВНОЛІТНІХ В КРАЇНАХ ЄВРОПИ

Соціальна трансформація, як відомо, це період становлення нових соціальних форм, утвердження нових принципів соціального устрою та виникнення нових соціальних інститутів. Відновне правосуддя, саме в такій формі, як воно існує сьогодні, сформувалося у середині 70-х років XX століття, але інтерес до відновлення порушених прав потерпілого мав місце ще в концепціях правосуддя стародавнього світу [1].

З кінця середньовіччя в Європі виникла система правосуддя, в якій зобов'язання правопорушника були скоріше перед державою, ніж не перед потерпілим, яка існує до наших часів.

Підхід, що лежить в основі концепції відновного правосуддя (restorative justice) надає можливості сторонам конфлікту відновити стан, який вони разом вважають справедливим, та завдяки цьому відновити стосунки. Що таке є справедливість для обох сторін? Справедливість є такою специфікацією стосунків між індивідами, коли всі вони усвідомлюють себе рівними стосовно певного раціонального принципу [2].

Відновне правосуддя не є заміною традиційного правосуддя, відновне правосуддя може бути одним з правових інструментів протидії злочинності, який надає правосуддю відновного характеру за рахунок використання певного способу вирішення кримінальних ситуацій і цей інструмент є ефективним, в першу чергу, стосовно неповнолітніх.

Тенденція до гуманізації суспільства, що зародилася в XVI-XVII століттях, значно посилилася в другій половині XX століття, коли європей-

ські науковці хоч і не використовували поняття «відновне правосуддя», але зосереджували увагу на недоліках тогочасної системи кримінального судочинства, особливо стосовно прав потерпілих [3].

Важливе місце в розвитку відновного правосуддя посідають праці німецького кримінолога Ганса фон Гентінга та румунського кримінолога Бенджаміна Мендельсона. Вони вважали, що потерпілі мають розглядатися не тільки як пасивні об'єкти злочину, а й як активні суб'єкти. Крім того, вони вважали, що в кримінальному процесі слід говорити насамперед про права потерпілих, а не про права правопорушників. На той час ці ідеї були революційними для юриспруденції, для правової науки в цілому [4].

Вивченням та дослідженням зазначених питань займалися також німецький кримінолог Сара Марджорі Фрей та американський учений Стівен Шеффер. Так, до прикладу, Фрей стверджувала, що система кримінального правосуддя ігнорує потерпілих і пропонувала обов'язкове відшкодування шкоди як використання принципу «повернення до попереднього стану». Шеффер, зокрема, стверджував, що інтерес до відновлення порушених прав бере свій початок в уявленнях стародавнього світу. На думку дослідника, до кінця Середньовіччя ці уявлення були забуті, і виникла судова система, яка визначала обов'язок порушника перед державою, а не перед потерпілим [5].

1975 року Мішель Фуко опублікував роботу, в якій однією з основних ідей була еволюція політичних технологій у західних суспільствах під час переходу від пізнього Середньовіччя до Нової історії і далі. Він зазначив, що з плином часу каральні механізми державної влади ставали дедалі гуманнішими. Злочинці стали відбувати покарання у в'язниці, скоротилася кількість тілесних покарань. Іншими словами, змінилася сама правова природа покарання. Сформувалися нові уявлення про суб'єкта правопорушення, ним стала людська свідомість [6].

Згодом критика системи кримінальних покарань у науковій доктрині поступилася місцем новій концепції відновного правосуддя, що пропонувала альтернативний підхід до розв'язання кримінальних спорів У 1970-1980-х роках низка кримінологів і психологів у Норвегії, Нідерландах та інших країнах виступили за відмову від довгих строків тюремного ув'язнення. У їхніх роботах пропонували як альтернативи тюремному ув'язненню, так і способи скорочення кількості вироків. Американський психолог доктор Альберт Іглаш і норвезький кримінолог Нільс Крісті першими звернули увагу на кризу системи кримінального правосуддя й альтернативні парадигми, які в деяких випадках могли б істотно замінити каральні функції правосуддя.

Погляди норвезького кримінолога Нільса Крісті були прогресивними для того часу. Він виступав проти смертної кари, проти збільшення кількості злочинців у в'язницях, за гуманізацію і мінімізацію покарання, але захищав інтереси жертв. На думку Крісті, суперечки мають вирішуватися насамперед між злочинцями і жертвами, які є основними учасниками злочину. У рамках відновного правосуддя Крісті вважав, що кримінальний процес має сприяти активній участі жертв, злочинців і членів спільноти. Держава не повинна домінувати в судах і виключати інших учасників процесу [7].

Голландський кримінолог, юрист, поет та історик Герман Біанкі також критично ставився до наявної системи виконання покарань. У своїх дослідженнях він стверджував, що існують більш ефективні способи боротьби зі злочинцями, ніж тюремне ув'язнення, і що використання покарання як основного елемента системи кримінального правосуддя є помилковим. На його думку, доцільно примирити жертв і злочинців та компенсувати жертвам моральну та матеріальну шкоду.

Велике значення для розвитку наукового корпусу знань у царині відновного правосуддя має наукова праця американця Раймонда Міхаловскі, в якій він виокремлює два типи суспільств: вільні від держави та організовані в рамках держави. У своїй відомій роботі під назвою «Порядок, закон і злочин» («Order, Law and Crime») Міхаловскі пише, що примітивні суспільства, які існували 30 тис. років тому, були невеликими, ґрунтувалися на економічній співпраці, були схильні до рівноправності та справедливості між членами суспільства, як осілими, так і кочовими, і надавали перевагу мирним способам розв'язання конфліктів. Натомість, зазначає Міхаловскі, кримінальне правосуддя XX століття зосередилося на помсті у вигляді невідворотного покарання, а не на примиренні сторін конфлікту та відшкодуванню збитків потерпілому і компенсації жертвам [8].

Засновником концепції відновного правосуддя в нашому теперішньому розумінні є американський професор і соціолог Говард Зер, який спробував систематизувати відновний підхід до правосуддя. Зер проаналізував парадигму кримінального правосуддя про злочин і покарання та дослідив історичні, релігійні, соціальні та практичні альтернативи цій парадигмі. Зер проаналізував досвід практичного застосування відновного правосуддя, а саме програми примирення жертви та правопорушника, історію перших експериментів у Канаді та США, цілі програм примирення та ефективність їх впровадження.

Висновки. Результати теоретичних та практичних досліджень в сфері відновного правосуддя свідчать про те, що відновне правосуддя щодо

неповнолітніх передбачає активне залучення потерпілих, самих неповнолітніх правопорушників, а також громади до процесу правосуддя; відновний процес спрямований не на покарання, а на примирення, відновлення стосунків, відшкодування збитків потерпілому, встановлення та підтримання належного суспільного порядку в громадах та реінтеграцію неповнолітніх правопорушників у суспільство з метою запобігання скоєння ними правопорушень у майбутньому.

