



Комітет Верховної Ради України з питань цифрової трансформації
Національна академія правових наук України
Науково-дослідний інститут інформатики і права НАПрН України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Факультет соціології і права
Навчально-науковий центр інформаційного права
та правових питань інформаційних технологій
Інтернет Асоціація України

СОЦІАЛЬНА І ЦИФРОВА ТРАНСФОРМАЦІЯ: ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ

МАТЕРІАЛИ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

10 ГРУДНЯ 2020 РОКУ

Київ – 2020

УДК 34:004(477)

С 69

Рекомендовано до друку:

*Вченою радою Науково-дослідного інституту інформатики і права
Національної академії правових наук України.*

Протокол № 12 від 29.12.2020 р.

С 69 Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання : матеріали науково-практичної конференції, 10 грудня 2020 р., м. Київ / упоряд.: О.А. Баранов, В.М. Фурашев, С.О. Дорогих. – Київ : Фенікс, 2020. – 272 с.

ISBN 978-966-928-617-8

Збірник містить матеріали конференції, де розглянуто актуальні питання, що стосуються правового забезпечення соціальної трансформації на основі використання цифрових технологій та проблем правового регулювання суспільних відносин в соціальних комунікаціях і у сфері застосування технологій Інтернету речей, у сферах публічного управління, нацбезпеки та оборони держави, економіки, охорони здоров'я, освіти, науки, культури, фінансової та банківської діяльності тощо, а також проблем забезпечення інформаційних прав людини, діяльності нових медіа, засобів масової інформації та соціальних мереж в умовах цифрової трансформації із використанням штучного інтелекту, робототехніки, правотворення, технологій блокчейн у різних сферах соціальної діяльності: управління державою, Індустрії 4.0, транспорту, роздрібною торгівлі, охорони здоров'я, інфраструктури міст тощо.

Доповіді учасників конференції можуть бути корисними для спеціалістів у сферах правотворення, правозастосування та правоохоронної діяльності, фахівців різних галузей права, науково-педагогічних працівників та здобувачів вищої освіти.

Матеріали подано у авторській редакції.

УДК 34:004(477)

ISBN 978-966-928-617-8

- © Комітет Верховної Ради України з питань цифрової трансформації, 2020
- © Науково-дослідний інститут інформатики і права НАПрН України, 2020
- © Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», 2020
- © Інтернет Асоціація України, 2020
- © Колектив авторів, 2020

ЗМІСТ

ПРОГРАМНІ ПИТАННЯ КОНФЕРЕНЦІЇ

ПЛЕНАРНІ ВИСТУПИ

Баранов О.А.

ЕКОНОМІКА РЕЗУЛЬТАТУ, ІНТЕРНЕТ РЕЧЕЙ ТА ПРАВО .. 10

Дубняк М.В.

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ
КРИПТОВАЛЮТИ В УКРАЇНІ. 20

Азьмук Н.А.

МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ РИНКУ ПРАЦІ В
КОНТЕКСТІ СТАНОВЛЕННЯ ЦИФРОВОЇ ЕКОНОМІКИ ... 28

Забара І.М.

ДО ПИТАННЯ ПРОБЛЕМАТИКИ МІЖНАРОДНО-
ПРАВОВОГО РЕГУЛЮВАННЯ ЦИФРОВОЇ ЕКОНОМІКИ .. 33

Некіт К.Г.

ЩОДО ПОНЯТТЯ ТА СУТНОСТІ СМАРТ-КОНТРАКТІВ ... 37

Доронін І.М.

ЗАГРОЗИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ В УМОВАХ
ЦИФРОВИХ ТРАНСФОРМАЦІЙ ТА МЕЖІ ДЕРЖАВНОГО
РЕГУЛЮВАННЯ 40

Богущий П.П.

ЦИФРОВА ТРАНСФОРМАЦІЯ СОЦІАЛЬНИХ КОМУНІКАЦІЙ
ТА НАЦІОНАЛЬНА БЕЗПЕКА УКРАЇНИ 45

ВИСТУПИ УЧАСНИКІВ КОНФЕРЕНЦІЇ

Марущак А.І.

СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ ОСВІТНІХ
ПРОЄКТІВ ІЗ ПІДВИЩЕННЯ КІБЕРГІГІЄНИ НАСЕЛЕННЯ
УКРАЇНИ. 49

Головко О.М.	
ЦИФРОВА ОСВІТА ТА ЄС: ІНТЕРНЕТ РЕЧЕЙ В ДІЇ	52
Бежєвець А.М.	
ТРАНСФОРМАЦІЯ ПРАВА НА ІНФОРМАЦІЮ В УМОВАХ КАРАНТИНУ	55
Шастун А.Д., Амоша О.О., Паньков Д.В.	
СТРАТЕГІЧНІ ПРІОРИТЕТИ УКРАЇНИ В СВІТЛІ ЦИФРОВІЗАЦІЇ ЕКОНОМІКИ ТА ПОДОЛАННЯ ЗАГРОЗ КОРОНАКРИЗИ	59
Водько Ю.В.	
ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ СОЦІАЛЬНОЇ ТРАНСФОРМАЦІЇ НА ОСНОВІ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ. 64	
Діденко Г.Ю.	
«УНІВЕРСИТЕТ ТРЕТЬОГО ВІКУ» ЯК МЕХАНІЗМ СОЦІАЛІЗАЦІЇ ЛЮДЕЙ СТАРШОГО ВІКУ В УМОВАХ СОЦІАЛЬНОЇ ТА ЦИФРОВОЇ ТРАНСФОРМАЦІЇ	68
Зінчук Д.О.	
ПРАВОВІ ПЕРСПЕКТИВИ МЕДІАЦІЇ З ВИКОРИСТАННЯМ ЦИФРОВИХ ТЕХНОЛОГІЙ	71
Радзієвська О.Г.	
ПРОБЛЕМИ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНИХ ПРАВ ЛЮДИНИ В УМОВАХ СОЦІАЛЬНИХ ТА ЦИФРОВИХ ТРАНСФОРМАЦІЙ	73
Гуменюк І.О.	
ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ВИКОРИСТАННЯ ІТ У СФЕРІ СОЦІАЛЬНОГО ЗАХИСТУ: ОКРЕМІ АСПЕКТИ	77
Дранник В.А.	
ЩОДО ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СОЦІАЛЬНОЇ СФЕРИ	82
Капіца Ю.М.	
ПИТАННЯ ІМПЛЕМЕНТАЦІЇ ДИРЕКТИВИ 2019/790 ПРО АВТОРСЬКЕ ПРАВО В ЄДИНОМУ ЦИФРОВОМУ РИНКУ В ЄВРОПЕЙСЬКОМУ СОЮЗІ.	84
Муханов В.М., Голюк М.В.	
ПОРУШЕННЯ АВТОРСЬКИХ ПРАВ У МЕРЕЖІ ІНТЕРНЕТ . .	88

Войтко А.А.	РИЗИКИ ПОРУШЕННЯ ПРАВА НА НЕ ВТРУЧАННЯ В ОСОБИСТЕ ЖИТТЯ ПРИ ВИКОРИСТАННІ ДАНИХ СОЦІАЛЬНИХ МЕРЕЖ.	91
Ніжнік В.В	МЕДІАЦІЯ В СУДОЧИНСТВІ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА.	96
Воронько М.А.	КОНФІДЕНЦІЙНІСТЬ В ОНЛАЙН МЕДІАЦІЇ.	100
Гуменюк А.О.	ЕФЕКТИВНІСТЬ ДИСТАНЦІЙНОЇ РОБОТИ МЕДІАТОРА В УМОВАХ ПАНДЕМІЇ.	104
Данілевич Д.Р.	ДИСТАНЦІЙНА РОБОТА МЕДІАТОРА.	106
Сорока М.М.	ЗДІЙСНЕННЯ ДИСТАНЦІЙНОЇ МЕДІАЦІЇ: МОЖЛИВОСТІ ЧИ ВИКЛИКИ?.	111
Томик В.В.	МЕДІАЦІЯ В ЦИВІЛЬНИХ СПРАВАХ: ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ В УМОВАХ ПАНДЕМІЇ.	114
Брайчевський С.М.	ПРОБЛЕМА ПРИРОДНОЇ МОВИ В СИСТЕМАХ ІЗ ШТУЧНИМ ІНТЕЛЕКТОМ.	119
Гиляка Олег Сергійович	МІЖНАРОДНИЙ ДОСВІД ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СУДОЧИНСТВІ.	124
Шваб І.О.	ЗАРУБІЖНИЙ ДОСВІД ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПУБЛІЧНОМУ АДМІНІСТРУВАННІ.	128
Ситник О. В.	ОСОБЛИВОСТІ ПЕРЕДАННЯ ПРАВА НА ДОМЕННЕ ІМ'Я ПОТОЧНИМ РЕЄСТРАНТОМ ДОМЕННОГО ІМЕНІ МАЙБУТНЬОМУ РЕЄСТРАНТУ.	133
Шуміло О.М.	ЕКОЛОГІЧНИЙ КРАУДФАНДИНГ ЯК ЗАСІБ СОЦІАЛЬНОЇ ТРАНСФОРМАЦІЇ: ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ.	136

Шахбазян К.С

ПРАКТИКА ОХОРОНИ АВТОРСЬКОГО ПРАВА НА НАУКОВІ
ЖУРНАЛИ ТА МОНОГРАФІЇ ВИДАВНИЦТВАМИ В ЄС ПРИ
КОМЕРЦІЙНОМУ ВИКОРИСТАННІ ТА НАДАННІ ВІЛЬНОГО
ДОСТУПУ ДО ВИДАНЬ ЧЕРЕЗ ІНТЕРНЕТ 141

Бойко О.І., Костенко І.В.

РЕКЛАМА ЯК ОБ’ЄКТ АВТОРСЬКОГО ПРАВА:
ЮРИДИЧНИЙ АНАЛІЗ ЧЕРЕЗ ПРИЗМУ ВІТЧИЗНЯНОГО
ЗАКОНОДАВСТВА 146

Холдоєнко А.В.

РЕКЛАМА ЯК ВАЖІЛЬ ВПЛИВУ НА СУСПІЛЬСТВО 150

Бережницький Р.В.

ПРОБЛЕМАТИКА ПРАВОВОЇ ОХОРОНИ КОМП’ЮТЕРНОЇ
ПРОГРАМИ В УКРАЇНІ 155

Васько В.А.

ПРОБЛЕМА ВИЗНАЧЕННЯ ЗМІСТУ ЮРИДИЧНОЇ
ВІДПОВІДАЛЬНОСТІ РОЗРОБНИКІВ ВІДКРИТОГО
ВИХІДНОГО ПРОГРАМНОГО КОДУ БЛОКЧЕЙН-ПРОЄКТІВ .
160

Касперович О.Ю.

ПІДВИЩЕННЯ СТІЙКОСТІ СФЕРИ ПРАЦІ ТА ЗАЙНЯТОСТІ
В УМОВАХ ПАНДЕМІЇ COVID-19 ЧЕРЕЗ ЗАЛУЧЕННЯ
ЦИФРОВИХ ТЕХНОЛОГІЙ: НАПРЯМИ УДОСКОНАЛЕННЯ
РЕГУЛЯТОРНОЇ ПОЛІТИКИ 166

Рашевська К.Є.

ІНТЕГРАЦІЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ
ТЕХНОЛОГІЙ У ТРАДИЦІЙНІ МЕХАНІЗМИ ВИРІШЕННЯ
МІЖНАРОДНИХ ТОРГОВЕЛЬНИХ СПОРІВ 171

Солончук І.В.

АНТИКОРУПЦІЙНІ ПИТАННЯ РЕФОРМУВАННЯ
СУДОЧИНСТВА В УМОВАХ СОЦІАЛЬНОЇ ТА ЦИФРОВОЇ
ТРАНСФОРМАЦІЙ 177

Ткачук Т.Ю.

АКТУАЛЬНІ ДОМІНАНТИ СУЧАСНОГО ІНФОРМАЦІЙНОГО
СУСПІЛЬСТВА. 182

Фокиа Л.В.

АНАЛІЗ ПРАВОВИХ ПІДСТАВ ВПРОВАДЖЕННЯ ЦИФРОВОЇ
ПОШТОВОЇ МАРКИ В УКРАЇНІ. 185

Новікова О.Ф., Сидорчук О.Г.

ФОРМУВАННЯ ДЕРЖАВНОЇ АНТИКРИЗОВОЇ ПОЛІТИКИ
В УМОВАХ НОВІТНІХ ВИКЛИКІВ ТА НЕБЕЗПЕК ЧЕРЕЗ
ЗАЛУЧЕННЯ РЕСУРСІВ ЦИФРОВІЗАЦІЇ. 188

Панькова О.В., Красуліна Я.Є.

УКРАЇНА В КООРДИНАТАХ ЧЕТВЕРТОЇ ПРОМИСЛОВОЇ
РЕВОЛЮЦІЇ (ПЛАТФОРМА «ПРАЦЯ 4.0») ТА ПАНДЕМІЙНОЇ
СОЦІОЕКОНОМІЧНОЇ РЕАЛЬНОСТІ. 194

Бедрата А.В.

ПРОБЛЕМИ ПРОВЕДЕННЯ ПРОЦЕДУРИ МЕДІАЦІЇ ЗА
УМОВИ ВИКОРИСТАННЯ СИСТЕМИ ЕЛЕКТРОННИХ
КОМУНІКАЦІЙ. 199

Бруслик А.В.

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ В УМОВАХ
ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ. 203

Іванів І.Р.

ЦИФРОВА ТРАНСФОРМАЦІЯ У СФЕРІ ОХОРОНИ
ЗДОРОВ'Я. 207

Пономарьов К.С.

ПРОЦЕДУРА МЕДІАЦІЇ В УКРАЇНІ В УМОВАХ
КАРАНТИННИХ ОБМЕЖЕНЬ. 210

Радченко К.В.

ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ ОБІГУ
ВІРТУАЛЬНИХ АКТИВІВ. 215

Фарадж Д.Ю.

ЮРИДИЧНА ВІДПОВІДАЛЬНІСТЬ РОБОТОТЕХНІКИ ЗІ
ШТУЧНИМ ІНТЕЛЕКТОМ. 218

Загорулько В.М.

PROBLEMS OF LEGAL REGULATION OF THE USE OF
ARTIFICIAL INTELLIGENCE IN IT. 220

Горлинський В.В., Горлинський Б.В.

ЦИФРОВА ТРАНСФОРМАЦІЯ УКРАЇНСЬКОГО
СУСПІЛЬСТВА: ІНСТИТУЦІЙНО-ПРАВОВІ ОСНОВИ
ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ. 225

Пономаренко І.С.

АКТУАЛЬНІ ПИТАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ
У СФЕРІ ОХОРОНИ ЗДОРОВ'Я 231

Ямчук Г.М.

ПРОБЛЕМИ ПРАВОВОГО ЗАХИСТУ ПЕРСОНАЛЬНИХ
ДАНИХ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ 237

Тарасюк А.В.

ПИТАННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ НА СУЧАСНОМУ
ЕТАПІ РОЗВИТКУ ГЛОБАЛЬНИХ ІНФОРМАЦІЙНИХ
ПРОЦЕСІВ 242

Ткачук Н.І.

ІНСТИТУЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ
НАЦІОНАЛЬНОЇ СИСТЕМИ ОЦІНЮВАННЯ РИЗИКІВ І
ЗАГРОЗ В УКРАЇНІ 246

Кухрівський Д.В.

ПИТАННЯ ВДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА З ПИТАНЬ
ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ, ІНФРАСТРУКТУРНОЇ
БЕЗПЕКИ, КІБЕРБЕЗПЕКИ 249

Моргун Г.В.