Список використаних джерел:

1. Свєтлічний І. В. Деякі актуальні питання кримінально-правової охорони прав неповнолітніх у кримінальному процесі, імплементації принципів відновного правосуддя щодо дітей та молодих людей / І. В. Свєтлічний // *Держава і право. Юридичні і політичні науки.* – 2020.- Вип. 88. – С. 212-224.
2. Свєтлічний І. В. Актуальні питання протидії злочинності неповнолітніх засобами відновного правосуддя / І. В. Свєтлічний, О. В. Свєтлічна // *Молодий вчений.* – 2021. – Вип. 11 (99). – С. 28-31.
3. Свєтлічний І. В. Відновне правосуддя як елемент кримінально-правової охорони прав дітей / І. В. Свєтлічний // *Часопис Київського університету права.* – 2021. – Вип. 4. – С. 383-386.
4. Свєтлічний І. В. Протидія злочинності неповнолітніх засобами відновного правосуддя: правовий і психологічний аспекти / І. В. Свєтлічний, О. В. Свєтлічна // *Держава і право. Юридичні і політичні науки.* – 2021. – Вип. 90. – С. 107-114.
5. Свєтлічний І. В. Кримінально-правова протидія злочинності неповнолітніх засобами відновного правосуддя / І. В. Свєтлічний, О. О. Малець // *Міжнародний науковий журнал «Правовий часопис Донбасу».* – 2022. – Вип. 4 (81) ч. 2. – С. 108-112.
6. Свєтлічний І. В. Роль відновного правосуддя у протидії злочинності неповнолітніх / І. В. Свєтлічний // *Юридичний науковий електронний журнал.* – 2022.- Вип. 1. – С. 254-257.
7. Дубовик О. І. Альтернативне правосуддя: розвиток наукової думки в 70–90 рр. XX століття / О. І. Дубовик // *Часопис Київського університету права.* – 2014. – Вип. 4. – С. 41–46.
8. Michalowski R. J. Order, law, and crime: an introduction to criminology. New York: Random House, 1985. 422 p.

Алієв Р. В.
кандидат юридичних наук, доцент,
начальник науково-дослідної
лабораторії проблем правового
забезпечення сектору безпеки і
оборони науково-дослідного відділу
проблем розвитку та впровадження
стратегічних комунікацій
інституту стратегічних комунікацій
Національного університету оборони
України

ЦИФРОВИЙ ЮРИДИЧНИЙ ДОКУМЕНТ: ПОНЯТТЯ, ОЗНАКИ, ПРАВОВИЙ СТАТУС

В епоху глобалізаційних процесів, цифрової трансформації та діджеталізації людство все частіше звертається за допомогою до вже існуючих видів цифрових документів, у тому числі юридичних. Так, ще двадцять років тому в українському суспільстві існувала проблема цифрової фіксації та оброблення будь-якої юридичної інформації (інформаційних правовідносин), що суттєво обмежувало права, свободи та обов'язки людини і громадянина в існуючих умовах розвитку інформаційних систем в Україні.

На сьогодні темпи цифрової трансформації досягли неабияких результатів, які ми маємо можливість використовувати у повсякденній життєдіяльності. Так, наприклад, на порталі «Дія» вже доступно понад 50 державних онлайн-послуг, а саме: «єРобота», «Пенсії, пільги та допомога», «Сім'я», «Ліцензії та дозволи», «Безпека та правопорядок», «Документи та громадянство», «Судові штрафи» тощо. Сплата штрафу за адміністративне правопорушення онлайн: нова послуга в «Дії», яка реалізовується Міністерством цифрової трансформації України разом з Державною судовою адміністрацією України, ДП «Центр судових сервісів» та ДП «Інформаційні судові системи». Крім того, Міністерство цифрової трансформації України створило простір для реалізації нових проєктів, таких як: «Дія.City» – унікальний простір, правовий режим для розвитку українських IT-компаній та «Е-резидентство» – це онлайн-сервіс, що надає можливість іноземцям онлайн вести бізнес в юрисдикції України та відкривати банківські рахунки [1].

Не залишаються поза увагою проблеми внутрішньо переміщених осіб (далі – ВПО) в умовах російсько-української війни. Так, для того, щоб зареєструвати статус ВПО та отримати довідку переселенця, пор-

тал “Дія” в цифровому форматі визначає алгоритм отримання статусу переселенця та оформлення і видачі довідки про взяття на облік внутрішньо переміщеної особи [2]. Це невичерпний перелік цифрових послуг, які надаються національними електронними інформаційними ресурсами під час реалізації правової політики у таких сферах: цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій та технологій, електронного урядування та електронної демократії. Водночас, виникає питання, чи має цифровий документ з того ж самого застосунку «Дія» юридичну силу, які його ознаки та правовий статус?

Дотепер в Україні сформовані певні правові та організаційні засади управління інформаційними ресурсами, які закріплені, насамперед у статті 34 Конституції України, в якій зазначено, що кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір [3, с. 17], та інших законодавчих актах України.

Свого часу Законом України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки” від 9 січня 2007 року № 537-V одним із завдань національної політики розвитку інформаційного суспільства в Україні було створення в електронній формі архівних, бібліотечних, музейних фондів та інших фондів закладів культури, формування відповідних інформаційно-бібліотечних та інформаційно-пошукових систем з історії, культури, народної творчості, сучасного мистецтва України тощо [4]. Нині вищезазначене завдання трансформоване у «Положення про Міністерство цифрової трансформації України» (далі – Мінцифри), затвердженого постановою Кабінету Міністрів України від 18 вересня 2019 р. № 856, відповідно до якого основними завданнями Мінцифри є формування та реалізація державної політики: у сфері впровадження електронного документообігу; у сфері розвитку цифрових навичок та цифрових прав громадян.

Теоретичні та практичні проблеми правового регулювання соціальної і цифрової трансформації, а також різні аспекти розвитку інформаційного суспільства досліджували вітчизняні науковці, такі як: С. Ю. Бєлявська (2016 р.), К. І. Бєляков (2013 р.), І. Ю. Крегул (2012 р.), Н. Б. Новицька (2016 р.), В. Г. Пилипчук (2013 р.), Г. М. Проскура (2021 р.), І. М. Сопілко (2014 р.), А. Ю. Старченко (2015 р.), Д. В. Сулацький (2011 р.), О. Ю. Харенко (2016 р.), О. Б. Червякова (2008 р.) та інші. Однак, проблемі визначення правового статусу цифрового юридичного документа його поняття та ознак не приділено належної уваги, тому назрів час закріплення його інформаційно-правового статусу.

Сьогодні розвиток інформаційного середовища характеризується комплексом нових досягнень прогресу, серед яких швидка зміна інформаційно-комунікаційних технологій; переведення інформації в цифровий формат; формування транснаціональних інформаційних потоків; переміщення капіталів у цю сферу як найбільш прибуткову; висока конкуренція серед провідних виробників, їх об'єднання і дезінтеграція [5. с. 764]. Саме завдячуючи електронній формі документа, впровадження електронного документообігу, став можливий наступний крок у розвитку інформаційного суспільства – розвиток цифрових навичок та цифрових прав громадян.

Складне питання цифрових прав громадян свого часу вивчали О. Б. Братасюк та Н. Ф. Ментух, які у своїх дослідженнях зазначають, що цифрові права людини – це окрема група прав людини, які пов'язані з використанням та/або реалізовуються в мережі Інтернет за допомогою спеціальних пристроїв (комп'ютерів, смартфонів тощо) [6]. До цих прав науковці відносять: 1) право на доступ до Інтернету – полягає в тому, що кожен має право на рівний доступ і використання вільного та безпечного Інтернету; 2) свобода вираження поглядів онлайн – означає право вільно висловлювати свої погляди, шукати, отримувати та поширювати інформацію онлайн; 3) право на приватність і захист персональних даних – кожен має право на приватність онлайн та захист персональних даних в Інтернеті (соціальних мережах, у заповненні Google-форм тощо); 4) право на свободу та особисту безпеку онлайн – реалізація цього права потребує механізму захисту від протиправних дій, тобто певні державні гарантії захисту від фізичного та психологічного насильства чи домагань, мови нетерпимості, нетолерантності та ворожнечі, дискримінації в онлайн-середовищі; держава має сприяти розвитку та функціонуванню безпечних Інтернет-технологій; 5) право на мирні зібрання, асоціації та/або використання електронних інструментів демократії – означає, що люди повинні мати свободу об'єднання та використовувати будь-які сервіси, вебсайти чи застосунки для створення, приєднання, мобілізації та участі в соціальних групах та асоціаціях; 6) право на цифрове самовизначення або право відключатися від онлайну, або бути забутим в онлайні – людина як користувач у системі (соціальній мережі, форумі, онлайн обговоренні) вправі сама, на власний розсуд визначити ім'я (ідентифікатор) або іншу апріорну інформацію про неї, яку вона буде використовувати в системі.

Таким чином, переведення публічно-правової та приватної інформації в цифровий формат, а саме в структуру цифрового юридичного документа, визначення його юридичної сили та правового статусу має стати

предметом наукових досліджень у контексті цифрових прав громадян. Це пояснюється тим, що чинне українське законодавство не містить тлумачення дефініції цифровий юридичний документ та не визначено його правовий статус. Натомість в Законі України «Про електронні документи та електронний документообіг» від 22 травня 2003 року № 851-IV зазначено, що електронний документ – це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.

Список використаних джерел:

1. Офіційний сайт Міністерства цифрової трансформації України. [Електронний ресурс]. URL: https://thedigital.gov.ua/projects (дата звернення 17.11.2023).

2. Про облік внутрішньо переміщених осіб. Постанова Кабінету Міністрів України № 509 від 01.10.2014 р. URL: https://zakon.rada.gov.ua/laws/show/509-2014-%D0%BF#n9 (дата звернення 17.11.2023).

3. Конституція України : чинне законодавство станом на 01 січня 2020 р.: Офіц. Текст. – К.: Норма права, 2020. – 100 с.

4. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: Закон України від 9 січня 2007 року № 537-V. URL: https://zakon.rada.gov.ua/laws/show/537-16#n14. (дата звернення 17.11.2023).

5. Правова доктрина України : у 5 т. – Х. : Право, 2013. Т. 2 : Публічно-правова доктрина України / Ю. П. Битяк, Ю. Г. Барабаш, М. П. Кучерявенко та ін. ; за заг. ред. Ю. П. Битяка. – 864 с.

6. О. Б. Братасюк. Н. Ф. Ментух. Поняття та класифікація цифрових прав в Україні. URL: file:///C:/Users/Asus/Downloads/download.pdf. (дата звернення 17.11.2023).

Заславська Л. В.
Старший науковий співробітник
Державної наукової установи
«Інститут інформації, безпеки і права
НАПрН України»

СУЧАСНІ ЗАГРОЗИ ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВУ

У постіндустріальну епоху, що наступила, індустрія інформаційних технологій органічно увійшла в усі сфери людської діяльності. Усі ці

тенденції насамперед свідчать про те, що суспільство переходить у нову стадію – стадію «інформаційного соціуму», що характеризується, різким зростанням ролі інформації, високим рівнем її ефективності, залежністю майбутнього від рівня розвитку інформаційного сектора економіки [1, с.1].

На даному етапі розвитку людства соціум вступив у нову фазу, де основним предметом праці є інформація і знання, знаряддям праці – інформаційні технології та засоби комунікації, а саме суспільство поступово стає інформаційним. Звернення суспільної свідомості до проблем інформаційної безпеки пов'язано з новими особливостями життя у сучасному суспільстві. Скорочуються соціальні практики аграрного та індустріального виробництва – вони технологізуються, стають інноваційними й інформаційно насиченими. Дедалі більша частина суспільства долучається до роботи з інформацією, інформація стає найважливішим ресурсом суспільства. Поряд з поняттями «промислова індустрія», «інфраструктура промисловості» дедалі частіше в діловій мові ми зустрічаємо поняття «інформаційна індустрія», «інформаційна інфраструктура» [2, с.75].

Нині у загальному розвитку культури як соціального феномена відбувається розвиток її інформаційної складової – інформаційної культури. Варто зазначити, що коли йдеться про інформаційну культуру, то цей соціальний феномен не обов'язково є породженням комп'ютерного XX століття. Формування інформаційної культури розпочалося з появою мови і писемності, що мало своїм наслідком швидке поширення знань. Інформаційна культура є складовою загальної культури, а інформаційна свідомість – відповідно, є суб'єктивним відображенням інформаційної культури особи.

У Стратегії розвитку інформаційного суспільства в Україні [3] зазначається, що розвинуті держави світу на межі XX-XXI століть поставили собі за мету прискорений перехід до нового етапу розвитку – інформаційного суспільства, що дасть змогу забезпечити рівень суспільного добробуту, здійснити перехід від економіки з паливно-сировинною спрямованістю (індустріальне суспільство) до економіки, заснованої на знаннях, досягти скорочення числа загроз національній безпеці, залучити громадян до всіх благ інформаційного суспільства. У вказаній вище Стратегії сформульовано визначення поняття електронна культура – форма культури, яка передбачає стимулювання та мотивування поширення здобутків у сфері культури за допомогою інформаційно-комунікаційних технологій. Втім, нині це поняття вже застаріле й використовується вже інший термін – «цифрова культура», притаманний сучасному етапу розвитку цифрових технологій.

Інформаційну культуру не варто порівнювати лише з володінням певними навичками, а саме: рівнем володіння комп'ютерною технікою чи інформаційними технологіями. Суспільство потребує усвідомлення особою всієї різноманітності зв'язків, які існують в сучасному суспільстві, розуміння своїх можливостей та обов'язків, уміння передбачати наслідки своїх дій (наслідків розповсюдження інформації, зокрема, неправдивої, т. зв. фейків); та співставлення їх з існуючими в соціумі цінностями такими як чесність, правдивість, або, наприклад, право на приватність та на свободу думки. Сьогодні формування інформаційного суспільства означає зростання інтелектуального потенціалу особи і суспільства загалом, зокрема, з огляду на швидкість передачі знань за допомогою всесвітньої мережі Інтернет. Водночас, використання сучасних технологій, мережі Інтернет, нової цифрової техніки супроводжується такими явищами, як залежність користувача, низький рівень культури безпеки, поширення небажаного контенту, несанкціонований доступ до інформації та особистих даних, кіберзлочинність, витоки інформації. Тож постає питання про відповідальності особи за свою діяльність в інформаційному просторі, та необхідність забезпечення інформаційної безпеки як протидія вказаним вище загрозам. Тобто сфера інформаційної культури має важливий правовий аспект, зокрема той, що охоплюється поняттям «інформаційна безпека».