СУТНІСТЬ ПАТЕНТНОГО ТРОЛІНГУ ЯК ПРАВОВОГО
ЯВИЩА ТА ЙОГО ВПЛИВ НА СФЕРУ ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ 252

Фурашев В.М.

ОСОБЛИВОСТІ ОСВІТНЬОГО ПРОЦЕСУ ПІДГОТОВКИ
ПРАВНИКІВ ДЛЯ РОБОТИ В УМОВАХ СОЦІАЛЬНОЇ ТА
ЦИФРОВОЇ ТРАНСФОРМАЦІЇ 257

Клименко К.О.

ПРАВОВІ АСПЕКТИ ЗАСТОСУВАННЯ АДВОКАТСЬКОЇ
ТАЄМНИЦІ ЯК СКЛАДОВОЇ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ
АДВОКАТА 260

Сай В.І.

РЕГУЛЮВАННЯ ОНЛАЙН-МЕДІА В КОНТЕКСТІ
ЗАКОНОПРОЕКТУ ПРО МЕДІА. 263

Баранов О.А., Головка О.М., Дубняк М.В.

ЦІЛІ, ЗАВДАННЯ ТА ПЕРСПЕКТИВИ ПРОЕКТУ
«ЄВРОІНТЕГРАЦІЯ: ЗАКОНОДАВСТВО ТА ІНТЕРНЕТ
РЕЧЕЙ» (EULIOT) 266

ПРОГРАМНІ ПИТАННЯ КОНФЕРЕНЦІЇ

Під час роботи конференції пропонуються для розгляду наступні питання:

1. Правове забезпечення соціальної трансформації на основі використання цифрових технологій у сферах публічного управління, нацбезпеки та оборони держави, економіки, промисловості, сільського господарстві, охорони здоров'я, освіти, науки, культури, фінансової та банківської діяльності тощо.

2. Проблеми правового регулювання суспільних відносин в соціальних комунікаціях, зокрема: забезпечення інформаційних прав людини, діяльності нових медіа, засобів масової інформації та соціальних мереж, бібліотечної, архівної та музейної діяльності в умовах цифрової трансформації.

3. Особливості правового забезпечення розвитку сучасної інформаційної інфраструктури суспільства, зокрема: системи електронних комунікацій, надання мультимедійних послуг, електронних національних ресурсів, електронних реєстрів, дата -центрів, впровадження хмарних технологій та використання великих даних, виробництва програмного забезпечення та комп'ютерних технологій.

4. Проблеми правового регулювання суспільних відносин в сфері застосування технологій Інтернету речей, зокрема, із використанням штучного інтелекту, робототехніки, криптовалют, технологій блокчейн у різних сферах соціальної діяльності: управління державою, Індустрії 4.0, транспорту, роздрібною торгівлі, охорони здоров'я, інфраструктури міст тощо.

5. Питання вдосконалення законодавства з питань захисту персональних даних, інфраструктурної безпеки, кібербезпеки тощо.

6. Особливості освітнього процесу підготовки правників для роботи в умовах соціальної та цифрової трансформації.

7. Проведення презентації проекту «Євроінтеграція: законодавство та Інтернет речей» (EULIoT), який буде виконуватись в рамках програми Єрасмус+, модуль Жан Моне.

ПЛЕНАРНІ ВИСТУПИ

Баранов О.А.

доктор юридичних наук, старший науковий співробітник, керівник НДЦ цифрових трансформацій і права НШП НАПрНУ

ЕКОНОМІКА РЕЗУЛЬТАТУ, ІНТЕРНЕТ РЕЧЕЙ ТА ПРАВО

Колись давно, в ужиток увійшла ідіома: «здати під ключ», що означало закінчувати будівництво будинків, квартир або виробництво інших товарів, повністю підготував їх для використання споживачами без необхідності проведення додаткових робіт. Однак, в умовах масового ринку, виробник товарів або надавач послуг був вимушений орієнтуватись на потреби середньостатистичного споживача. Тому незважаючи на очікувану привабливість стратегії «все під ключ», все ж вона не могла принципово вирішити проблему того, що довгі, довгі роки споживачі були змушені задовольнятися тим, що їм пропонували, а не отримувати те, що їм було цікавим і бажаним. У загальному це призводило до великих економічних втрат, які фактично несли споживачі, змушені частково «руйнувати» результати попередньої роботи виробників і за свій рахунок самостійно вдосконалювати властивості отриманих товарів або послуг, адаптуючи їх до своїх реальних потреб.

Згадані та інші «системні» рішення задоволення потреб конкретних споживачів створювали ілюзію ефективності економічних процесів, але при цьому не враховувалися зайві трудовитрати, витрати матеріальних ресурсів і часу, які несли величезна кількість «щасливих» споживачів, що були змушені займатися не властивою для себе діяльністю. Більш того, економіка потерпала від вкрай негативного явища не реалізації великих обсягів вже виробленої продукції або пропонованих послуг, які не задовольнили вимог конкретного споживача.

Поряд з іншими факторами цей системний недолік системи масового виробництва товарів та послуг призводив до виникнення періодичних кризових явищ в економіці. Це зумовило появу безлічі конкуруючих економічних теорій виходу людства з кризового становища, практично в кожній з яких пропонуються певні моделі соціальної трансформації.

З урахуванням широковідомих цивілізаційних викликів, що склалися на початок 21 століття, особливостей формування сучасного профілю споживача можна стверджувати, що науковці та практики з усією очевидністю приходять до усвідомлення доцільності і необхідності зміни парадигми економічної діяльності. Один з варіантів нової парадигми має свою назву – це **економіка результату** [1].

Після виникнення на початку третього тисячоліття активного інтересу до Інтернет у речей (Internet of Things, IoT) як одного з найбільш значущих досягнень останньої промислової революції, сформувався економічно обґрунтований, системний рух передових країн щодо створення та втілення в життя стратегій впровадження технологій IoT. Завдяки першим вражаючим результатам втілення в життя цих стратегій, стали з'являтися публікації, присвячені усвідомленню можливих локальних і глобальних наслідків застосування технологій IoT.

Особливий інтерес викликають публікації, в яких розкривається нова стратегія розвитку економічної сфери – стратегія розвитку **економіки результату** (outcome economy) [2,3]. Цікавим є той факт, що спочатку в більшості з подібних публікацій їх авторами були топ менеджери транснаціональних технологічних компаній з проблематики IoT, які зобов'язані прогнозувати напрями розвитку бізнесу з горизонтом планування 10-20-30 років. Лягати

Джо Баркай, поглиблюючи ідею створення «економіки результату», підкреслює: рішення IoT, які добре підходять для реалізації стратегії економіки результату, можуть бути побудовані на відкритих масштабованих системах, які дозволяють використовувати міць різноманітних взаємопов'язаних партнерських екосистем, що потенційно створює гнучке середовище, яке дозволяє виявити

можливості обслуговування клієнтів, реагування на ринкові зміни і конкурентні загрози [4] .

Аналогічну логіку розуміння економіки результату демонструє Ю. Джоші, який розповідав про гірничодобувну компанію, що платить виробнику обладнання за здобутий нею обсяг вугілля замість того, щоб купувати дороге капітальне обладнання [3]. Або – про компанію, яка виробляє автомобільні шини і замість того, щоб продавати самі шини, отримує компенсацію за паливну економію, яку забезпечують її шини, тобто за результат. І те, і інше вже стало реальністю в світі IoT. Одночасно, Джоші зазначає в якості феномена наступну проблему: для виконання «незрозумілої», на перший погляд, вимоги споживача необхідно буде залучати до співпраці певну, іноді значну, кількість партнерів.

Такий шлях розвитку економіки стає можливим тільки для компаній, які будують свою стратегію на: розвитку широкого спектра потенційних коопераційних зв'язків; участі у спеціально сформованих екосистемах взаємодії; використанні розширеної аналітики та формуванні нових потоків даних, щоб отримати своєчасну інформацію про потреби і патерни поведінки споживачів [5].

Сформулюємо попереднє визначення **«економіки результату»** – це економіка в який будь-яка діяльність, що пов'язана із задоволенням потреб людини, має своїм результатом те, що замовлені споживачем роботи, товари, або послуги доставляються або надаються у вказані ним час та місце.

Для економіки результату справедливим буде твердження про те, що оперативна (в режимі реального часу) організація економічної кооперації (кооперації виробництва) економічних акторів будь-якої юрисдикції та географічної локації може бути реалізована лише завдяки наявності потенційної можливості організації функціонального зв'язку будь-якого комплексу IoT з будь-яким іншим комплексом IoT. А ось можливість такої потенційної функціональної зв'язності впливає з сутності феномену технології Інтернету речей, аналізу принципів побудови, особливостей функціонування комплексів IoT, що обумовлено використанням

інтернет-технологій, технологій штучного інтелекту, хмарних обчислень, обробки великих даних (big data), робототехніки та т. п.

Таким чином, саме можливість гнучко і оперативно створювати ситуативну тимчасову кооперацію суб'єктів економічної діяльності на основі функціонального взаємозв'язку технологій Інтернету речей, інваріантної від наявності історії таких зв'язків, виду і типу робіт, товарів або послуг, використовуваних технологій, від державної юрисдикції, місця розташування економічних акторів і споживачів є базовою основою реалізації нового тренду економічного розвитку – формування та реалізації *економіки результату*.

В такому випадку для економіки результату найважливішою конкурентною перевагою буде залученість в життя клієнта (споживача). Саме залученість потенційно дозволить одержувати не інформацію, а знання! спектру проблем споживача, знання навіть про такі проблеми, про які він може ще й не здогадуватись.

У сучасному світі активно використовують таргетинг як механізм реклами, що дозволяє виділити зі всієї наявної аудиторії певну частину, яка задовольняє заданим критеріям (цільову аудиторію), і показати конкретну рекламу саме їй [6].

Механізм рекламного таргетингу полягає в тому, що збираються однаковий певний набір даних про велику кількість людей, сукупність яких і складає так звані «великі дані». Після обробки великих даних за допомогою різних видів і методів таргетування здійснюють диференціацію аудиторії, тим самим створюючи умови для формування цільових груп, члени яких мають однаковий набір ознак з близькими якісними і / або кількісними показниками споживацьких потреб. В подальшому здійснюється таргетована реклама певних товарів або послуг найбільш релевантних потребам і інтересам конкретної цільової групи людей.

Тому, в умовах економіки результату таргетинг стає гранично важливим, наріжним системним фактором. Дійсно, для будь-якого економічного актора є критично необхідним мати функціональну можливість превентивно визначати зміст конкретних життєвих проблем, споживацьких потреб окремого *конкретного* споживача з тим, щоб формувати саме йому ре-

зультативні пропозиції щодо їх вирішення. Для реалізації цієї функції необхідно використовувати певні методи, способи і механізми вивчення потреб, переваг, особливостей можливої поведінки кожного конкретного споживача в різних життєвих ситуаціях. Подібну функцію економічного актора можна реалізувати на основі функціонального таргетингу.

Дамо визначенні: ***функціональний таргетинг*** – це методи, способи і механізми збору і обробки неструктурованої інформації про людину (споживача) з різних джерел, що дозволяють з високою достовірністю визначити якісні та кількісні характеристики його потреб, вподобань, патернів його поведінки для подальшого формування індивідуальних пропозицій товарів та послуг в потрібному місці і в потрібний час з метою максимально повного вирішення його проблемних ситуацій.

Функціональність таргетингу полягає в тому, що він забезпечує виробничу функцію конкретного економічного актора з продажу товарів або надання послуг конкретному споживачеві, які були б релевантними його потребам і інтересам.

Тому функціональний таргетинг не може бути зведений до простого збору та аналізу великих даних про об'єкт досліджень. Це перш за все наукова інтерпретація та апроксимація отриманих результатів обробки великих даних про споживача з використанням положень соціології, соціальної психології та психології особистості, з урахуванням ментальних, культурних і релігійних особливостей окремих груп людей тощо.

В умовах економіки результату буде значно трансформуватися зміст конкуренції. Виходячи із сутності економіки результату, компанії перейдуть від конкуренції обсягів продажу товарів і послуг до конкуренції за досягнення вимірювальних результатів, важливих для споживача. Тому економічні актори стратегічно будуть націлені не на конкуренцію з обсягів виробництва, що неминуче призводить до циклічного перевиробництва, а на конкуренцію за можливість доставити споживачу товар або послугу в конкретне місце і в конкретний час для задоволення його ексклюзивних індивідуальних споживчих вимог. Такий вид конкуренції будемо на-

живати *конкуренцією результату*, зміст і наслідки реалізації якої будуть принципово відрізнятися від традиційної конкуренції.

На практиці, конкуренція результату буде створювати системні передумови для формування глобального режиму економії всіляких природних і вироблених ресурсів завдяки тому, що обсяги їх використання безпосередньо залежатимуть від результатів функціонального таргетування. Це означає, що ресурси будуть використовуватися строго в межах і обсягах, необхідних для задоволення конкретних, а не передбачуваних, потреб (вирішення проблем) конкретного споживача, а не ймовірного, середньостатистичного, актуальних для нього в цей час і в цьому місці. Світова економіка може назавжди позбутися синдрому недоцільного накопичення ресурсів про запас і про всяк випадок.

Тому, реалізація стратегії економіки результату дозволяє поєднати, здавалося б, несумісне. Масовий ринок економіки результату призначений для задоволення індивідуальних, ексклюзивних потреб. Або, іншими словами, економіка результату – це фактично перехід від знеособленого масового ринку для пересічного масового споживача до масового ринку з «людським обличчям», орієнтованого на інтереси конкретного споживача.

Такий перехід стає можливим тільки в рамках економіки результату, основою якої є функціонально таргетована економічна діяльність у умовах масового ринку з усіма його перевагами масштабування бізнес-процесів. При цьому *функціонально таргетована економічна діяльність* – це діяльність економічних акторів з доставки результатів роботи, товарів або послуг в потрібне місце і в потрібний час з характеристиками і параметрами релевантними індивідуальним запитам та інтересам конкретного споживача.

Отже, *економіка результату* — це функціонально таргетована економічна діяльність суб'єктів масового ринку по задоволенню індивідуальних потреб будь-якого конкретного споживача за рахунок можливості створення ситуативної оперативної кооперації на основі функціональної взаємодії з будь-якими іншими суб'єктами ринку.

На основі цього визначення сформулюємо **базовий принцип економіки результату** – для кожного споживача будь-які результати робіт, товари або послуги, релевантні його індивідуальним потребам та інтересам, мають бути доставлені йому в потрібний час і місце на планеті.

Таким чином, **економіка результату** – це людиноцентристська економіка з величезним ресурсозберігаючим та інноваційним потенціалом, зі зміненою природою екосистем коопераційного взаємодії і конкуренції, що базується на глобальній соціо-технологічній інфраструктурі (інфраструктурі IoT).

Перехід до економіки результату означає перехід до абсолютно нового змісту і рівню цінностей у взаєминах як між економічними акторами, так і між ними і споживачами, а це означає необхідність проведення масштабної соціальної трансформації внаслідок того, що:

- а) першою необхідною умовою такого переходу є перетворення, зміна або корекція мети функціонування органів публічної влади, бізнес-структур у всіх сегментах економічної діяльності;
- б) другою необхідною умовою такого переходу є перетворення, зміна або корекція світогляду, системи цінностей та способу життя споживачів, а також опанування ними відповідними сучасними знаннями та навичками;
- в) такий перехід неминуче спричинить за собою зміну інституційної структури і функцій системи публічного управління і регулювання в економічній сфері, системи інститутів громадянського суспільства;
- г) еволюційно стануть виникати і розвиватися сегментно орієнтовані об'єднання економічних акторів для оптимізації процесів кооперації, координації та створення умов для гнучкого й оперативного формування функціональних взаємозв'язків в процесі економічної діяльності;
- д) потрібно проведення істотної модернізації системи правового забезпечення нових методів, способів і механізмів реалізації функцій публічного управління і регулювання в економічній сфері,

- е) має бути проведена масштабна робота з формування правового забезпечення швидкого і з мінімальними транзакційними витратами формування і функціонування предметно орієнтованих екосистем коопераційної взаємодії економічних акторів різної галузевої приналежності, виконання робіт і надання послуг в інтересах конкретних користувачів в умовах різної державної юрисдикції;
- ж) приведеється проводити масштабний реінжиніринг колишніх і створювати нові бізнес-моделі і бізнес-процеси в економічній діяльності.