Поняття «інформаційна безпека» міститься в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007, а саме: «Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, під час якого запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [4]. Проте, слід враховувати, що даний правовий акт розроблявся і був прийнятий до початку явних проявів гібридної війни, і по-друге, на наше переконання даному підходу притаманний однобічний підхід до забезпечення інформаційної безпеки. Слід визначити інформаційну безпеку України як стан, за якого в умовах дії реальних та потенційних загроз забезпечується самозбереження, сталий і прогресивний розвиток інформаційної сфери, зокрема захищеність інформаційної інфраструктури, інформаційного простору, інформаційних ресурсів, інформаційних процесів та їх суб'єктів, а також досягнення відповідних національних цілей та реалізація національних інтересів в інформаційній сфері [5, с.88].

Однак поняття інформаційної безпеки безперечно означає захист людини, суспільства та держави від протиправних посягань і пов'язане із

нормальним забезпеченням права особи на інформацію зокрема, та захисту всього комплексу прав і свобод людини, інтересів суспільства і держави.

Основою правового забезпечення інформаційної культури є статті 11, 32, 34 Конституції України [6], якими визначено інформаційні та культурні прав і свободи людини й громадянина. У ст. 34 зазначається, що кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань; кожному надається право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб. Отже, держава є гарантом безперешкодної реалізації та належного захисту прав громадян на інформацію, а відповідно, і є гарантом інформаційної культури.

Науковці, які вивчають інформаційну культуру вважають, що сучасна цивілізація характеризується тим, що жодна сфера буття людини не може нормально функціонувати й розвиватися без своєчасного та повного забезпечення необхідною інформацією, уміння її швидко, якісно і адекватно сприймати, обробляти, зберігати, використовувати та передавати. Розповсюдження інформації, знань, правових знань, культурних надбань, видів творчості, завжди має певні наслідки для прогресивного розвитку суспільства. Задля того, щоб вміти розрізняти правду від брехні, необхідно розуміти як формуються інформаційні потоки, хто їх формує і з якою метою. Осмислення вказаного дасть змогу не стати жертвою різних фейків чи дезінформації агресора, спрямованих проти держави чи окремих осіб.

Список використаних джерел:

1. Теплицький І. О., Семеріков С. О Інформаційна безпека як нова складова інформаційної культури. – Режим доступу https://core.ac.uk/download/pdf/77240925.pdf

2. Дзьобань О. П., Мануйлов Є. М., Інформаційна безпека в контексті інформаційної культури . *Інформація і право* № 1(20)/2017, с.74-81

3. Про схвалення Стратегії розвитку інформаційного суспільства в Україні Розпорядження Кабінету Міністрів України від 15 травня 2013 р. № 386-р. – Режим доступу https://www.kmu.gov.ua/npas/246420577

4. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.2007 № 537-V

5. Довгань О. Д., Ткачук Т. Ю., Концептуальні засади законодавчого забезпечення інформаційної безпеки України. *Інформація і право*. № 1(28)/2019. С.86-99

6. Конституція України – Режим доступу https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

Васько В. А.
аспірант Державної наукової установи «Інститут інформації, безпеки і права НАПрН України»

ВИКЛИКИ ЗАСТОСУВАННЯ МЕХАНІЗМІВ ДЕЦЕНТРАЛІЗОВАНОГО СУДОЧИНСТВА ЯК АЛЬТЕРНАТИВНОГО СПОСОБУ ВИРІШЕННЯ СПОРІВ

Зі збільшенням транскордонних взаємозв'язків, які стали можливими за рахунок швидкого обміну інформацією традиційні централізовані системи, в тому числі й ті, що забезпечують здійснення правосуддя, стикаються з безпрецедентними викликами. Зростаюча поширеність нових видів спорів у онлайн-спільнотах часто за участю анонімних або псевдонімних користувачів, які походять з різних правових юрисдикцій, стимулює інтерес до розробки інноваційних методів вирішення конфліктів.

Однією з відповідей на такі виклики стала індустрія онлайн вирішення суперечок (далі – ОВС), що використовує ІТ технології для сприяння механізмам альтернативного вирішення спорів (далі – АВС). Іншими словами, ОВС по суті означає проведення процесів АВС в режимі онлайн [1]. На сьогодні ОВС охоплює широкий спектр способів врегулювання конфліктів включаючи механізми переговорів, медіації, посередництва, арбітражу та інші. Гібридні процеси, які поєднують як онлайн, так і офлайн елементи, також входять до сфери застосування ОВС [1].

Нині численні платформи електронної комерції пропонують власні системи ОВС. Проте наявні рішення у цій сфері не відповідають очікуваному трансформаційному потенціалу, пропонуючи лише незначні вдосконалення існуючих методів врегулювання конфліктів. Саме тому сучасні технології, такі як блокчейн та похідні від неї технології були покликані створити нові механізми АВС у віртуальному середовищі.

Застосування технології блокчейн у сфері ОВС породило нову парадигму, що в наукових колах більш відома під назвою «децентралізоване судочинство» (далі – ДС). Один із перших кроків у формалізації визначення децентралізованого судочинства було зроблено авторитетними вченими у галузі правого регулювання застосування технології блокчейн Федеріко Астою та Бруно Деффайнсом. Науковці стверджують, що для того, щоб система вирішення спорів вважалася системою децентралізованого судочинства, остання повинна відповідати трьом умовам: 1) бути побудованою як децентралізована автономна організація DAO на архітектурі технології блокчейн, 2) ґрунтуватися на механізмі, що використовує криптоекономічні стимули, і 3) створювати відчуття справедливості [2].

Застосування технології блокчейн сприятиме підвищенню рівня довіри до індустрії ОВС. Специфічний спосіб прийняття рішень через систему голосування вузлами мережі блокчейн-спільноти забезпечує цілісність процесу вирішення спорів і запобігає будь-яким маніпуляціям щодо роботи з доказами, відбором незалежних суддів тощо. Система ОВС будучи створена на основі блокчейну гарантує, що процес вирішення спорів відбуватиметься виключно за заздалегідь погодженими її учасниками правилами, які відповідатимуть принципу «код – це закон» [3].

Децентралізовані системи судочинства мають певну схожість з традиційними механізмами АВС, зокрема арбітражем. Обидва мають на меті забезпечити альтернативні шляхи вирішення спорів поза межами традиційних судових систем. Однак, між децентралізованим арбітражем і традиційним арбітражем існують суттєві відмінності. Традиційний арбітраж, як правило, має більш централізовану та формалізовану структуру зі встановленими міжнародними та національними інституціями правилами. З іншого боку, децентралізованому арбітражу бракує такого уніфікованого підходу до регулювання [4].