Зрозуміло, що реалізація базового принципу економіки результату в умовах масового ринку неможлива без найширшого використання комп'ютерних і телекомунікаційних технологій (цифрових технологій) і, перш за все, мова йде про технології IoT.

Отже, ми маємо право зробити висновок про те, що перехід до економіки результату означає проведення в сфері економічної діяльності масштабної соціальної трансформації на базі цифрової трансформації. Тому, що без цифровізації, як фундаментальної умови, не уявляється можливим: гнучко і оперативно забезпечувати створення ситуативного функціонального взаємозв'язку суб'єктів економічної діяльності; формувати предметно орієнтовані екосистеми коопераційної взаємодії; використовувати розширену ринкову аналітику; забезпечувати функціональне таргетування як на глобальному рівні, так й в місцевих масштабах.

Цифровізація в контексті економіки результату – це проведення тотальної трансформації бізнес-процесів, масове впровадження нових інноваційних бізнес моделей, орієнтованих на використання досягнень четвертої промислової революції, в першу чергу, передових технологій IoT та інших комп'ютерних технологій.

Таким чином, реалізація ідеології економіки результату вимагає трансформаційного переходу від традиційних, фіксованих, відносно стабільних бізнес-моделей до оперативно трансформованим гібридним бізнес-моделям на основі цифровізації всіх складових бізнес-процесів.

В подальших дослідженнях будемо використовувати наступні терміни:

- **соціальна трансформація** – це перетворення, зміна або корекція мети функціонування, структури і функцій суспільства, в тому числі, методів, способів і механізмів реалізації цих функцій, для нейтралізації або сприяння впливу зовнішніх і внутрішніх дій на його подальший розвиток;
- **цифрова трансформація** – це соціальна трансформація, яка відбувається на основі максимального використання цифрових технологій таких як: Інтернет речей, Індустрія 4.0, штучний інтелект, робототехніка, обробка великих даних, хмарні обчислення, електронні комунікації, а також, нано- та біотехнологій, генної інженерії та багатьох інших.

Аналізуючи зазначені дефініції та реальний зміст соціальної і цифрової трансформації, можна зробити висновок про їх діалектичний зв'язок як зв'язок відповідних філософських категорій «зміст» і «форма».

Для нашого випадку: зміст – це соціальна трансформація, яка полягає в зміні або перетворенні соціуму, іноді, корінному. Використання цифрових технологій означає особливу форму реалізації будь-якої соціальної трансформації – цифрову трансформацію. При цьому може мати місце відомі наслідки діалектичного зв'язку категорій «змісту» і «форми». Конкретний зміст соціальної трансформації може детермінувати вибір форм (методів, способів, засобів і механізмів) цифрової трансформації. У свою чергу реалізація конкретних форм цифрової трансформації може привести до необхідності зміни змісту соціальної трансформації.

У загальному випадку, і соціальна трансформація, і цифрова трансформація неминуче призводять до зміни в тій чи іншій мірі:

- змісту і складу системи суспільних відносин, які охоплюються ними, а іноді, навіть до появи нових за змістом груп суспільних відносин;
- парадигми функціонування держави, соціуму і його окремих сегментів, життєдіяльності окремих людей;

- бізнес-процесів в будь-яких сферах функціонування суспільства: політика, економіка, державне управління, військова справа, освіта, культура, охорона здоров'я, розваги, особисте життя тощо, перш за все на інноваційній основі.

Тому будь-які трансформації безперечно призводять до необхідності корекції або зміни відповідної соціальної моделі суспільства і будь-яких інших видів моделей соціуму (державного управління, економічної, інформаційної, соціальної тощо). А це неминуче тягне за собою зміну правової моделі, яка має відповідати конкретній соціальній моделі суспільства або певного сегменту життєдіяльності соціуму.

Таким чином, сучасні і майбутні соціальні та цифрові трансформації при реалізації стратегії економіки результату призводять до істотної зміни системи і структури суспільних відносин як в цілому в суспільстві, так і в окремих його сегментах. Такі зміни є причиною необхідності проведення відповідних теоретико-правових досліджень і подальшого удосконалення системи законодавства.

Література

1. *Industrial Internet of Things: Unleashing the Potential of Connected Products and Services* (World Economic Forum 2015) 39. <http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf> дата звернення 09.12.2020.

2. C Meley, “The Outcome Economy, Powered by IoT” (Teradata, June 20, 2017) <<https://www.teradata.co.uk/Blogs/The-Outcome-Economy,-Powered-by-IoT>> дата звернення 09.12.2020.

3. Y Joshi, ‘The Paradox in the Industrial IoT Outcome Economy: Collaborating with Partners, Mistrusting Customers’ (EVEREST GROUP, August 20, 2018) <https://www.everestgrp.com/2018-08-paradox-industrial-iot-outcome-economy-collaborating-partners-mistrusting-customers-sherpas-blue-shirts-46333.html> дата звернення 09.12.2020.

4. B Joseph, ‘The Outcome Economy: How the Industrial Internet of Things is Transforming Every Business’ (ABEBOOKS, 2016) <<https://www.abebooks.com/9781530381463/Outcome-Economy-Industrial-Internet-Things-1530381460/plp>> дата звернення 09.12.2020.

5. *Industrial Internet of Things: Unleashing the Potential of Connected Products and Services* (World Economic Forum, 2015)

39. <http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf> дата звернення 09.12.2020.

6. 'Таргетинг' <<https://ru.wikipedia.org/wiki/%D0%A2%D0%B0%D1%80%D0%B3%D0%B5%D1%82%D0%B8%D0%BD%D0%B3>> дата звернення 09.12.2020.

Дубняк М.В.

кандидат юридичних наук, старший
викладач КПП ім. Ігоря Сікорського

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ КРИПТОВАЛЮТИ В УКРАЇНІ

Спроби правового регулювання криптовалюти в Україні беруть початок у 2017 році з поданням до Верховної Ради України проекту Закону про обіг криптовалюти в Україні (№ 7183 від 06.10.2017). Наперед відзначимо, даний законопроект був першою, але не останньою спробою, за ним було подано на розгляд ще ряд законопроектів, зокрема:

1. Проект Закону про обіг криптовалюти в Україні (7183 від 06.10.2017)

2. Проект Закону про стимулювання ринку криптовалют та їх похідних в Україні (7183-1 від 10.10.2017)

3. Проект Закону про внесення змін до Податкового кодексу України (щодо стимулювання ринку криптовалют та їх похідних в Україні) (7246 від 30.10.2017)

4. Проект Закону про внесення змін до Податкового кодексу України та деяких інших законів України щодо оподаткування операцій з криптоактивами (2461 від 15.11.2019)

5. Проект Закону про віртуальні активи (3637 від 11.06.2020)

6. Проект Закону про токенизовані активи та криптоактиви (4328 від 05.11.2020)

Ми звернулись до цієї теми з огляду на прийняття в першому читанні проекту Закону про віртуальні активи (№ 3637), і подання на розгляд законопроекту про токенизовані активи і криптовалюти (№ 4328), що свідчить про активізацію роботи комітетів Верховної Ради України в цьому напрямку і чергову спробу законодавчого регулювання правового статусу криптовалюти.

Метою даної публікації є аналіз підходів до визначення поняття криптовалюти у вищенаведених законопроектах, та узагальнення зауважень техніко-юридичного характеру щодо підходів до формулювання дефініцій “криптовалюта” в правовому полі.

У проекті Закону про обіг криптовалюти в Україні (7183 від 06.10.2017) відзначено, що криптовалюта це – програмний код (набір символів, цифр та букв), що є об’єктом права власності, який може виступати засобом міні, відомості про який вносяться та зберігаються у системі блокчейн в якості облікових одиниць поточної системи блокчейн у вигляді даних (програмного коду) [1].

Проте, визначення певної речі об’єктом власності та/або предметом певного договору не може розглядатися як його особливого риса, яка відрізняє саме цю річ від усіх інших, що має відображатися у визначенні цієї речі [2].

Проект Закону про стимулювання ринку криптовалют та їх похідних в Україні (7183-1 від 10.10.2017) пропонує таке визначення криптовалюти – децентралізований цифровий вимір вартості, що може бути виражений в цифровому вигляді та функціонує як засіб обміну, збереження вартості або одиниця обліку, що заснований на математичних обчисленнях, є їх результатом та має криптографічний захист обліку. Криптовалюта для цілей правового регулювання вважається фінансовим активом [3].

В основу такого визначення покладено критерій форми вираження (цифровий вигляд), критерій цінності (є виміром вартості, та засобом обміну та одиницею обліку) та технічний критерій (заснований на математичних обчисленнях, має криптографічний захист).

У Проекті Закону про внесення змін до Податкового кодексу України (щодо стимулювання ринку криптовалют та їх похідних

в Україні) (7246 від 30.10.2017) було запропоновано звільнити від оподаткування прибуток підприємства, що надають фінансові послуги на ринку криптовалют та операції з майнінгу криптовалют [4].

При цьому, у пояснювальній записці відзначено, що нормативно правове регулювання повинно розглядатись у комплексній взаємодії, оскільки спрямовані на вирішення спільного завдання, а саме, створення умов для стимулювання розвитку діяльності криптовалют в Україні та їх видобування (реальні умови для майнерів), використання криптовалют у повсякденному житті та захист прав, законних інтересів споживачів й надавачів цих послуг, професійних учасників ринку [5].

У проекті Закону про внесення змін до Податкового кодексу України та деяких інших законів України щодо оподаткування операцій з криптоактивами (2461 від 15.11.2019) зазначено, що – віртуальний актив – особливий вид майна, який є цінністю у цифровій формі, яка створюється, обліковується та відчужується електронно. До віртуальних активів відносяться криптоактиви, токен-активи та інші віртуальні активи.

Криптоактив – вид віртуального активу у формі токenu, який створюється, обліковується та відчужується в розподіленому реєстрі та не посвідчує майнових та/або немайнових прав власника криптоактиву.

Токен-актив – вид віртуального активу у формі токenu, який створюється, обліковується та відчужується в розподіленому реєстрі, посвідчує майнові та/або немайнові права власника токен-активу, які відповідають зобов'язанням особи, яка випустила токен-актив. Операції з токен-активом оподатковуються за правилами, що застосовуються до майнових та/або немайнових прав, які посвідчує токен-актив. Токен – електронна одиниця обліку у формі запису в розподіленому реєстрі [6].

Запропоновані визначення понять «віртуальні активи», «криптоактиви», «токен-активи» є надто загальними та не дозволяють чітко визначити об'єкт оподаткування, виокремивши його від інших об'єктів цивільних прав, що, в кінцевому плані, може вико-

ристовуватись, з одного боку, для мінімізації податкових платежів шляхом приховування реального змісту господарської операції, а, з другого боку, для неодноразового оподаткування одного й того ж об'єкта.

Визначення ж віртуального активу як «особливого виду майна, який є цінністю у цифровій формі, яка створюється, обліковується та відчужується електронно», не може розглядатися як їх особлива риса, яка відрізняє саме ці об'єкти цивільних прав від усіх інших, описує не зміст відповідного явища, а лише вказує на його форму [7].

Крім того, у міжнародній практиці не існує єдиних підходів до визначення змісту вказаних інструментів, їх регулювання та оподаткування. Станом на 2017 рік, було запропоновано три можливих підходи до спроб правового регулювання операцій з криптовалютою:

1. на загальних підставах (розглядаючи операції для цілей оподаткування з «криптовалютами», «токенами» як операції з майном.
2. режим оподаткування для законних засобів платежу (в частині криптовалют)
3. режим фінансових інструментів, в тому числі цінних паперів (для токен-активів) [7].

Предметом правового регулювання Податкового Кодексу є «відносини, що виникають у сфері справляння податків і зборів» (ст. 2) тому визначення дефініцій “віртуальна валюта” “токен актив” “криптоактив” можуть застосовуватись лише для цілей оподаткування, а не регулювання правового статусу вказаних активів.

Отже, спроби визначення правового статусу криптовалюти через зміни і доповнення Податкового законодавства визнавались завідомо хибною траєкторією діяльності законотворців, що певно і мало наслідком відкликання вищенаведених законопроектів.

02.12.2020 у першому читанні прийнято Проект Закону про віртуальні активи (3637 від 11.06.2020), який визначає віртуальний актив – сукупність даних в електронній формі, яка має вартість та існує в системі обігу віртуальних активів. Віртуальний ак-

тив може бути як самостійним об'єктом цивільного обороту, так і посвідчувати майнові або немайнові права, зокрема, права вимоги на інші об'єкти цивільних прав [8].

Отже, за змістом вказаного припису «віртуальний актив», який посвідчує майнові і немайнові права, не визнається об'єктом цивільного обороту, а тому його участь у системі обігу віртуальних активів виглядає сумнівною.

Крім того у тексті законопроекту є такі види віртуальних активів: фінансові віртуальні активи, інвестиційні віртуальні активи, проте їх дефініцій в ст.1 Проекту не наведено. А дефініції “забезпечений/ не забезпечений віртуальний актив” розуміється «посвідчення ним майнових або немайнових прав». Однак, що саме мається на увазі під таким посвідченням у проекті також не визначено [9].

Цікаво відзначити, поняття віртуального активу (у проекті закону в первісній редакції від 09.06.2020) визначалось як особливий вид майна, який є цінністю в електронній формі, існує в системі обігу віртуальних активів, та може знаходитись у цивільному обігу.

Вказаний підхід віднесення віртуального активу до правового режиму майна, шляхом доповнення статті 190 Цивільного кодексу України (ст 190 ЦК України “Майном як особливим об'єктом вважаються окрема річ, сукупність речей, *віртуальні активи* а також майнові права та обов'язки [6]) вже був застосований у 2017 році, однак простого доповнення статті Цивільного Кодексу України недостатньо, для повноцінного визначення правового статусу, характерних ознак для віртуальних активів [7].

У проекті Закону про токенозовані активи та криптоактиви (4328 від 05.11.2020) у ст.1 визначення термінів криптоактив і токенозований актив повністю збігаються, зокрема – це вид віртуального активу, що існує виключно в системі обліку цифрових даних у вигляді запису з ідентифікатором інформації, що є похідною від первинного активу. При цьому, первинний актив – майно у будь-якому вигляді, що знаходиться у розпоряджанні користувача системи обліку цифрових даних та використовується для створен-

ня токенизованого активу з метою здійснення правочину, пов'язаного з цим майном, зокрема, але не виключно, для використання у господарських цілях або для особистого використання.

У статті 4 проекту Закону № 4328 вказано, що токенизований актив – є майновим правом у цифровому вигляді, в основі якого знаходиться токен розподіленого реєстру у вигляді ідентифікатора певної інформації, похідної від первинного активу.

У статті 7 проекту Закону № 4328 відзначено, що криптоактив є майном у цифровому вигляді, в основі якого знаходиться токен розподіленого реєстру у вигляді ідентифікатора певної інформації, що не є похідною від первинного активу. Непохідність – відсутністю безпосереднього правового зв'язку криптоактиву з правомочном щодо первинного активу.