Відсутність централізованого органу в децентралізованому арбітражі може бути як сильною стороною, так і викликом. З позитивного боку, це може підвищити ефективність, прозорість та нейтральність процесу. Смарт-контракти можуть автоматизувати певні аспекти арбітражу, а децентралізований характер може зменшити ризик упередженості. Однак відсутність єдиної нормативної бази викликає занепокоєння щодо застосовного права під час вирішення конфліктів системами ДС, що в свою чергу має значний вплив на послідовність вирішення спорів та захист прав і свобод учасників індустрії ОВС.

Конвенція про визнання та виконання іноземних арбітражних рішень, (далі –Конвенція), є фундаментальним інструментом у сфері міжнародного арбітражу. Проте між науковцями точаться дискусії щодо того чи можуть її положення застосовуватись до децентралізованого судочинства, оскільки в ній прямо передбачено, що «Конвенція застосовується щодо визнання та приведення у виконання арбітражних рішень, винесених на території держави іншої, ніж та держава, де запитується визнання та приведення у виконання таких рішень» [5,6]. Натомість у децентралізованих системах, у випадку анонімності учасників, арбітражний процес може взагалі не мати чіткого територіального зв'язку, а в іншому випадку може залучати сторони та арбітрів з різних правових юрисдикцій. Таким чином, невизначеність щодо юрисдикції формально суперечить застосуванню норм Конвенції до концепції децентралізованого судочинства.

Ще одна проблема застосування Конвенції до децентралізованого судочинства полягає в тому, що суди можуть відмовити у виконанні рішень, прийнятих за допомогою систем ДС на підставі ст. 5 Конвенції [5] або у випадку суперечності арбітражного рішення публічному порядку. Наприклад, суд може вважати, що одна зі сторін не мала можливості себе захистити, або що процедура арбітражу не відповідала вимогам законодавства країни, де відбувся арбітраж тощо.

Але з іншого боку, рішення, прийняті в системах децентралізованого судочинства, щодо конфліктів, які випливають з групи спорів пов'язаних із застосуванням блокчейну не будуть потребувати схвалення національними судами через самозабезпечувальний характер розумних контрактів, що лежать в основі ДС [3]. Тому проблематика правового регулювання та затвердження децентралізованих арбітражних рішень є більш актуальною для групи спорів не пов'язаних із застосуванням технології блокчейн та похідних від неї технологій.

Натомість, багато, хто з науковців взагалі заперечують можливість механізмів ДС вирішувати традиційні конфлікти. Наприклад, М. Бухвальд стверджує, що система ДС є потенційно не придатною до вирішення складних економічних та правових спорів поза ланцюгом блоків за рахунок неможливості збору доказів у реальному часі [7].

Крім того, залишається проблема невідповідності ДС основним принципам АВС, що викликає значне занепокоєння щодо дотримання належної правової процедури, включаючи забезпечення основних прав та свобод учасників системи. Відтак для подолання цих викликів на нормативному рівні необхідно врегулювати механізми ДС. Але хоч з одного боку, регулювання і може забезпечити певну правову визначеність, котра буде запобігати можливим зловживанням від використання децентралізованого судочинства. З іншого боку, ДС ґрунтується на ідеї автономності та відсутності централізованого контролю, тому будь-яке регулювання з боку централізованих інституцій порушить його основні принципи.

Таким чином, нова парадигма децентралізованого судочинства породжує проблеми взаємодії між класичним правом та правом саморегулюючих систем блокчейну. У зв'язку з цим, як альтернативу правового регулювання ДС для вирішення спорів поза межами блокчейну ми пропонуємо розробити квазі-правові рекомендації, котрі не носитимуть імперативного характеру.

Також на сучасному етапі розвитку галузі децентралізованого судочинства оптимальним є використання гібридних процесів ОВС, так як це, наприклад, зробив один із цивільних судів Мексики в своєму рішенні від 28 травня 2021 року, визнавши та виконавши арбітражне рішення,

що ґрунтується на блокчейн-протоколі [6]. Проте в цьому випадку суд не виконав безпосередньо рішення винесене платформою ДС, а виконав, рішення арбітражного суду, яке в свою чергу імплементувало рішення платформи децентралізованого судочинства Kleros у свій висновок по справі.

У даному випадку предмет спору існував поза межами блокчейну. Тому з метою виконання рішення винесеного платформою ДС, його необхідно було легалізувати. Після прийняття рішення в онлайн-режимі, арбітр в офлайн-режимі виніс рішення, яке включало в себе рішення прийняте платформою децентралізованого судочинства Kleros. Однак важливо відзначити, що в даній справі сторони погодились на використання механізмів ДС та боржник відмовився оскаржувати дане рішення в національному суді, хоч і мав на це право. Відтак неможливо передбачити, чи підтримав би суд подібне рішення за інших обставин. Таким чином, рано робити висновки, що механізми децентралізованого судочинства можна вважати альтернативним способом вирішення традиційних спорів.

Отже, на сьогодні використання механізмів децентралізованого судочинства для вирішення нескладних спорів похідних від застосування блокчейну та відповідно виконання таких рішень не викликає критичних зауважень за рахунок ключових особливостей самої технології. Натомість щоб такий механізм став прийнятним як альтернативний спосіб вирішення спорів поза блокчейн-середовищем він повинен відповідати концепції належної правової процедури, що в свою чергу суперечитиме головній ідеї децентралізації таких систем. За відсутності правового регулювання ДС може слугувати виключно доповненням до існуючих механізмів ОВС та АВС.

Список використаних джерел:

1. UNCITRAL Technical Notes on Online Dispute Resolution. New York, 2017. URL: https://bit.ly/3R9MieX.

2. Ast F., Deffains B. When Online Dispute Resolution Meets Blockchain: The Birth of Decentralized Justice. *Stanford Journal of Blockchain Law and Policy*. 2021. URL: https://bit.ly/3ujwywG.