У проекті закону відсутнє єдине розуміння поняття токенизованого активу та криптоактиву. Натомість у різних статтях ці поняття визначаються як – 1. віртуальні активи, як режим майнових прав у цифровому вигляді,

2. майна, у цифровому вигляді.

Такий підхід до визначення дефініцій розкриває лише зовнішню форму вираження токенактиву та криптоактиву, однак, не дозволяє однозначно відокремити за певними характеристиками ці явища один від одного, з метою встановлення їх сутнісних ознак, які впливають на вибір режиму правового регулювання.

Висновки: З аналізу запропонованих дефініцій криптовалют наведених у вищезазначених законопроектах вбачається, що виокремити сутнісні ознаки для формулювання дефініцій є досить проблематичним. Зокрема, пропонуються різні підходи до розуміння криптовалют:

1. програмний код, який є об'єктом права власності і виступає засобом міни
2. віртуальний актив, який посвідчує майнові права
3. цифровий вимір вартості (як одиниця обліку) який функціонує, як засіб обігу.
4. особливий вида майна, що має цінність у цифровій формі
5. сукупність даних в електронній формі, які мають вартість.

Варто вказати, що три основних підходи до визначення дефініцій криптовалюти це – 1.вид інформації, 2.майно, 3.одиниця вартості (цінності). Інший критерій – що, цей об’єкт виступає засобом і предметом обміну. Разом з тим, цих ознак виявилось недостатньо для відокремлення цього об’єкту від інших дефініцій, інших об’єктів та правових режимів. Не вирішеним це питання залишається і в двох останніх законопроектах, які залишають більше питань і протиріч. Отже, є місце для наступних наукових розвідок, формулювання пропозицій в цьому напрямку.

Дослідження проведено в межах виконання міжнародного проекту в сфері освіти «European Integration: legislation and the IoT» («Європейська інтеграція: законодавство та Інтернет речей») у межах напряму Жан Моне «Модуль» програми «Erasmus+» №620017-EPP-1-2020-1-UA-EPPJMO-MODULE (спільний проект КПП ім. Ігоря Сікорського, Еразмус+ Жан Моне Фонду та Виконавчого агентства з питань освіти, аудіовізуальної діяльності та культури за підтримки ЄС)». Підтримка Європейською комісією випуску цієї публікації не означає схвалення змісту, який відображає лише думки авторів, і Комісія не може нести відповідальність за будь-яке використання інформації, що міститься в ній.

Список використаних джерел:

1. Проект Закону про обіг криптовалюти в Україні реєстр. № 7183 від 06.10.2017 URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684
2. Висновок Головного науково-експертного управління на проект Закону України «Про обіг криптовалюти в Україні» (реєстр. № 7183 від 06.10.2017 р.) URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684
3. Проект Закону про стимулювання ринку криптовалют та їх похідних в Україні реєстр. № 7183-1 від 10.10.2017 URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62710
4. Проекті Закону про внесення змін до Податкового кодексу України (щодо стимулювання ринку криптовалют та їх похідних в Україні) реєстр.№7246 від 30.10.2017 URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62816

5. Пояснювальна записка до проекту Закону України «Про внесення змін до Податкового кодексу України

6. (щодо стимулювання ринку криптовалют та їх похідних в Україні реєстр № 7246 від 30.10.2017 URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62816

7. Проект Закону про внесення змін до Податкового кодексу України та деяких інших законів України щодо оподаткування операцій з криптоактивами реєстр. № 2461 від 15.11.2019 URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67423

8. Висновок Головного науково-експертного управління на проект Закону України «Про внесення змін до Податкового кодексу України та інших законів України щодо оподаткування операцій з криптоактивами» реєстр. № 2461 від 15.11.2019 URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67423

9. Проект Закону про віртуальні активи реєстр. №3637 від 11.06.2020 URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69110

10. Висновок Головного науково-експертного управління на проект Закону України «Про віртуальні активи» реєстр. № 3637 від 11.06.2020 URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69110

11. Проект Закону про токенизовані активи та криптоактиви реєстр. № 4328 від 05.11.2020 URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=70353

Азьмук Н.А.

доктор економічних наук, доцент
заступник директора з навчально-
методичної роботи, Черкаський
державний бізнес-коледж

МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ РИНКУ ПРАЦІ В КОНТЕКСТІ СТАНОВЛЕННЯ ЦИФРОВОЇ ЕКОНОМІКИ

Ключовою ознакою сучасної економіки є перехід до нового технологічного укладу, який обумовлює зміну продуктивних сил та виробничих відносин. Зміна технологічного укладу створює нові форми і види зайнятості, моделі організації трудової діяльності, трансформує процес і характер праці, соціально-трудова відносина та способи взаємодії між суб'єктами ринку праці. У результаті підвищення рівня гнучкості виробництва та індивідуалізації товарів і послуг набувають поширення нестандартні форми зайнятості. Гнучка зайнятість стає новим способом оптимізації виробництва й організації процесу праці. Цифровізація економіки спричиняє використання у процесі виробництва штучного інтелекту, роботів, хмарних технологій, збільшує попит на ринку праці на працівників, які мають цифрові навички.

Однак система державного управління недостатньо готова до таких змін. Швидкі темпи впровадження цифрових технологій в управлінські та виробничі процеси посилюють дисбаланс між розвитком національного ринку праці та цифровою економікою. Перш за все це обумовлено нескоординованістю рішень і дій різних органів влади – як законодавчої, так і виконавчої, їх ізольованістю при формуванні стратегій цифрового, соціально-економічного та освітньо-професійного розвитку. Поза межами державного регулювання залишаються сучасні динамічні процеси цифровізації, що змінюють структуру ринку праці, сприяють інтеграції галузевих ринків і секторів економіки, формують новий цифровий сегмент, який через глобальний характер нехтує національними інтересами. Цифрові технології створюють нову форму трудової міграції – цифрову. Формування глобального цифрового сегмента ринку пра-

ці супроводжується економічними та соціальними протиріччями, які особливо гостро проявляються в інституціонально недостатньо розвинутих країнах, таких як Україна. Це потребує посилення орієнтації державної політики соціально-економічного розвитку в напрямі забезпечення збалансування процесів трансформації національного ринку праці та становлення цифрової економіки. Незважаючи на ухвалення останнім часом цілої низки нормативно-правових документів щодо економічного розвитку, розвитку освіти і науки України, цифрової трансформації суспільства, актуальним є вдосконалення методологічного апарату виявлення та оцінювання тенденцій трансформації ринку праці, обґрунтування стратегічних пріоритетів регулювання зайнятості з позиції поліпшення конкурентних позицій країни при переході до цифрової економіки.

Проблеми збалансування розвитку цифрових технологій і трансформації зайнятості в системі управління національною економікою посилюються неузгодженістю між собою різних за рівнем і змістовним наповненням стратегій соціально-економічного розвитку. теоретико-методологічні та практичні питання трансформації ринку праці, ідентифікації та регулювання цифрових форм зайнятості набувають нових аспектів у контексті сучасних процесів глобалізації та тенденцій розвитку цифрової економіки. Відсутність у сучасній теорії управління теоретико-методологічних положень, які системно розкривають особливості, тенденції трансформації ринку праці при переході до цифрової економіки, а також недостатність наукових доробків прикладного характеру з діагностики ринку праці та розробки цифрових інструментів регулювання зайнятості обумовлюють актуальність такого роду досліджень.

Поява та поширення нестандартних форм зайнятості обумовлена змінами технологій зовнішнього та внутрішнього середовища. В ході дослідження ринку праці в контексті сучасного економічного розвитку і становлення цифрової економіки доцільно виявити зв'язки між змінами технологічних укладів і трансформацією форм зайнятості.

Підвищення гнучкості та індивідуалізація виробництва, зменшення енерго- і матеріаломісткості, зростання нематеріального

виробництва приводять до поширення нестандартних форм зайнятості. Ознакою переходу до цифрової економіки є формування та поширення цифрової зайнятості. Передумовою для визначення змісту категорії «цифрова зайнятість» є визначення критеріїв віднесення до неї зайнятих осіб. Критеріями віднесення до цифрової зайнятості є відповідність таким вимогам:

- процес праці відбувається виключно з використанням цифрових технологій;
- оцифровані соціально-трудові відносини;
- учасники проєктної команди взаємодіють через онлайн-платформи та інші цифрові засоби;
- результатом праці є цифровий продукт; оплата за працю здійснюється через цифрові платіжні та фінансові системи.

Цифрова зайнятість реалізується цифровими працівниками, а її трактування обумовлює змістовне наповнення цієї економічної категорії.

Цифровий працівник – це особа, яка виконує трудові функції у цифровий спосіб, обіймає цифрову посаду та отримує грошову винагороду за виконання трудових функцій через цифрові платіжні системи. Зміст категорії «*цифрове робоче місце*» розкривається в таких положеннях: робоче місце обладнане відповідно до змісту та характеру праці й інтегроване у цифровий або віртуальний робочий простір; його особливістю є наявність цифрових пристроїв, підключених до корпоративної комп'ютерної мережі підприємства. Цифрове робоче місце може бути стаціонарним або рухомим, останнє можливе за наявності відповідного змісту праці, яка не потребує складного обладнання та забезпечує мобільність працівника.

Зростання попиту на *цифрову смарт-зайнятість* й на інтелектуальну робочу силу з цифровими навичками при переході до V і VI технологічних укладів обумовлюється:

- упровадженням нових технологій та формуванням високопродуктивних робочих місць, цифровий характер яких визначається ключовими технологіями V і VI укладів;
- оцифровуванням трудового процесу при переході економіки до V і VI укладів, що зумовить потребу в працівниках із цифровими навичками;

- швидкими змінами технологій, що актуалізує потребу в постійному оновленні навичок працівниками;
- оптимізацією онлайн-навчання для опанування нових навичок.

Цифровий ринок праці – це специфічний сегмент глобального ринку праці, на якому попит і пропозиція формуються у цифровий спосіб та створюються умови для участі економічно активного населення у глобальному цифровому розподілі праці через залучення до глобального цифрового виробництва. Товаром цифрового ринку праці виступає результат трудової діяльності, створений за допомогою цифрових технологій.

Таблиця 1

Параметри, методи і показники діагностики національного ринку праці в умовах цифровізації економіки [1, с.15-16]

Складові параметру	Методи та показники оцінювання
Параметр «гнучкість»	
Зовнішня гнучкість	<i>Методи:</i> кількісний та якісний аналіз, групування, порівняльний аналіз, експертне опитування. <i>Показники:</i> рівень мобільності національного ринку праці, рівні зайнятості та безробіття населення; субіндекси індикатора «ринок праці» Індексу глобальної конкурентоспроможності
Внутрішня гнучкість	<i>Методи:</i> кількісний та якісний аналіз, групування, порівняльний аналіз, експертне опитування. <i>Показники:</i> частки неформально зайнятих, самозайнятих, зайнятих неповний робочий день, Субіндекси індикатора «ринок праці» Індексу глобальної конкурентоспроможності
Цифрова гнучкість	<i>Методи:</i> розробка наукової гіпотези, математичне моделювання, соціологічне опитування, експертне опитування. <i>Показники:</i> кількість зайнятих, обсяг реалізації, додана вартість у сфері чистих цифрових продуктів, частка працівників, які використовували ІКТ

Гнучкість оплати праці	<i>Методи:</i> системний, кількісний та якісний аналіз, групування, порівняльний аналіз. <i>Показники:</i> динаміка середньомісячної заробітної плати, погодинна ставка, субіндекси індикатора «ринок праці» Індексу глобальної конкурентоспроможності
Параметр «соціальний захист»	
Захист робочих місць	<i>Методи:</i> системний, аналіз документів, соціологічне й експертне опитування. <i>Показники:</i> оборот робочої сили, охоплення працівників колективними договорами, субіндекси індикаторів «ринок праці», «інституції» Індексу глобальної конкурентоспроможності
Підтримка зайнятості	<i>Методи:</i> системний, аналіз документів, експертне опитування. <i>Показники:</i> наявність вакансій, кількість працевлаштованих
Гарантія виплати заробленого доходу	<i>Методи:</i> кількісний та якісний аналіз, групування, аналіз документів, соціологічне опитування, експертне опитування. <i>Показники:</i> заборгованість з виплат по оплаті праці, субіндекси індикатора «інституції» Індексу глобальної конкурентоспроможності
Комбінований захист	<i>Методи:</i> соціологічне й експертне опитування. <i>Показники:</i> рівень доступності окремих соціальних послуг

Отже, під впливом цифровізації економіки з'являється новий вид зайнятості – цифровий, що обумовлює необхідність формування й удосконалення відповідного понятійно-категоріального апарату; зокрема, таких понять, як «цифрова зайнятість», «цифровий працівник», «цифрове робоче місце», «цифрова посада», а також їх нормативно-правовий статус. Запропонована методологія дозволяє виконати поглиблене оцінювання процесів трансформації зайнятості та соціально-трудоих відносин, які відбуваються на національному ринку праці в умовах цифрової економіки.

Література:

1. Азьмук Н.А. Стратегічні напрями збалансування розвитку національного ринку праці та цифрової економіки. Автореферат дисертації на здобуття наукового ступеня доктора економічних наук за спеціальністю 08.00.03 – економіка та управління національним господарством, ІЕП НАН України, 2020. – с. 50.

Забара І.М.

кандидат юридичних наук, доцент,
доцент кафедри міжнародного
права Інституту міжнародних
відносин Київського національного
університету імені Тараса Шевченка

ДО ПИТАННЯ ПРОБЛЕМАТИКИ МІЖНАРОДНО-ПРАВОВОГО РЕГУЛЮВАННЯ ЦИФРОВОЇ ЕКОНОМІКИ

Становлення і розвиток глобального інформаційного суспільства концептуально передбачає виконання комплексу заходів – філософських, організаційних, економічних, правових та інших. Прийняті Світовим самітом з інформаційного суспільства ще у 2003/2005 роках Принципи, План дій, Зобов'язання і Програма [1] були з часом доповнені Заявою ССІС+10 про виконання рішень ССІС та Концепцією ССІС на період після 2015 року.

Одним з актуальних, важливих і таких, що зберігають потенційне значення напрямків сталого розвитку, в умовах формування інформаційного суспільства на базі інформаційно-комунікаційних технологій (далі – ІКТ), постало і залишається питання «електронного бізнесу».

Концепція ССІС на період після 2015 року [2] передбачає у цьому питанні дотримання визначених загальних орієнтирів, що дають змогу державам не тільки планувати, розвивати і бачити власні досягнення, але й оцінювати власний розвиток у порівнянні з іншими державами. Передбачається, що розвиток «електронного бізнесу» [2] здійснюватиметься шляхом:

а) забезпечення для комерційних підприємств можливості використання відповідних ІКТ і використання в повній мірі переваг *інформаційної економіки*, в тому числі шляхом створення сприятливого середовища для купівлі-продажу товарів і послуг мережами ІКТ.

б) посилення заохочення усіх зацікавлених сторін у просуванні переваг *електронного бізнесу* і стимулюванні розвитку нових додатків, контенту і послуг електронного бізнесу, у тому числі для мобільних пристроїв та соціальних мереж.

с) розвиток динамічного сектору ІКТ для підтримки продуктивного використання ІКТ, сталого росту і розвитку, створення робочих місць, торгівлі і інновацій в рамках широких стратегій скорочення масштабів бідності шляхом зростання добробуту;

д) сприяння входженню мікропідприємств, малих і середніх підприємств і залучення молоді та жінок-підприємців в усі сектори електронного бізнесу з урахуванням нових технологічних тенденцій.