3. Bergolla L., Seif K., Eken C. Kleros: A Socio-Legal Case Study Of Decentralized Justice & Blockchain Arbitration. *SSRN Electronic Journal*. 2021. URL: https://bit.ly/47CqVsx

4. Chevalier M. From Smart Contract Litigation to Blockchain Arbitration, a New Decentralized Approach Leading Towards the Blockchain Arbitral Order. *Journal of International Dispute Settlement*. 2021. Vol. 12, no. 4. P. 558–584. URL: https://bit.ly/49IZBtX

5. Конвенція про визнання та виконання іноземних арбітражних рішень : Конвенція Орг. Об'єдн. Націй від 10.06.1958 р. URL: https://bit.ly/3QOqsMD

6. Virues M. Accommodating Kleros as a Decentralized Dispute Resolution Tool for Civil Justice Systems: Theoretical Model and Case of Application. URL: https://bit.ly/46no2dt

7. Buchwald M. Smart Contract Dispute Resolution: The Inescapable Flaws of Blockchain-Based Arbitration, 168 U. Pa. L. Rev. 1369 (2020). URL: https://bit.ly/3G9XKRb

Конончук Б. Р.
здобувач вищої освіти Хмельницького університету управління та права імені Леоніда Юзькова

ПЕРСПЕКТИВИ ЗАПРОВАДЖЕННЯ ЕЛЕКТРОННОГО ГОЛОСУВАННЯ НА МІСЦЕВИХ РЕФЕРЕНДУМАХ

Цифрова трансформація в Україні не можлива без інтеграції електронного управління, яке охоплює автоматизацію надання адміністративних послуг, що в основному базуються на використанні інформаційно-комунікаційних технологій. Ця інтеграція також включає в себе впровадження систем електронного судочинства та розширення компонентів електронної демократії, включаючи можливість електронного голосування на місцевих референдумах.

Нормативно-правовою основою впровадження електронного голосування в Україні є розпорядження Кабінету Міністрів України від 8 листопада 2017 року № 797-р, яким затверджено Концепцію розвитку електронної демократії в Україні та план заходів щодо її реалізації [1, с.116].

Зараз, хоча Закон України «Про всеукраїнський референдум», прийнятий 26 січня 2021 року, передбачає можливість впровадження електронного голосування, сам законопроект щодо цієї ініціативи так і не було розроблено. Він набуде чинності тільки після ухвалення закону, що регулює застосування інноваційних технологій для електронного голосування. Згідно статті 116 зазначеного закону, електронному голосуванню можуть піддаватися виборці, які мають право голосу на спеціальних дільницях для електронного голосування [2].

Процес електронного голосування виконується за допомогою автоматизованої інформаційно-телекомунікаційної системи. Дата та час

проведення електронного голосування повинні співпадати зі строками звичайного голосування на паперових дільницях для всеукраїнського референдуму. Після закінчення строку для електронного голосування, дільнична комісія для електронного голосування на основі даних інформаційно-телекомунікаційної системи визначає загальну кількість виборців, включених до списку для електронного голосування, загальну кількість учасників електронного голосування, кількість голосів, поданих на користь та проти питання всенародного референдуму. Проте зміст цього закону не надає належних відповідей щодо конкретної технології впровадження електронного голосування в Україні [3, с.78].

На сьогодні в Україні створено початкову нормативно-правову базу, що може бути використана для подальшого правового забезпечення порядку електронного голосування:

1. Закон України № 2155-VIII від 05.10.2017 р. «Про електронні довірчі послуги» дає можливість запровадити в Україні сучасні електронні методи ідентифікації особи, серед яких Mobile ID.

2. Закон України № 2163-VIII від 05.10.2017 р. «Про основні засади забезпечення кібербезпеки України» визначає основні цілі, напрями та принципи державної політики у сфері кібербезпеки, також повноваження та обов'язки державних органів в цій сфері.

3. Прийнятий 19.12.2019 р. Виборчий кодекс України передбачає активне використання інформаційно-комунікативних технологій у частині реєстрації виборців та уточнення відомостей про виборців у Державному реєстрі виборців.

4. Відповідно до Закону України № 698-V від 23.07.2020 р. «Про Державний реєстр виборців» Реєстр ведеться в електронній формі; заява щодо включення до Реєстру особи, яка має право голосу, може бути надіслана нею до органу ведення Реєстру в електронній формі за електронним цифровим підписом.

Система голосування в Україні, яка існує, має низку таких суттєвих недоліків, як: тривалі терміни підготовчого етапу голосування та його проведення, незахищеність від фіктивних і повторних голосувань, проблема здійснення права на голосування пенсіонерів, інвалідів та людей з обмеженими можливостями. Натомість електронне голосування може вирішити ці питання. На підставі положень наднаціонального права Європейського Співтовариства е-голосування має численні переваги як перспективна форма е-демократії: дає змогу виборцям віддати свої голоси на виборчій дільниці не лише свого виборчого округу, полегшує виборцю віддати свій голос, сприяє участі у виборах і референдумах усіх тих, хто має права голосу, а особливо громадян, які перебувають за

кордоном, розширює доступ до процесу голосування для осіб з особливими потребами або тих, кому важко бути фізично присутнім на дільниці, поступово знижує витрати на проведення виборів та референдумів, доставляє результати голосування надійно та швидко, надає вищий рівень послуг із пропозицією різних можливостей для голосування, збільшує час виборця для роздумів і вираження волевиявлення через збільшення кількості днів голосування, збільшує довіру до результатів голосування шляхом формування екзит-полів у режимі часу з їхньою візуалізацією на екранах телебачення та плазмових моніторах у людних місцях [4, с.148-153].

Отже, цифрова трансформація в Україні вимагає інтеграції електронного управління та електронного голосування, яке може покращити демократичні процеси, забезпечити більшу доступність голосування та збільшити довіру до виборчих процесів. Однак важливо розробити конкретний законопроект та забезпечити кібербезпеку впровадження цих технологій.

Список використаних джерел:

1. «Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації». Розпорядження Кабінету міністрів України. від 26.09.2020. №797-р. Ст.116. URL:https://zakon.rada.gov.ua/laws/show/797-2017-%D1%80#Text (дата звернення 23.10.2023)

2. «Про Всеукраїнський референдум». Закон України від 31.03.2023. № 1135-IX. URL: https://zakon.rada.gov.ua/laws/show/1135-20#Text

3. Гаврік Р. О. Перспективи запровадження електронного голосування в Україні в контексті реалізації концепції розвитку електронної демократії та врахування досвіду естонської республіки. П 68 Правові засади організації та здійснення публічної влади, 78. 2022.

4. Щебетун І. С., Довгань Ю. В. «Електронна демократія: досвід зарубіжних країн і перспективи її впровадження в Україні.» Право і суспільство 2 2020. С. 148-153.

Паскар А. А.
здобувачка вищої освіти Одеського національного університету імені І. І. Мечникова
Науковий керівник: д.ю.н., проф. Степанова Т. В.

РОЗВИТОК ІНСТИТУТУ ЗАБЕЗПЕЧЕННЯ: МІЖНАРОДНИЙ ДОСВІД

Інститут забезпечення в процесуальному праві України являє собою допоміжний механізм у процесі вирішення справи, що безпосередньо впливає на реалізацію прав і виконання обов'язків учасників процесу. Для вдосконалення функціонування інституту забезпечення в Україні та проведення позитивних реформ, необхідно досліджувати його розвиток на прикладі інших правових систем, в яких безпосередньо також розвивається даний інститут.

Забезпечення доказів в Німеччині здійснюється виключно за згодою на це іншої сторони, оскільки докази можуть бути втрачені або їх використання буде утрудненим [1]. Тому відповідно до Цивільного процесуального уложення докази забезпечуються шляхом перевірки свідчень, допиту свідка, призначення експертизи. Недоліком є те, що Цивільним процесуальним уложенням не врегульована сутність забезпечення доказів.