е) підвищення доступності статистичних даних по електронному бізнесу, що є необхідними для оцінки економічних і соціальних наслідків».

Проте, стрімкий розвиток сфери ІКТ визначає і нові напрямки і горизонти. Зокрема, початкові назви «інформаційна економіка», «електронний бізнес» вже не вважаються такими, що можуть охопити усі прояви використання ІКТ у секторі економіки. Доцільним вважається термін «*цифрова економіка*». Це відмічає і Конференція ООН з торгівлі і розвитку (ЮНКТАД) у своїх доповідях [3].

Разом з тим, вважається, що процес поширення використання ІКТ продовжується і ми вже маємо і матимемо в подальшому справу з трьома складовими елементами, а саме: власне цифровим сектором, цифровою економікою і цифровізованою економікою [4], [3].

Не звертати увагу на це явище – «цифрову економіку» – вже неможливо, оскільки, за різними підрахунками, її обсяг вже вийшов на рівень двозначних чисел щорічного економічного

зростання у масштабах світової економіки. Причиною такого зростання виступають технологічний, економічний і політичний чинники.

Для розуміння явища і змін, які воно несе, варто звернутись до історії його розвитку.

На початковому (базовому) рівні розвитку – 1970-1990 рр. – зміни в економіці були пов'язані зі становленням і розвитком відносин на основі Інтернету, який і до сьогодні виступає основою цифрової економіки.

Цей етап характеризується наявністю Інтернету та технічною інфраструктурою, як початковою умовою його функціонування: виробництвом комплектуючих та програмного забезпечення, використанням ІТ-консалтингу, наданням інформаційних послуг і розвитком телекомунікацій. Зауважимо, що всі зазначені складові функціонують і розвиваються незалежно від існування нових технологій вищих рівнів.

На другому рівні – 2000-2010 рр. – розвиток ІКТ створив передумови для зміни у світовій економічній системі.

Цей процес, (за даними ОЕСР, 2015 р.) характеризується наступним:

- впровадженням цифрових датчиків у якомога більшу кількість приладів («Інтернет речей»),
- створенням нових персональних приладів (мобільних телефонів, смартфонів, планшетів, ноутбуків, лептопів, пристроїв для тривимірного друку, а також нових цифрових моделей («хмарна» зберігання даних, цифрові платформи, цифрові послуги),
- зростаючою інтенсивністю використання масивів даних із застосуванням технологій «великих даних» (big data), нових методів аналізу даних і алгоритмів прийняття рішень, нових технологій автоматизації і роботизації.

Цей етап характеризується значними обсягами інформації, що передається і зберігається. Зауважимо, що обмін інформацією є можливим і без дротових та бездротових пристроїв проте, цифрова економіка без цього не функціонуватиме.

При цьому розвиток ІКТ здійснює як позитивний, так і негативний вплив. Негативний вплив має прояв через дезорганізацію діючих і виникнення нових економічних процесів, систем, секторів; зміну поточної моделі споживання; зміну у діловій активності і моделях бізнесу.

Враховуючи широкий спектр визначень «цифрової економіки» [4], дотримуватимемось того підходу, що характеризує її як «скупність усіх прикладів екстенсивного використання ІКТ і створення нових технологій» [4].

Якщо «приклад екстенсивного використання ІКТ» вже давно є предметом наукових правових дискусій, і у певних випадках вже знайшли відображення в міжнародних актах універсального, регіонального і двостороннього співробітництва, то питання нових технологій, їх використання (і, можливо, і обмежень) залишається відкритим для дискусій і наукових розробок.

До таких «перспективних елементів цифрової економіки», враховуючи різні підходи, можна віднести наступне:

а) складові, що є новими видами економічної діяльності, які не існували до появи ІКТ:

- платформна економіка;
- економіка «вільного заробітку» (гіганоміка, gig-economy);
- економіка «спільного споживання» (sharing-economy);

б) складові, які виступають новітніми видами діяльності:

- нейротехнології і штучний інтелект;
- квантові технології;
- «нові» технології «великих даних» (big data +),
- системи розподільного реєстру;
- промисловий Інтернет;
- нові виробничі технології (на базі ІКТ);
- робототехніка і сенсорики;
- технології бездротового зв'язку;
- технології віртуальної і додаткової реальності.

Застосування «перспективних елементів цифрової економіки», зрозуміло, потребує як сучасного наукового осмислення, так і їх економічного використання і відповідного міжнародно-правового регулювання.

Використана література

1. Geneva Declaration of Principles. WSIS-03/GENEVA/DOC/0004; Geneva Plan of Action. WSIS-03/GENEVA/DOC/0005. [Електронний ресурс]. – Режим доступу: http://www.itu.int/net/wsis/documents/doc_multi.asp?lang=en&id=1161|1160
2. WSIS + 10 Statement on implementation of WSIS Outcomes and the WSIS + 10 Vision for WSIS Beyond 2015. [Електронний ресурс]. – Режим доступу: <http://www.itu.int/net/wsis/documents/HLE.html>
3. ЮНКТАД Доклад о цифровой экономике 2019. Создание стоимости и получение выгод: последствия для развивающихся стран.
4. Bukh R., Heeks R. (2017) Defining, Conceptualising and Measuring the Digital Economy. Global Development Institute working papers. No. 68. Режим доступа: <https://diodeweb.files.wordpress.com/2017/08/diwpkpr68-diode.pdf>

Некіт К.Г.

кандидат юридичних наук, доцент,
докторант кафедри цивільного права
Національний університет «Одеська
юридична академія»

ЩОДО ПОНЯТТЯ ТА СУТНОСТІ СМАРТ-КОНТРАКТІВ

Для розуміння сутності смарт-контракту необхідно проаналізувати його технічну та юридичну сутність.

З технічної точки зору, смарт-контракт є комп'ютерним кодом, який при настанні певного стану або умов здатен працювати автоматично відповідно до заздалегідь визначених функцій. Це фрагмент програмного коду, який виконує певні задачі у випадку виконання заздалегідь встановленої у програмі умови [1]. Цей код здатен зберігатися у розподіленому реєстрі та записувати будь-які зміни в нього [2, с. 53]. При використанні технології блокчейн чи інших розподілених реєстрів смарт-контракт зберігається та дублюється в ньому, алгоритми смарт-контракта визначаються його програмним кодом усередині мережі розподіленого реєстру. Тому кожен, хто має доступ до розподіленого реєстру, може перевірити,

що смарт-контракт функціонує відповідно до передбачених умов, що забезпечує неможливість їх зміни [3, с. 109]. Технічна сторона смарт-контракту відображена у його визначеннях як різновиду кодування, способу функціонування блокчейну, як фрагмента коду, який реалізований на платформі блокчейн та ініціюється блокчейн-транзакціями, а також організовує внесення записів у базу даних [4].

Деякі дослідники аналізуючи технічні аспекти смарт-контрактів звертають увагу в першу чергу на забезпечення ними виконання зобов'язань. Вони підкреслюють, що смарт-контракти це комп'ютерні програми, пов'язані із виконанням зобов'язань. Вони мають дві функції: смарт-контракт або безпосередньо виконує, або відстежує виконання (порушення) волі, узгодженої сторонами [5].

Доволі поширеним визначенням поняття смарт-контракту з юридичної точки зору є його розуміння як угоди сторін, що існує у формі програмного коду, який функціонує у розподіленому реєстрі даних та забезпечує самовиконуємість умов такого договору при настанні заздалегідь визначених у ньому обставин [6, с. 41].

Розуміння смарт-контрактів як договорів, що самовиконуються, зустрічається також в європейській [7] та американській доктринах. Так, Ф. Алабі зазначає, що договір, який виконується автоматичним/автоматизованим способом, є набором домовленостей сторін, на підставі яких здійснюється угода між ними [8].

Зустрічаються визначення смарт-контракту як запрограмованого договору, умови якого прописані у програмному коді і який автоматично виконується за допомогою блокчейну [9]. Однак відразу зазначимо, що смарт-контракти можуть існувати і на базі інших розподілених реєстрів, не лише блокчейну. Смарт-контракт визначається також як форма вираження договору у спеціальній комп'ютеризованій системі, яка забезпечує автономний механізм формального контролю та виконання його умов [10]. Пропонується також визначати смарт-контракт як типову (спеціальну) договірну конструкцію, тобто договір, укладений за допомогою електронних або інших технічних засобів, умовами якого передбачено виконання зобов'язань, що виникають з нього, при настанні ви-

значених обставин без спрямованого на виконання зобов'язання окремо вираженого додаткового волевиявлення його сторін шляхом застосування інформаційних технологій, визначених умовами договору [2, с. 58].

Отже, потрібно розуміти, що поняття смарт-контракту охоплює як технічний, так і юридичний аспект. Деякі дослідники навіть ведуть мову про два різні терміни – smart contract і legal smart contract. Під першим розуміється програмний код, під другим – сформульовані та автоматизовані за допомогою коду умови угоди. Необхідність розрізняти ці два поняття обумовлена тим, що допускаються різні моделі використання смарт-контрактів. Перша модель припускає, що програмний код не замінює угоди, а лише автоматизує виконання (так звана зовнішня (external) модель). При другій моделі відносини між сторонами можуть оформлюватись за одним з двох варіантів: код або повністю замінює звичайний договір, або є складовою частиною такого договору. Це так звана вбудована або внутрішня (internal) модель [2]. Іноді для позначення цих моделей використовуються терміни legal smart contract і smart contract code [1]. Представляється, що вказані терміни можуть бути враховані при позначенні різновидів смарт-контрактів та їх класифікації.

Отже, все ж таки необхідно розрізняти поняття смарт-контракту як технічного явища (комп'ютерної програми) та юридичного. З цією метою доцільно ввести у правове поле одночасно два терміни, які дозволять розрізняти і різні моделі використання смарт-контрактів. Якщо смарт-контракт не замінює угоди, а лише автоматизує виконання, доцільно вести мову про «програмний код» або «код контракту». Якщо ж у смарт-контракті повністю прописані умови угоди таким чином, що він може її замінити повністю або частково, доцільно використовувати термін «юридичний смарт-контракт».

Література:

1. Smart contracts and distributed ledger – a legal perspective // ISDA Linklaters Whitepaper. August 2017. P. 5-6.
2. Гринь О.С., Гринь Е.С., Соловьев А.В. Правовая конструкция смарт-контракта: юридическая природа и сфера применения // Lex russica. 2019. № 8 (153). С. 51-62.
3. Богданова Е.Е. Проблемы применения смарт-контрактов в сделках с виртуальным имуществом // Lex russica. 2019. № 7(152). С. 108-118.
4. Новоселова Л. «Токенизация» объектов гражданского права // Хозяйство и право. 2017. №12. С. 29-44.
5. Вашкевич А.А. Смарт-контракты: что, зачем и как. М.: Симплонер, 2018. URL: <https://www.simplawyer.com/store/smart-contracts/smart-contracts-book/>
6. Савельев А.И. Договорное право 2.0: «умные контракты» как начало конца классического договорного права // Вестник гражданского права. 2016. № 3. С. 32-60.
7. Kerikmae T., Rull A. The future of law and technologies. Springer International Publishing Switzerland, 2016. 239 p.
8. Alabi F. Taking contracting digital: examination of the smart contracts experiment. New York University. Elsevier. 2017. №9. P. 8-9.
9. Волос А.А. Смарт-контракты и принципы гражданского права // Российская юстиция. 2018. № 12. С. 5-7.
10. Лукоянов Н.В. Правовые аспекты заключения, изменения и прекращения смарт-контрактов. URL: https://e-notabene.ru/lr/article_28115.html

Доронін І.М.

доктор юридичних наук, доцент
зав. наукової лабораторії НДІ
інформатики і права НАПрН України

ЗАГРОЗИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ В УМОВАХ ЦИФРОВИХ ТРАНСФОРМАЦІЙ ТА МЕЖІ ДЕРЖАВНОГО РЕГУЛЮВАННЯ

У сучасних умовах визначення та конкретизація загроз національній безпеці в системі державного управління відбувається відповідно до порядку, регламентованому спеціальними законодавчими актами.

Зокрема, визначаючи, що «існування, самозбереження і прогресивний розвиток України як суверенної держави залежать від здійснення цілеспрямованої політики щодо захисту її національних інтересів», в Концепції (основах державної політики), затвердженій постановою Верховної Ради України від 16.01.1997 № 3/97, було вперше встановлено існування загроз національній безпеці. Тоді ж був запропонований підхід до визначення та систематизації таких загроз у певних блоках – за сферами. Мова йде про загрози у політичній, економічній, соціальній, військовій, екологічній, науково-технологічній, інформаційній сферах.

У прийнятому 19.06.2003 Законі України «Про основи національної безпеки України», який визначав засади державного управління у сфері національної безпеки протягом 15 років, такий підхід до визначення було збережено. Водночас, зміни стосувались дефініції окремих сфер. Так, загрози конкретизувались у зовнішньо- та внутрішньополітичній сферах, сфері державної безпеки, військовій та безпеки державного кордону, економічній, соціальній, гуманітарній, екологічній, науково-технологічній, інформаційній сферах.

Більша деталізація та конкретна характеристика загроз визначалась у документах стратегічного планування. Першим таким документом була Стратегія національної безпеки України «Україна у світі, що змінюється», затверджена Указом Президента України від 12.02.2007. Цей документ конкретизував визначення загроз у певних сферах. У подальшому документи стратегічного планування, що ухвалювалися з 2007 року, відображали політичні погляди, що характеризували державну політику того чи іншого Президента України.

Ухвалення у 2018 році Закону України «Про національну безпеку України» докорінно змінило порядок визначення загроз національній безпеці. Так, визначення загроз національній безпеці має відбуватись у документах стратегічного планування. Зазначено зумовлювало необхідність більш гнучкого підходу у реагуванні на актуалізацію тих чи інших загроз. У цьому аспекті варто про-

аналізувати зміст двох останніх Стратегій національної безпеки України, ухвалених після початку агресії проти України.

Так, Стратегія національної безпеки, затверджена Указом Президента України від 26.05.2015 № 287/2015, містить деталізований перелік загроз національній безпеці, який відповідав зовнішньо- і внутрішньополітичній ситуації в умовах протидії агресії проти України. Основною актуальною загрозою визначались агресивні дії Росії «що здійснюються для виснаження української економіки і підриву суспільно-політичної стабільності з метою знищення держави Україна і захоплення її території». У подальшому актуальні загрози було систематизовано за певними блоками, до числа яких віднесено «неефективність системи забезпечення національної безпеки і оборони України», «корупцію та неефективну систему державного управління», «економічну кризу, виснаження фінансових ресурсів держави, зниження рівня життя населення», а також загрози енергетичній, екологічній, інформаційній, кібербезпеці, безпеці критичної інфраструктури.

На відміну від цього, ухвалена вперше відповідно до оновленого законодавства, Стратегія національної безпеки (затверджена Указом від 14.09.2020 № 392), що характеризує державну політику Президента України В.Зеленського, демонструє доволі абстрактний підхід як до визначення загроз так і їх характеристики. 24 пункти цього розділу містять в основному публіцистичне і несистематизоване викладення загальної безпекової ситуації, як саме вона сприймається авторами документа. Як показує аналіз його змісту, можливо вести мову про визначення основної загрози у сфері безпеки – це «наслідки зміни клімату та зростання техногенного навантаження на навколишнє природне середовище». У цьому ж пункті міститься перехід до інфекційних хвороб як загрози національній безпеці.

Отже, юридичне визначення загроз, що відповідно до приписів чинного законодавства, покладене на державні органи та посадові особи, відповідальні за стратегічне планування у сфері національної безпеки, у правовій системі існує. Саме розуміння таких загроз і має зумовлювати обсяги державного регулювання та державного

втручання у суспільні відносини в умовах цифрової трансформації суспільства.

Загальний підхід до державного впливу та правової регламентації викладено мною у деяких публікаціях [1, 2]. У цьому контексті варто нагадати, що доволі несистемний підхід, обраний в державному управлінні стосовно регулювання, зумовлений низкою чинників, що далеко не завжди враховують існування загроз національній безпеці. Так, загальним є постійне намагання створення в нашій державі різноманітних преференцій та інших форм «державної підтримки». Водночас, складнощі полягають у визначенні співвідношення державного стимулювання та можливості державних обмежень у цій сфері. Зокрема, для належного розвитку будь-якої економіки важливою є передбачуваність. Зрозуміло, що повною мірою це стосується і розвитку інноваційних галузей економіки, цифрової економіки у сучасних умовах тощо. Водночас, в системі державних інструментів впливу в інтересах національної безпеки є можливість застосування окремих обмежувальних заходів (санкцій). Відповідно до Закону України “Про санкції” вони мають застосовуватись за чітким та прозорим механізмом, інакше вони становитимуть загрозу розвитку економіки. Прикладом цього є прийняття рішення про фактичне блокування Інтернет-ресурсів з посиланням на п. 25 ч. 1 ст. 4 зазначеного Закону України, яка передбачає можливість застосування “інших санкцій” окрім уже перелічених у попередніх 24 пунктах цієї статті.

Іншим важливим питанням є забезпечення захисту державних ресурсів, а також дотримання вимог щодо обмеження поведінки з певними видами інформації. Так, проблематичним є застосування чинного законодавства до певних технологій (блокчейн та інші прояви DLT), хоча окремі пропозиції з цього приводу активно обговорюються в науковій літературі [3-5]. Законодавчі вимоги в Україні продиктовані у першу чергу відповідальністю держави за збереження інформації, що перебуває у її власності, або щодо якої обов’язок збереження викликаний необхідністю забезпечення національної безпеки. У такому разі суб’єкт, юридично відповідальний за збереження, визначений. Це держава в особі відповідних

уповноважених державних органів. Тому подальше державне регулювання вимагатиме належної регламентації повноважень тих чи інших державних органів. На жаль стан стратегічного планування у державі на цей час підстав для оптимізму не дає.

Підсумовуючи викладене можливо прийти до наступного основного висновку. Враховуючи, що визначення “цифровий” стосовно відносин у суспільстві та його окремих інститутів не містить нового змісту порівняно з тими, що вживались до опису ідентичних процесів у минулому (“електронний” та ін.), за винятком “цифрової економіки”, яка полягає у виробництві та продажу товарів та послуг, які не існують у фізичному світі, але використовуються людьми, відповідні заходи держави з регулювання суспільних відносин мають у першу чергу виходити із існування загроз національній безпеці. У такому разі законодавча та нормативно-правова база потребуватиме певного оновлення, але лише на підставі ретельного аналізу суті та перспектив розвитку технологій та їх впливу на загрози національній безпеці.

Список використаної літератури.

1. Доронін І.М. Цифровий розвиток та національна безпека у контексті правових проблем. Інформація і право. 2019. № 1. С. 29-36.
2. Доронін І.М. Правові аспекти національної безпеки в умовах технологічних трансформацій цифрової епохи. Стан та перспективи реформування сектору безпеки і оборони України: мат. II Міжнарод. наук.-практ. конф. (Київ, 30.11.2018). Київ, 2018. С. 186–187.
3. Reijers W., O’Brolchain F., Haynes P. Governance in Blockchain. Technologies & Social Contract Theories. Ledger. 2016. № 1. P. 134-151.
4. Katina, P. F., Keating, C. B., Sisti, J. A., Gheorghe, A. V. Blockchain governance. International Journal of Critical Infrastructures. 2019. Vol 15(2). P. 121-135.
5. De Filippi P., Mannan M., Reijers W. Blockchain as a confidence machine: The problem of trust & challenges of governance. Technology in Society. 2020. T. 62.101284.

Богущий П.П.

кандидат юридичних наук, доцент,
головний науковий співробітник
Науково-дослідного інституту
інформатики і права НАПрН України

ЦИФРОВА ТРАНСФОРМАЦІЯ СОЦІАЛЬНИХ КОМУНІКАЦІЙ ТА НАЦІОНАЛЬНА БЕЗПЕКА УКРАЇНИ

Сучасність характеризується поширенням електронних комунікацій, які заповнюють усі сфери соціального існування. Подальшим потужним поступом у розвитку електронних комунікацій стали цифрові технології. Наскільки обґрунтованим є узагальнене твердження про характеристику соціальних трансформацій сучасного суспільства як цифрових – питання, що має власне філософське обґрунтування та підлягає вирішенню у тому числі внаслідок правового дискурсу.

Цифрова трансформація суспільства сьогодні є об'єктивним процесом, але не завжди та в усьому здійснюється відповідно до певних правил, визначених національним законодавством з урахуванням міжнародно-правових принципів та підходів стосовно закріплення та реалізації прав, свобод людини.

Право на інформацію все більше набуває ознак одного з основних прав людини, а свобода електронних, цифрових комунікацій стає важливою для соціальних комунікацій, для реалізації можливостей кожної особи. Однак правове регулювання усього складного комплексу суспільних відносин, які виникають на основі електронних комунікацій, цифровізації суспільства, і передусім економічних відносин, не є досконалим, не в усіх випадках супроводжує сам процес електронних комунікацій, не забезпечує ефективність цифрових змін, які все більше набувають ознак революційних.

Відома статистика свідчить про стрімкий та всеохоплюючий розвиток процесу електронних комунікацій в українському су-

спільстві, що стає передумовою для цифровізації усіх аспектів соціальної діяльності, яка відбувається в умовах тривалих та непередбачуваних наразі соціальних трансформацій українського суспільства. За різними джерелами (Forbes Україна, 2015; Graham et al., 2017; OLI, 2018), в 2013–2017 роках наша країна посіла перше місце в Європі та четверте місце у світі за обсягом фінансових потоків і кількістю завдань, що виконуються на цифрових робочих платформах, Україна також посідає перше місце у світі в ІТ-фрілансі. Фріланс у сфері ІКТ в Україні зріс на 27% лише у 2017 році [1]. Зауважимо, що пов'язаність соціальних і цифрових трансформацій є взаємозалежною, але існуючі у цьому процесі закономірності не в усьому виявляються у сучасних українських реаліях.

Цифровізація економіки, соціального управління, адміністрування, впровадження електронного урядування є відмінними ознаками соціально-економічних змін у державах, які не перебувають в умовах трансформації економічної, політичної та правової систем. А такі трансформації є характерними для нинішнього стану України. Вказана обставина не може вважатися непереборною у здійсненні цифровізації економічних та інших суспільних відносин в Україні, проте не урахувати усіх складних та непередбачуваних умов соціальної трансформації було б відвертою помилкою.

Окрім необхідності забезпечення права людини на інформацію, на доступ до використання можливостей електронних ресурсів, на використання усіх сучасних досягнень цифрових технологій в адмініструванні, важливим є забезпечення безпеки не лише в інформаційній сфері, що стає очевидним, але в усіх напрямках, які формують стан національної безпеки, і, де здійснюється цифровізація. Вирішальним у цьому необхідно визнати якісне правове регулювання усіх соціальних комунікацій, що зазнають цифровізації. Посилює такий висновок необхідність забезпечення свободи вибору громадянам, які не сприймають цифровізації, якщо це стосується їхніх особистих прав та свобод. Звичайно, така категорія громадян, суб'єктів соціальних комунікацій є значно меншою у співвідношенні до усього населення країни, проте не урахувати

їхніх потреб і не зважати на наявність іншості у цьому загальному або ж глобальному процесі з позицій права було б невірним.

Цифрова трансформація соціальних комунікацій, попри інноваційність, притаманну більшості галузям соціальної діяльності, попри спрощення будь-якого відомого раніше алгоритму дій для досягнення результату, передбачає чітко визначену залежність у прийнятті рішення від програми, розрахованої на певну процедуру. Відчуженість людини від участі в адмініструванні або ж в управлінні має свої переваги, а в деяких галузях виробництва стає незамінною, що обумовлює, зокрема, створення та використання робототехніки. Однак, в усіх випадках цифрової форми соціальних комунікацій має зберігатися основа, якою є дуальність забезпечення прав та свобод людини і забезпечення національної безпеки. Така основа передбачає звернення до права, що не може зазнавати обмежень у жодному випадку, а приведення цифровізації у відповідність з правовими вимогами не є формальним актом.

Програмування певних (якщо не усіх) правових вимог у процесі цифрової трансформації соціальних комунікацій залишає обґрунтовані сподівання на збереження та реалізацію ціннісної системи, яку підтримує у суспільстві право. Якщо погодитися з висловленою теорією існуючих етапів соціальної трансформації українського суспільства [2], то сучасний етап такої трансформації якраз і полягає у трансформаційних змінах ціннісної системи. Звичайно виникає питання – як зберегти систему цінностей у процесі цифрової трансформації за умови зміни самої системи? Власне це питання і є основоположним для забезпечення національної безпеки у складному процесі цифрової трансформації.

Варто також зауважити, що збереження найважливіших соціальних цінностей у спосіб їхнього правового визнання та охорони є важливою складовою захисту національних інтересів, які розглядаються як об'єкти права національної безпеки [3]. За таких обставин можна зробити висновок, що цифрова трансформація сучасного українського суспільства для досягнення своєї мети має здійснюватися на основі права, за умови надійного захисту прав, свобод людини і громадянина, орієнтуючись на існуючу ціннісну

систему суспільства для визначення і захисту національних інтересів, які розглядаються об'єктами права національної безпеки.

Список використаної літератури :

1. Федулова Л.І. Цифрова трансформація (цифровізація) регіонів України. Аналітична записка. URL: <http://academy.gov.ua/pages/dop/198/files/4ba4c1b4-cefe-4f27-b58b-3aee7c8cf152.pdf>.
2. Гловаха Євген. Українське суспільство: шляхи трансформації. Український соціологічний журнал. – 2016. – №1-2. – С.26-30.
3. Богущкий П. П. Концептуальні засади права національної безпеки України : монографія. Київ-Одеса: Фенікс. – 2020. – С.172-186.

ВИСТУПИ УЧАСНИКІВ КОНФЕРЕНЦІЇ

Марущак А.І.,

доктор юридичних наук, професор,
професор Національної академії
Служби безпеки України,
стратегічний радник Міжнародної
академії інформації

СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ ОСВІТНІХ ПРОЄКТІВ ІЗ ПІДВИЩЕННЯ КІБЕРГІГІЄНИ НАСЕЛЕННЯ УКРАЇНИ

Людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнані в Україні найвищою соціальною цінністю. Держава Україна має юридично і технологічно гарантувати повагу до приватного життя людини та унеможливити тотальний контроль над особою через створення надпотужних баз персональних даних, використання технологій штучного інтелекту, розпізнавання облич тощо.

Крім того, маніпуляції суспільною свідомістю, посилені використанням інформаційних технологій, створюють небезпеку антидемократичного розвитку українського суспільства, закладають глибокі соціальні конфлікти. Держава, шляхом інтенсивної освітньої політики, має відновлювати втрачені навички критичної обробки інформації людиною.

Крім того, маючи конкурентний потенціал вітчизняних фахівців у сфері інформаційних технологій, Україна фактично виключена зі світових економічних процесів через застарілість організації публічного управління, неспроможність політичних еліт протягом значного періоду незалежності України впровадити належний захист інтересів вітчизняних ІТ-компаній та їх працівників.

З іншого боку, забезпечення інформаційних прав людини і громадянина як основи для реалізації громадянських, політичних, економічних, соціальних, екологічних та інших прав, гарантованих Конституцією України, передбачає підвищення рівня інформаційно-правової культури громадян України.

Процеси діджиталізації суспільного життя зумовлюють необхідність побудови систем безпеки використання новітніх інформаційних технологій як у державному управлінні, так і серед бізнесу та звичайних громадян. І, хоча, підходи до побудови таких систем різняться для кожного з перерахованих видів суб'єктів – від імперативного для державних органів до диспозитивного для звичайних громадян, поєднує їх необхідність розуміння державними службовцями, працівниками сфери бізнесу і приватними користувачами основ кіберграмотності (кібергігієни).

Питання актуалізується з об'єктивним дорученням українського суспільства до новітніх інформаційних технологій. Так, нещодавно Кабінет Міністрів України затвердив Концепцію розвитку штучного інтелекту в Україні, яка серед іншого передбачає удосконалення середньої, вищої освіти та підвищення кваліфікації з метою підготовки кадрів у сфері штучного інтелекту, стимулювання наукових досліджень у галузі, підвищення рівня кібербезпеки, удосконалення законодавства у сфері кіберзахисту тощо [1].

Питання кібергігієни у тій або іншій мірі включені до навчальних програм спеціальностей з кібербезпеки та інформаційних технологій. Однак, проекти, спрямовані на підвищення рівня кібергігієни населення, мають фрагментарний і розпорошений характер. Такі освітні проекти в Україні потребують систематизації на основі наукових підходів задля усунення їх дублювання, уникнення витрачання бюджетних та залучених (донорських) ресурсів на проекти, що вже мають аналогічні об'єктні спрямування.

З цією метою можна класифікувати проекти, спрямовані на підвищення рівня кібергігієни населення, за суб'єктами їх реалізації (державні органи, громадські організації, бізнес-структури), за джерелами фінансування (державний бюджет, міжнародні донорські ресурси, благодійні і бізнес-ресурси), за категоріями осіб,

на які спрямовані (діти, молодь, працездатне населення України, пенсіонери, окремі професійні спільноти тощо).

До фінансованих державою відносимо, наприклад, нещодавно запроваджений Мінцифри України проект «Цифрограм», так званий національний тест на цифрову грамотність, який передбачає перевірку базових знань та навичок із цифрової грамотності у таких сферах: основи комп'ютерної грамотності, інформаційна та медіа грамотність, уміння працювати з даними, безпека у цифровому середовищі тощо [2].

Прикладом фінансованих ЄС проектів є створення онлайн-курсу про цифрові права для дітей, у якому зокрема розкриваються права дітей доступу до мережі, вільно висловлювати думки в мережі, право на інформацію тощо [3].

Міжнародні громадські організації, наприклад, УЄФА також пропонують своїм учасникам курси з питань найкращих практик з використання новітніх інформаційних технологій і захисту персональних даних [4].

Таких прикладів проектів, спрямованих на підвищення рівня кібергігієни населення, є багато. Виражаємо надію, що новостворена при Держспецзв'язку України Ради з інформаційної та кібербезпеки, до якої увійшов і представник Міжнародної академії інформації [5], буде спроможна систематизувати наявні і доступні в Україні проекти з кібергігієни задля масштабування їх на усі верстви населення України.

Література:

1. Кабмін затвердив концепцію розвитку штучного інтелекту в Україні. URL: <https://www.epravda.com.ua/news/2020/12/2/668750/>, 2 грудня 2020.
2. Мінцифра запускає «Цифрограм» – національний тест на цифрову грамотність. URL: <https://thedigital.gov.ua/news/mintsifra-zapuskac-tsifrogram-natsionalniy-test-na-tsifrovu-gramotnist>, 02 листопада 2020.
3. Цифрові права та безпека для дітей. URL: <http://minzmin.org.ua/digital>.
4. UEFA Cybersecurity and GDPR course. URL: <https://uefaacademy.com/cybersecurity/>.

5. Представник Академії обраний до складу Ради з інформаційної та кібербезпеки Державної служби спеціального зв'язку та захисту інформації України. URL: <https://interacademy.info/predstavnyk-akademii-obranyi-do-skladu-rady-z-informatsiinoi-ta-kiberbezpeky-derzhavnoi-sluzhby-spetsialnoho-zv-iazku-ta-zakhystu-informatsii-ukrainy/>. 3 грудня 2020.