А законодавство Франції передбачає можливість ініціювати забезпечення за зверненням сторони, перелік підстав для забезпечення не передбачається, забезпечення доказів здійснюється судом і оскарженню не підлягає [2].

Однак інститут заходів забезпечення позову у Франції на початку 1991 року був суттєво реформований на підставі Закону «Про виконання судових рішень» та Декрету про внесення змін до цивільного процесуального законодавства. Для застосування забезпечення позову повинна існувати крайня необхідність (в загальному розумінні такого стану). Так, ситуація буде розцінюватися як стан крайньої необхідності, якщо збиток, заподіяний однією зі сторін без застосування таких забезпечувальних заходів, стане непоправним. Суд не повинен вирішувати будь-які аспекти по суті спору з метою обґрунтування застосування заходів забезпечення позову. Крім того, суд повинен встановити, що збиток дійсно є невідворотним і необхідно запобігти його виникненню [6].

Цікавим для дослідження є приклад Японії, де питання про забезпечення доказів вирішується виключно судом у випадках, коли існують обста-

вини, за яких було б важко скористатись доказами, за умови, що вони не досліджувались раніше. Клопотання про забезпечення доказів може бути подано як до подачі позовної заяви (в такому випадку суд призначає особу, котра буде виступати від імені опонента), так і після [3]. Водночас суд може з власної ініціативи забезпечити докази. Розгляд заяви про забезпечення доказів здійснюється за участю сторін, а ухвала суду оскарженню не підлягає.

В Казахстані та Республіці Молдова забезпечення доказів до подання позовної заяви здійснюється нотаріусами, після подання – судом [4].

Механізм заходів забезпечення позову створив нову процедурну основу для ефективних дій вітчизняного правовласника щодо захисту своїх прав не тільки в Україні, але й в інших розвинених країнах.

В Англії ст. 25 Закону «Про юрисдикцію у цивільних справах та судових рішеннях» в рамках судового провадження наділяє Високий суд Англії та Уельсу повноваженнями приймати заходи забезпечення позову в будь-якій формі, за винятком видачі наказів про арешт майна або компетенції про примусове витребування доказів. Згідно з правовою позицією лорда Диплока, для накладення судом заходів забезпечення позову позивач, зокрема, повинен довести, що: його доводи не є безпідставними; баланс інтересів сторін переважує на користь видачі тимчасового судового припису; простої компенсації збитків не буде достатньо для відновлення порушеного права; а заявник, зі свого боку, повинен надати суду зустрічне забезпечення [5].

Вивчення зарубіжного досвіду щодо врегулювання судових витрат в адміністративному судочинстві показує, що існують різні підходи до оплати адміністративного судочинства: від установлення безкоштовного правосуддя в адміністративних справах у Франції до ретельного нормативно-правового закріплення порядку стягнення витрат на судочинство у Німеччині (норми трьох законів регулюють такі витрати) [7, с. 43].

Особливістю для більшості європейських країн (Бельгія, Німеччина, Австрія, Польща тощо) є вжиття терміна «процесуальні витрати» щодо витрат, пов'язаних зі здійсненням того чи іншого юрисдикційного процесу, які включають судові витрати (збір чи мито і судову заставу (аванс) на покриття майбутніх витрат у судочинстві) і позасудові витрати [7, с. 44]. Вважаємо, що вказане поняття потрібно запозичити у вітчизняне національне законодавство.

Стосовно визначення та розподілу судових витрат актуальним є аналіз досвіду Польщі у сфері адміністративного судочинства. У Законі «Про провадження в адміністративних судах» Республіки Польщі зазначено, що процесуальні витрати (зокрема, судові витрати) – це необхідні витрати у процесі, який сторона вела особисто або через уповноважену особу,

яка не є адвокатом чи юрисконсультом, що охоплюють судові витрати, вартість проїзду сторони або уповноваженої особи в суд та еквівалент втраченого ними заробітку, які не можуть перевищувати оплати праці одного адвоката чи юрисконсульта, оплату праці адвоката або юрисконсульта, але не вище за ставки оплати, визначеної в окремих положеннях, витрати одного адвоката або юрисконсульта, судові витрати і витрати особистої явки сторони за викликом суду (стаття 205 § 2) [8, с. 326].

У континентальній Європі діє загальне правило: «витрати покладаються на того, на чию користь не прийнято рішення», у США – «кожна сторона несе власні витрати».

Серед особливостей судових витрат окремих країн можна виділити такі: у Великобританії стороні, на користь якої винесено рішення, відшкодовуються реально понесені витрати, зокрема, витрати органу публічної адміністрації. У Франції створено на рівні держави спеціальну організацію, яка надає допомогу у покритті витрат на правосуддя малозабезпеченим особам. А в Естонії існує найвищий у Європі відсоток судового збору (12,3%) [7, с. 44]. У більшості досліджуваних країн стягнені процесуальні витрати покривають витрати на здійснюване адміністративне судочинство.

Цікавим є досвід правового регулювання виплат експертам і спеціалістам у рамках провадження в адміністративних спорах, передбачений ст. 39 Закону Литовської Республіки «Про провадження у адміністративних справах», де зазначено, що для зберігання і стягнення сум, що підлягають виплаті свідкам, фахівцям, експертам та експертним організаціям, для кожного суду відкривається спеціальний рахунок у банку за місцем знаходження суду [9].

Отже, розгляд міжнародного досвіду розвитку інституту забезпечення є досить важливим для запозичення певних елементів процедури забезпечення, які притаманні іншим країнам, що можуть вплинути на вдосконалення даного інституту в процесуальному праві України. Доцільним буде запозичення зарубіжного досвіду щодо віднесення до судових витрат таких витрат, що пов'язані зі зберіганням речових доказів, а не лише з їх оглядом і забезпеченням. Зважений зарубіжний досвід, поєднаний з власними правовими, історичними та національними традиціями, дасть змогу досягти ефективного результату в правовому регулюванні.

Список використаних джерел:

1. Zivil prozessordnung. URL: https://dejure.org/gesetze/ZPO.

2. Code de procédure civile. URL: https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070716.

3. Code of Civil Procedure. Японія. URL: http://www.wipo.int/wipolex/ru/ text.jsp?file_id=337360#Part2Chap4Sec7.

4. Гражданский процессуальный кодекс Республики Казахстан: от 31.10.2015 №337-V URL: https://online.zakon.kz/Document/ ?doc_id=34329053#pos=1;-117.

5. Правова позиція лорда Диплока по справі «American Cyanamid v Ethicon Limited» (1975) AC 396 at 407−408. URL: https:// www.casemine.com/judgement/uk/6g34tgha.

6. Code of Civil Procedure of France. URL: https://www.jus.uio.no/ lm/france.arbitration.code.of.civil.procedure.1981/doc.html.

7. Пащенко К. С. Оновлений законодавчий підхід до інституту судових витрат в адміністративному судочинстві України. *Наукові записки Інституту законодавства Верховної Ради України.* 2018. № 2. С. 41–46. URL: http://nbuv.gov.ua/UJRN/Nzizvru_2018_2_8.