Головко О.М.

кандидат юридичних наук, старший науковий співробітник НДІ інформатики і права НАПрН України, ст. викладач кафедри публічного права НТУУ “КПІ імені Ігоря Сікорського”.

ЦИФРОВА ОСВІТА ТА ЄС: ІНТЕРНЕТ РЕЧЕЙ В ДІІ

ІоТ-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 навчальні заклади різних рівнів незалежно від форми власності чи напряму навчання в 2020 році вимушено перейшли на дистанційну форму навчання через вірусну загрозу у вигляді COVID-19. Почали з'являтися так звані smart школи, тобто такі, що використовують ІоТ технології в своїй безпосередній роботі [1]. В 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 [2]. Серед напрямів роботи в даному документі визначено розробку етичних

стандартів використання штучного інтелекту (AI) та отриманих даних про студентів та викладачів в процесі навчання.

Обсяги даних у формі матеріалів для навчання, балів, видів роботи навчального та наукового спрямування стали ще більшими, адже офлайн форми комунікації з учнями та студентами перестали бути доступними. Виник ряд важливих питань щодо відкриття доступу до лекцій в режимі реального часу чітко визначеному колу осіб, їх ідентифікація, встановлення фактичної присутності особи на заході, а не суто технічного приєднання до заняття тощо.

Прикладами використання технологій Інтернету речей є наступні:

1) 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.

2) 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.

3) 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, швидкість серцебиття можуть бути корисними при прийнятті викладачем дистанційного іспиту, коли досить складно повністю унеможливити використанням студентами додаткових джерел чи сторонньої допомоги [3, с. 1671-1672].

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 в навчальний процес, ефективності тих чи інших завдань та способів донесення інформації тощо.

Оскільки в вищевказаному Плані дій ЄС щодо цифрової освіти на 2021-2027 роки передбачено використання даних учнів та викладачів, які фактично будуть користувачами технології штучного інтелекту та IoT, варто встановити чіткі межі між тим, які дані можуть використовуватися в освітній діяльності, а які можна вважати втручанням в приватне життя. На нашу думку, варто застосовувати принцип співмірності та виправданості використання певних даних про фактичного користувача здобутків цифрової трансформації в сфері освіти.

Жодним чином не можна допускати безальтернативності надання доступу до даних користувача освітньої послуги чи особи, яка таку послугу надає. Більше того, використання таких даних є недопустимим без надання згоди не тільки в технічному розумінні цього слова, наприклад, через згоду на умови роботи певного додатку. На нашу думку, установа, організація чи фізична особа, що надає освітню послугу має до угоди про надання послуги долучати також додаток, в якому передбачено виключний перелік технологій AI та IoT, які планується використовувати при навчанні, а також згода на обробку конкретних видів даних, як можуть бути отримані з мікрофону, відеокамери, GPS-навігатора тощо. Специфіка освітньої діяльності в умовах пандемії, з одного боку, показала ще більшу необхідність застосування інноваційних технологій, а з іншого – вказала на потребу додаткового правового регулювання договірних відносин в цій сфері задля уникнення загроз конфіденційності та посягання на приватність. Цифрова трансформація відкриває значні перспективи застосування технологій IoT в системі освіти, втім, мають бути забезпечені правила гри для такої взаємодії, що можливо через передбачення в законодавстві певних правових запобіжників зловживанню цифровими технологіями з боку суб'єктів освітнього процесу.

Проведений аналіз здійснено в рамках виконання міжнародного проекту №620017-EPP-1-2020-1-UA-EPPJMO-MODULE в сфері освіти «Європейська інтеграція: законодавство та Інтернет речей» (EULIoT) в межах напрямку Жан Моне «Модуль» програми «Erasmus+» (спільний проект КПІ ім. Ігоря Сікорського, Еразмус+

Жан Моне Фонду та Виконавчого агентства з питань освіти, аудіовізуальної діяльності та культури за підтримки ЄС)». Підтримка Європейською комісією випуску цієї публікації не означає схвалення її змісту, який відображає лише думку автора; Комісія не несе відповідальності за будь-яке використання інформації, що міститься в цій публікації.

Література:

1. Kusmin, M.; Saar, M.; Laanpere, M. Smart schoolhouse – Designing IoT study kits for project-based learning in STEM subjects. In Proceedings of the Global Engineering Education Conference (EDUCON), Tenerife, Spain, 17–20 April 2018; pp. 1514-1517.

2. Резолюція Digital Education Action Plan (2021-2027). URL: https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en

3. Ilieva, Galina; Yankova, Tania. IoT in Distance Learning during the COVID-19 Pandemic. TEM Journal. Volume 9, Issue 4. pp. 1669-1674.

Бежевець А.М.

аспірантка КПП ім. Ігоря Сікорського

ТРАНСФОРМАЦІЯ ПРАВА НА ІНФОРМАЦІЮ В УМОВАХ КАРАНТИНУ

Завданням кожної держави є забезпечення прав і свобод громадян, їх недоторканості та безпеки, а також створення умов для неухильного дотримання всіма суб'єктами вимог чинного законодавства. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави відповідно до ч.2 ст. 3 Конституції України.

Перелік прав людини і громадянина, який містить законодавство України, не є вичерпним, а їх гарантування є фундаментальною засадою діяльності влади.

Безумовно, важливим напрямком при цьому є забезпечення прав людини в інформаційній сфері, що особливо актуальне на шляху до інформатизації всіх сфер суспільного життя. У сучасних

умовах цифрової трансформації суспільства та держави доступ до різноманітної інформації значно спрощується, що, з одного боку, є позитивним кроком, але, з іншого боку тягне за собою певні загрози, зокрема, щодо ймовірності розголошення конфіденційної інформації.

Коефіцієнт ризиків та загроз у сфері дотримання інформаційних прав особи значно підвищився в умовах пандемії, викликаній захворюванням на COVID-19.

Відповідно до ст. 34 Конституції України, кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір. Така конституційна гарантія знаходить своє відображення і у статті 5 Закону України «Про інформацію»: право на інформацію передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів.

Протягом 2020 року було прийнято низку законодавчих актів, які, серед іншого, значно розширювали для громадян та суспільства в цілому можливості у сфері доступу до інформації. Зокрема, це стосувалося висвітлення діяльності суб'єктів владних повноважень щодо стану, перебігу та наслідків карантину. Доступ громадян до такої інформації є надзвичайно важливим для усвідомлення ситуації, в якій вони опинилися, а також заходів, яких вживає держава для мінімізації її негативних наслідків.

Одночасно слід відмітити, що реалізація прав, передбачених статтею 34 Конституції України, може бути обмежена законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя. Така норма національного законодавства корелюється із пунктом 2 статті 29 Загальної декларації прав людини 1948 року, згідно якого при здійсненні своїх прав і свобод кожна людина повинна зазнавати тільки таких обмежень, які

встановлені законом виключно з метою забезпечення належного визнання і поваги прав і свобод інших та забезпечення справедливих вимог моралі, громадського порядку і загального добробуту в демократичному суспільстві.

Таким чином, використовуючи своє право на доступ та поширення інформації, особа не повинна порушувати права і свободи інших осіб, в першу чергу – конституційне право на невтручання в особисте і сімейне життя. Це конституційне положення, передбачене ст. 32 Основного закону, реалізується у принципах інформаційних відносин, визначених у ст. 2 Закону України «Про інформацію». Так, основними принципами інформаційних відносин є гарантованість права на інформацію; відкритість, доступність інформації, свобода обміну інформацією; достовірність і повнота інформації; свобода вираження поглядів і переконань; правомірність одержання, використання, поширення, зберігання та захисту інформації; захищеність особи від втручання в її особисте та сімейне життя.

Непорушність принципів є основою стабільного функціонування інформаційної сфери. Закріплюючи це законодавче положення на найвищому рівні, держава тим самим декларує захист приватного життя особи від неправомірного втручання як органів влади, так і від третіх осіб, в тому числі засобів масової інформації.

Відповідно до Рішення Конституційного Суду № 2-рп/2012 від 20.01.2012, в якому міститься офіційне тлумачення частин першої, другої статті 32 Конституції України, інформація про особисте та сімейне життя особи (персональні дані про неї) – це будь-які відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, а саме: національність, освіта, сімейний стан, релігійні переконання, стан здоров'я, матеріальний стан, адреса, дата і місце народження, місце проживання та перебування тощо.

Науковий інтерес і тему цього дослідження викликали непоодинокі публікації в ЗМІ, соцмережах, а також звичайні паперові оголошення, розміщені на будинках, в яких містилася інформа-

ція про хворих на коронавірус. Зокрема, 08 квітня 2020 року видання «Вести» оприлюднило перелік адрес будинків у столиці, де нібито живуть хворі на коронавірус COVID-19. Редакція пояснила це начебто суспільним інтересом і закликом дотримуватися карантину. В подальшому такі випадки було неодноразово помічено і в інших містах. Таку ініціативу підхоплювали і окремі «свідомі» громадяни.

Однак, чи є таке втручання в особисте життя виправданим?

Для відповіді на це питання автором проаналізовано ряд зазначених вище положень чинного національного законодавства. Вказані норми ґрунтуються на положеннях Резолюції № 1165 Парламентської Асамблеї Ради Європи, якою визначено, що право кожної людини на приватність і право на свободу вираження поглядів є основою демократичного суспільства; ці права не є абсолютними і не мають ієрархічного характеру, оскільки мають однакову цінність (пункт 11). Виходячи з цього право на приватність, закріплене у статті 8 Конвенції про захист прав людини і основоположних свобод 1950 року, повинне захищати приватне життя особи не лише від втручання влади, а й від подібних дій з боку інших осіб чи інститутів, зокрема засобів масової інформації (пункт 12 Резолюції № 1165).

Таким чином, на думку автора, публікація інформації про хворих на коронавірус, що дозволяє прямо або опосередковано ідентифікувати особу, є порушенням права на недоторканність особистого життя.

Проте, держава, яка взяла на себе зобов'язання щодо забезпечення цього права, так і не створила дієвого механізму перешкоджання втручанням в особисте та сімейне життя людини, як того вимагають сучасні умови.

Пандемія – 2020 внесла суттєві корективи в життя людей та суспільства, зокрема, дещо прискорюючи процес цифровізації. Однак, карантин вплинув і на свідомість людини, причому не завжди цей вплив був коректним. Саме цей період яскраво підкреслив проблеми порушення принципів інформаційних відносин, вказавши на недоліки законодавства у сфері доступу до інформації.

Таким чином, на думку автора, законодавство у сфері інформації потребує удосконалення, зокрема, з урахуванням норм міжнародного права.

Шастун А.Д.,

кандидат економічних наук, ст.
науковий співробітник Інституту
економіки промисловості НАН
України

Амоша О.О.,

кандидат економічних наук, ст.
науковий співробітник Інституту
економіки промисловості НАН
України

Паньков Д.В.

провідний інженер Інституту
економіки промисловості НАН
України

СТРАТЕГІЧНІ ПРІОРИТЕТИ УКРАЇНИ В СВІТЛІ ЦИФРОВІЗАЦІЇ ЕКОНОМІКИ ТА ПОДОЛАННЯ ЗАГРОЗ КОРОНАКРИЗИ

Нові демоекономічні реалії, новий формат глобалізації нової економіки (так зване друге і третє роз'єднання), нова технологічна, мережева, цифрова, віртуальна реальність обумовлюють формування нової соціальної, трудової життєдіяльності з новими організаційними та інституційними структурами, параметрами ринку праці нового світогосподарства, у якому докорінно змінюються життєдіяльність і поведінка людей. Нинішня світова системна криза, що розгорнулася на початку 2020 року, несе потрійне навантаження – вона є водночас і епідеміологічною, і економічною, і соціальною, і геополітичною. Пандемія COVID-19 завдала руйнівного удару по соціально-економічній системі світу, кожної країни, України, зокрема, зумовивши потрійні наслідки для економіч-

ного зростання – шок пропозиції, шок попиту, шок міжнародної торгівлі, а саме [1, с.16-17]:

1) шок пропозиції – органами законодавчої і виконавчої влади та місцевого самоврядування адміністративним шляхом призупинена господарська, підприємницька діяльність низки секторів економіки, і серед них – туризм, громадське харчування, транспорт, індустрія спорту та розваг, ресторанний та готельний бізнес тощо;

2) шок попиту – доходи суб'єктів господарської діяльності, а отже, й домогосподарств, що пов'язані із секторами економіки, діяльність яких призупинена, заборонена та обмежена, стрімко знизилися і цей процес триває; за період пандемії приватне споживання сконцентрувалося на товарах першої необхідності, на засобах протиепідеміологічного захисту, ліках тощо; попит на інші товари різко зменшився, що має негативний вплив на всі сфери економічної діяльності;

3) шок міжнародної торгівлі – обмеження вільного переміщення товарів, людей, зниження до мінімуму міграційних потоків, подорожей призвело до порушення глобальних логістичних ланцюгів, дефіциту проміжних товарів з країн, які зазнали найбільших втрат, що пов'язані з пандемією COVID-19.

Такі шоки вносять суттєві зміни у всі складові глобального і національних ринків праці, впливаючи одночасно на попит, пропозицію та ціну послуг робочої сили. Прогнозується, що у період коронакризи та подальшого постпандемійного відновлення глобалізація, як і провідні бізнес-моделі, набуватимуть нового формату. Зростання ризиків у розбудові ланцюгів доданої вартості у зв'язку з пандемією COVID-19, підвищення вартості робочої сили в країнах, до яких масово переводилися виробництва з заходу, зниження вартості роботизації та інших техніко-технологічних новацій «Індустрії 4.0» (які до того ж не страждають від нових/старих вірусів) створюють вагомі передумови для повернення провідними компаніями світового рівня багатьох виробничих потужностей. Можна очікувати нову «хвилю» роботизації у постпандемійний період у розвинених країнах світу, а отже, й відбуватиметься зниження

попиту на працю та подальша трансформація соціально-трудової сфери.

Коронакриза поглибила конфлікт між глобальними економічними викликами і національними інтересами, посилила напруженість торговельних відносин між провідними економіками, спричинила нарощування боргових зобов'язань тощо. Найменшу готовність до викликів пандемії демонструють малі сировинні економіки з високим рівнем боргового навантаження. Україна увійшла в нову соціоекономічну пандемійну реальність з величезною кількістю невирішених проблем як зовнішнього, так і внутрішнього характеру, з депресивним бізнес-кліматом, надмірним зовнішнім боргом, високим рівнем доларизації, тінізації і криміналізації господарської діяльності.

Поточний порядок денний політики ЄС на сьогодні будується безпосередньо у парадигмі Четвертої промислової революції (національні програми “Індустрія 4.0”, “Зайнятість 4.0” та ін.), цифровізації, суспільства знань, соціальної інклюзії. Це відповідає базовим засадам платформи **Праця 4.0**. Новітня політика Євросоюзу чітко зорієнтована на “людино-центричні” підходи [2, с. 11-15]. Ще у допандемійний період у рамках реалізації Цифрового порядку денного ЄС Європейський Союз прийняв стратегію Єдиного Цифрового Ринку – Digital Single Market [3], яка передбачала відповідні інвестиції на суму 300 млрд євро за 7 років на її реалізацію. Планувалося, що завдяки роботі парламентського комітету Україна матиме змогу приєднатися до цієї стратегії і розраховувати в такому разі не менше, ніж на 6 млрд. євро інвестицій в цифрову інфраструктуру». Проте коронакриза порушила заплановані наміри, змінила пріоритети, хоча роль EU-4-Digital залишається ключовою й набуває нової значущості [4, с. 22-23]. Сучасні підходи ЄС до забезпечення стійкості сфери праці та зайнятості, до збалансування європейських ринків праці є системними та корельованими як з рекомендаціями МОП, глобальними Цілями сталого розвитку, Цілями розвитку тисячоліття (ЦРТ) так і з викликами, ініційованими пандемією, процесами цифровізації, міграції, демографічних змін, європейської інтеграції тощо.