8. Тильчик В. В. Теоретико-методологічні та правові засади вирішення адміністративними судами спорів у сфері публічно-правових відносин : дис. … докт. юрид. наук. Запоріжжя, 2020. 448 с.

9. Про провадження у адміністративних справах: Закон Литовської Республіки від 14.01.1999 № VIII-1029. URL: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/1ac36e42c13d11e682539852a4b72dd4?jfwid=2r1mjq5h.

Ніколаєв К. Д.
кандидат сільськогосподарських наук, доцент

ПІДХОДИ ДО МОДЕЛЮВАННЯ ЕКОЛОГІЧНИХ РИЗИКІВ В КОНТЕКСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

У сучасних умовах завдання моделювання екологічних ризиків для забезпечення національної безпеки України є актуальним і вкрай суттєвим. Зростаюча індустріалізація, зміни клімату та природні катастрофи ставлять перед країною значні виклики, які можуть впливати на екологічну стабільність та загальну національну безпеку.

Доречно зазначити, що національна безпека включає в себе не лише військовий аспект, але й економічний, соціальний та екологічний. Відсутність належного управління природними ресурсами та неврахування екологічних аспектів може призвести до серйозних наслідків для національної безпеки.

Слід додати, що моделювання екологічних ризиків дозволяє передбачати можливі негативні наслідки екологічних факторів на різних рів-

нях: від забруднення повітря та води до змін клімату. Врахування цих аспектів у моделях національної безпеки дозволяє розробляти ефективні стратегії запобігання та реагування на можливі екологічні загрози.

На думку вченого О. Мотайла, що варто більш докладно розглянути різноманітні методи моделювання екологічних ризиків. Отже, давайте ближче розглянемо ці методи та стратегії.

1. Математичні моделі для прогнозування впливу забруднення:

- математичні моделі можуть використовуватися для визначення взаємозв'язку між різними факторами забруднення та їх впливом на природні ресурси. Наприклад, моделі можуть враховувати концентрації забруднюючих речовин у повітрі, воді чи ґрунті та їх вплив на рослинність, водні ресурси та здоров'я людей;
- використання диференціальних рівнянь та статистичних методів дозволяє прогнозувати зміни в екосистемі відповідно до різних сценаріїв забруднення.

2. Сучасні технології симуляцій для моделювання екологічних криз:

- використання комп'ютерних симуляцій дозволяє створити віртуальні моделі екосистем, в яких можна аналізувати можливі екологічні кризи;
- ці технології дозволяють враховувати багато факторів одночасно та аналізувати їх взаємодію, що допомагає прогнозувати наслідки екологічних змін;
- важливо також враховувати велику кількість даних, щоб симуляції були максимально точними. Сучасні технології обробки даних та штучного інтелекту можуть сприяти у покращенні точності таких моделей.

Отже, ці методи дозволяють не лише прогнозувати можливі ризики, але і визначати ефективні заходи запобігання та реагування на екологічні кризи, що допомагає зберегти екологічну стабільність та забезпечити національну безпеку.

Доречно врахувати особливості, що визначають Україну, такі як значна залежність від вугільної енергетики та труднощі в управлінні водними ресурсами. Перше, велика залежність від вугільної енергетики є ключовим економічним фактором, але водночас створює значні екологічні виклики. Викиди забруднюючих речовин та парникових газів під час вугільного виробництва можуть призводити до серйозних проблем для повітря та здоров'я населення. Розвиток стратегій поступового відмовлення від вугільної енергії та переходу до більш екологічно чистих джерел є важливим кроком у забезпеченні сталого розвитку.

Друге, проблеми з управлінням водними ресурсами набувають особливого значення в умовах зміни клімату. Періодичні посухи та зміни в режимі опадів можуть призводити до дефіциту води та загострення конфліктів за водні ресурси. Розробка ефективних систем водопостачання та стратегій управління водними ресурсами стає критичною для забезпечення водної безпеки та уникнення екологічних криз.

Поглиблене вивчення цих аспектів в контексті національної безпеки України дає можливість визначити конкретні пріоритети та розробляти цілеспрямовані стратегії, спрямовані на покращення екологічної стійкості країни.

Необхідно відмітити думку вчених О. Резнікова, К. Войтовського та А. Лепіхова, що в умовах зростаючого усвідомлення екологічних проблем, національні уряди та громадяни шукають способи зменшення екологічних ризиків та покращення стану природи. Почнемо з аналізу кількох ключових напрямків при розгляді стратегій та політик, спрямованих на забезпечення екологічної безпеки. Ці напрямки включають в себе розвиток відновлювальних джерел енергії, впровадження ефективних систем управління відходами та стимулювання використання екологічно чистих технологій у виробництві.

Давайте розглянемо стратегії та політики, щоб визначити їх можливості та вплив на забезпечення екологічної стійкості.

Таблиця 1.

Стратегії та заходи для зменшення екологічних ризиків

Напрямок	Конкретні заходи
Розвиток відновлювальних джерел енергії (далі – ВДЕ)	− сприяння створенню проєктів сонячної, вітрової та гідроенергетики; − впровадження систем фінансової підтримки та фінансової підтримки та податкових пільг для інвестицій у сектор ВДЕ
Ефективне управління відходами	− впровадження систем сортування відходів на побутовому та промисловому рівнях; − розробка та вдосконалення інфраструктури для подальшої переробки та утилізації відходів; − проведення освітніх кампаній для підвищення свідомості щодо відповідального використання ресурсів та уникання відходів
Заохочення екологічно чистих технологій	− надання державних пільг та фінансових стимулів для підприємств, що використовують екологічно чисті технології; − фінансування досліджень та інновацій для створення нових, більш екологічно безпечних технологій

Складено та узагальнено автором

Проаналізувавши вищезазначене можна дійти висновку, що екологічні ризики стають невід'ємною частиною національної безпеки України. Моделювання цих ризиків виявляється ключовим інструментом для передбачення та управління можливими наслідками, особливо в умовах зростаючих викликів, таких як зміни клімату та екологічні кризи. Стратегії, що охоплюють розвиток відновлювальних джерел енергії, ефективне управління відходами та заохочення чистих технологій, визначають перспективний шлях для сталого розвитку. Реалізація цих стратегій потребує не лише технологічних інновацій, але й активної державної підтримки, щоб гарантувати безпеку країни та сприяти створенню майбутнього, що відзначається екологічною безпекою.

Наукове видання

СОЦІАЛЬНА І ЦИФРОВА ТРАНСФОРМАЦІЯ: ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ

МАТЕРІАЛИ
III ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

Київ, 23 листопада 2023 року

Матеріали подано в авторській редакції

Підписано до друку 28.11.2023.
Формат 60x84/16. Ум-друк. арк. 8,6
Наклад 100 прим. Зам. № 2312-09.

Видавець ПП «Фенікс»
(Свідоцтво суб'єкта видавничої справи ДК № 1044 від 17.09.02).
Україна, м. Одеса, 65009, вул. Зоопаркова, 25.
e-mail: fenix-izd@ukr.net