На такі пріоритети має бути зорієнтована Стратегія соціально-економічного відновлення та розвитку України. Небезпідставно за ініціативи Президента України восени 2020 р. було здійснено аудит економіки держави, представлено його результати (6 листопада 2020 року) на платформі Центру економічного відновлення [5]. Результати аудиту показали, що нереалізований потенціал нашої країни складає 1 трлн. доларів США. Уряд України ставить перед собою амбіційне завдання – реалізувати цей потенціал, що спричинило до розробки проєкту «Національної економічної стратегії України 2030». Реалізація візії розвитку української економіки із визначенням напрямків і стратегічних цілей в межах цього проєкту Стратегії зводиться до такого [6]:

- 1) сформувані конкурентоспроможні умови для бізнесу та інвестицій і відновити довіру до держави,
- 2) виграти конкуренцію за капітал на світовому ринку,
- 3) стимулювати розвиток інновацій і модернізацію секторів економіки для забезпечення їх конкурентоспроможності на міжнародному ринку,
- 4) сприяти розвитку людського потенціалу і виграти конкуренцію за таланти.

Стратегічні цілі забезпечення цифрового розвитку в Україні за змістом проєкту зорієнтовані на створення умов для переходу на «цифрові» технології; трансформацію ресурсних секторів економіки в високопродуктивні, інтелектуальні та конкурентоспроможні; трансформацію сфер життя із архаїчних в сучасні та ефективні цифрові; створення нових можливостей для реалізації людського капіталу, розвитку інноваційних, креативних та «цифрових» індустрій та бізнесу.

У зв'язку з тим, що пандемія COVID-19 завдала руйнівного удару по економіці та сфері праці як в Україні, так і в світі, зумовивши потрійні довгострокові наслідки для національної економіки, до змісту проєкту Національної економічної стратегії України 2030 необхідно додати окремий сегмент «Подолання ризиків, загроз впливу пандемії COVID-19 на національну економіку, сферу праці та зайнятості та подальше постпандемійне відновлення із

залученням ресурсів цифровізації». Також цей сегмент має бути врахованим при подальшому формуванні відповідної нормативно-правової бази, а саме – при розробці Плану заходів з реалізації Національної економічної стратегії України 2030. Виставлений на обговорення проект Стратегії невиправдано не містить також таких сегментів, як «розвиток соціально-трудової сфери та ринку праці», «розвиток соціального діалогу в системі соціально-трудових відносин та державно-приватного партнерства» тощо. Життєздатна Стратегія соціально-економічного відновлення та розвитку України потребує системних дій держави, потужних партнерських відносин з бізнесом, реалізації політики узгоджених рішень суб'єктів соціального діалогу (сторін соціально-трудових та соціально-економічних відносин). Важливу роль відіграватиме протипандемійна регуляторна політика України, забезпечення умов для соціально-економічної стабільності й постпандемійного відновлення, зміцнення конкурентоспроможності національної економіки й можливостей забезпечення стійкості та гнучкості із залученням ресурсів мережево-цифрових, інформаційно-комунікативних технологій, платформної економіки.

Література

1. Колот А., Герасименко О. Сфера праці в умовах глобальної соціо-економічної реальності 2020: виклики для України. URL: <http://library.fes.de/pdf-files/bueros/ukraine/16344.pdf>
2. Работать ради лучшего будущего – Глобальная комиссия по вопросам будущего сферы труда. Женева, Международное бюро труда, 2019. 88 с. URL: https://www.ilo.org/wcmsp5/groups/public/---dgreports/--cabinet/documents/publication/wcms_662472.pdf
3. EU Digital Single Market URL: <https://eufordigital.eu/ru/discover-eu/eu-digital-single-market/>
4. Sparreboom Th., Tarvid A. Imbalanced Job Polarization and Skills Mismatch in Europe. *Journal for Labour Market Research*. July 2016. Vol. 49, Issue 1. P. 15-42. URL: <https://doi.org/10.1007/s12651-016-0196-y>
5. Уряд на платформі Центру економічного відновлення опублікував «Національну економічну стратегію 2030». URL: <https://www.ukrinform.ua/rubric-economy/3131102-kabmin-opublikuvav-nacionalnu-ekonomichnu>

strategiu-do-2030-roku.html https://nes2030.org.ua/?fbclid=IwAR2n7HwFWa2nptw7alD__If6j8neTGLRaMJ0XyV1OQcmCf34NHsjAXiw9YM#rec245567940

6. Вектори економічного розвитку до 2030 URL: https://nes2030.org.ua/?fbclid=IwAR2n7HwFWa2nptw7alD__If6j8neTGLRaMJ0XyV1OQcmCf34NHsjAXiw9YM#rec245890384

Водько Ю.В.

студентка КПІ ім. Ігоря Сікорського

Науковий керівник: **Дубняк М.В.**

к.ю.н. старший викладач кафедри

інформаційного права та права

інтелектуальної власності КПІ ім.

Ігоря Сікорського

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ СОЦІАЛЬНОЇ ТРАНСФОРМАЦІЇ НА ОСНОВІ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ

В еру, коли стрімко розвиваються цифрові технології і впроваджуються у всі сфери суспільного життя, неможливо залишати непоміченими зміни і у правовому регулюванні даних явищ. Безумовно, кожна галузь має свої особливості, завдання та цілі і від них залежить те, як швидко прохідиме їхня цифровізація, яка є незворотнім процесом сучасності. В розрізі нашого дослідження найбільш актуальним питанням постає саме правове регулювання цифровізації, оскільки, встановлення державою нормативних правил демонструє те, що вона зацікавлена у розвитку цієї сфери. У світі, де технології розвиваються з космічною швидкістю, складно постійно оновлювати законодавство, зважаючи на необхідність глибокого юридичного аналізу, проте саме це є необхідною умовою для розвитку суспільства та держави, для якого достатньо простих і зрозумілих правил, які б дозволяли швидко, якісно і ефективно перетворювати сфери суспільного життя у комфортне середовище для соціальної взаємодії.

Насамперед, найпершим завданням нашого дослідження є визначення термінів, які є необхідними для подальшого аналізу питань. Розпорядженням Кабінету Міністрів України «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації» запропоновано таке визначення поняття «цифровізація» як «насичення фізичного світу електронно-цифровими пристроями, засобами, системами та налагодження електронно-комунікаційного обміну між ними, що фактично уможливило інтегральну взаємодію віртуального та фізичного, тобто створює кіберфізичний простір» [1]. Це поки що єдине легальне визначення, яке можна відшукати в законодавстві. На нашу думку, недоліком вказаної дефініції є те, що з одного боку, присутнє його обмеження та конкретизація для можливості розуміння його сутності, а з іншого боку, поняття сформульовано із недостатньо глибоким аналізом та прогнозуванням перспектив розвитку цифровізації, оскільки засоби, системи та пристрої, за допомогою яких здійснюється цифрова взаємодія постійно зазнають змін, тому їхня характеристика потребує більш точного узагальнення та об'єктивного вираження.

У своїй праці, Баранов О.А. пропонує визначати соціальну трансформацію як корінне перетворення мети, структури та функцій суспільства або його окремих частин заради адаптації до суттєвих змін внутрішніх та зовнішніх умов, які є загрозою ефективності його подальшого розвитку [6]. Ми підтримуємо дану позицію, оскільки дійсно соціальна трансформація це в першу чергу про глибину змін у суспільній взаємодії та її призначення загалом. Щодо позначення змін внутрішніх та зовнішніх умов лише як загроз ефективності подальшого розвитку суспільств, вважаємо, що слід додати також, те, що дані зміни є і можливостями, які поруч із загрозами створюють виклики, через подолання яких відбувається прогрес.

Указ Президента України №392/2020 «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» визначає, що головною ціллю державної політики національної безпеки є реалізація нор-

ми Конституції України про те, що людина, її життя і здоров'я, честь і гідність, недоторканність і безпека – найвища соціальна цінність в Україні [2]. Таким чином, питання державної політики у сфері національної безпеки охоплює без перебільшення всі сфери суспільного життя і ми можемо розглядати питання соціальної трансформації на основі використання цифрових технологій на основі глобального та загального аналізу реалізації державної політики цифровізації.

Поруч з питанням правової регламентації цифровізації у галузі національної безпеки доречно зауважити про те, що сьогодні в Україні кількість цифрових послуг розширюється з кожним днем, але можливості скористатися ними є не скрізь. Як доречно зауважує у своїй праці Подольчак Н.Ю. однією із найбільших проблем виступає відсутність інтернет-комунікацій у малих населених пунктах, частині автомобільних та залізничних шляхів, гірській місцевості тощо [5]. Поліпшення ситуації з інтернет-мережами в Україні дозволить більшій кількості населення використовувати електронні можливості, що збільшить попит та конкуренцію в цифровій економіці. Вирішення даної проблеми покладено Міністерство цифрової трансформації, яке було утворене 2 вересня 2019 р. [3]. І, слід зауважити, за досить нетривалий час органу державної влади вдалось реалізувати потрібні та актуальні проекти, пов'язані з цифровізацією – це зокрема впровадження додатку «Дія» – мобільного застосунку із цифровими документами та порталу із публічними послугами, онлайн-сервісу для просування цифрової освіти серед населення тощо.

Доронін І.М. аналізуючи проблеми державного управління у сфері розвитку цифрових технологій зауважує, що дані питання детально розглядаються в економічному, управлінському, політологічному контексті, натомість у правовій науці можливо спостерігати вельми вузьке розуміння зазначених проблем – в рамках відповідних галузей правової науки [4]. Така диференціація на окремі галузі і встановлення між ними бар'єрів не сприяє комплексному розгляду питань правового регулювання.

Отже, як результат нашого дослідження маємо підсумувати, що на даному етапі розвитку цифровізації, правове забезпечення соціальної трансформації на основі використання цифрових технологій є ще недостатньо розробленим та конкретизованим. Реалізація даної мети можлива у поєднанні досліджень з різних галузей науки. Існує достатня кількість перешкод із забезпеченням доступу населення до інтернет-мереж, а також комунікаційного простору і поруч з вирішенням питання правової регламентації цифровізації необхідно поліпшувати ситуацію з прикладними проблемами, які є основою для проведення подальших змін. Позитивні приклади реалізації проєктів у сфері цифровізації в Україні створюють простір для генерації нових ідей та реалізації можливостей, які дозволяють краще зрозуміти яким чином слід покращувати правове забезпечення.

Список використаної літератури:

1. Концепція розвитку цифрової економіки та суспільства України на 2018-2020 роки / Кабінет Міністрів України. URL: <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80/conv#Text> (дата звернення: 07.12.2020).
2. Стратегія національної безпеки України / Ради національної безпеки і оборони України. URL: <https://zakon.rada.gov.ua/laws/show/392/2020#Text> (дата звернення: 07.12.2020).
3. Положення про Міністерство цифрової трансформації України / Кабінет Міністрів України. URL: <https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text> (дата звернення: 07.12.2020).
4. Доронін І.М. Цифровий розвиток та національна безпека у контексті правових проблем. *Інформація і право*. № 1(28). 2019. С. 29-36.
5. Подольчак Н. Ю., Білик О. І., Левицька Я. В. Сучасний стан цифровізації в Україні. *Ефективна економіка*. 2019. № 10. – URL: <http://www.economy.nauka.com.ua/?or=1&z=7300> (дата звернення: 07.12.2020).
6. Баранов О.А. Цифрова трансформація як джерело правових проблем. *Актуальні проблеми управління інформаційною безпекою держави: 2020 рік*: матеріали XI Всеукр. наук.-практ. конф. 15 трав. 2020 р. Київ : НА СБУ, 2020. С. 5-7.

Діденко Г.Ю.

студентка Новокаховського
гуманітарного інституту

Науковий керівник: **Пшенична М В.,**
к.е.н.

«УНІВЕРСИТЕТ ТРЕТЬОГО ВІКУ» ЯК МЕХАНІЗМ СОЦІАЛІЗАЦІЇ ЛЮДЕЙ СТАРШОГО ВІКУ В УМОВАХ СОЦІАЛЬНОЇ ТА ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Для більшості осіб вихід на пенсію є явищем психологічно неприємним та невтішним. Завершення трудової діяльності та відірваність від звичного кола спілкування призводить до вивільнення додаткового часу, що сприймається як період самотності, непотрібності та нереалізованості. Для того, щоб люди похилого віку почували себе повноцінними членами суспільства, дієвим інструментом в Стратегії державної політики з питань здорового та активного довголіття населення є їх залучення до системи безпервної освіти. Саме освіта впродовж життя та навчання в «університеті третього віку» дозволить спрямувати потенціал літніх осіб на персональний розвиток, соціальну адаптацію і збереження активної життєвої позиції людей на довгі роки.

For most people, retirement is a psychologically unpleasant and disappointing phenomenon. Completion of work and detachment from the usual circle of communication leads to the release of additional time, which is perceived as a period of loneliness, uselessness and unrealized. In order for the elderly to feel like full members of society, their involvement in the system of lifelong learning is an effective tool in the Strategy of State Policy on Healthy and Active Longevity. The education during the life and study at the «University of the third age» will direct the potential of older people to personal development, social adaptation and maintaining an active life position for many years.

За останніми аналітичними даними, Україна входить до тридцятки найстаріших країн світу. Згідно з національним демографічним прогнозом на період до 2025 року частка осіб віком від 60

років становитиме 25 %, а у 2030 році – понад 26 %. Тож, цілком зрозумілою є гостра необхідність розробки та впровадження в сферу соціальної роботи дієвого інструментарію культурно-дозвілєвого напрямку взаємодії з особами літнього віку.

У січні 2018 року Кабінет Міністрів України своїм розпорядженням схвалив Стратегію державної політики з питань здорового та активного довголіття населення на період до 2022 року. Документ передбачає комплексні заходи щодо підтримки громадян похилого віку, забезпечення їх активної участі в суспільному розвитку, підвищення якості життя, захисту прав.

Одним із пріоритетних кроків соціалізації вважаємо популяризацію ідеї «університетів третього віку»», адже концепція освіти для людей похилого віку є частиною сучасної парадигми безперервної освіти, актуальність якої полягає у глибинній потребі об'єднання людства на основі певних ціннісних і цільових орієнтирів світового співтовариства. Обумовлена вона прогресом науки та техніки, широким застосуванням інноваційних технологій та цифровою трансформацією.

Поняття «освіта впродовж життя» виникло у XX столітті, але його витоки можна віднайти ще у стародівніх філософів. На теренах наших земель відомий лікар і педагог М. І. Пирогов у 1855 р. відкрив першу безкоштовну школу для дорослих. В свою чергу, про безперервність освіти на міжнародному рівні заговорили у 1968 р. на генеральній конференції ЮНЕСКО та у 1972 р. на міжнародній конференції освіти дорослих.

Перший університет для людей зрілого віку був заснований у 1973 р. в Тулузі (Франція) професором П'єром Велла. Згодом ця ідея отримала популярність і швидко поширилася земною кулею. Сьогодні в багатьох країнах світу (США, Японія, Франція, Німеччина, Польща, Білорусія, Молдова та ін.) відкриті спеціальні курси, навчальні центри, народні університети та факультети для літніх людей.

Спільною рисою закладів освіти, зорієнтованих на старше покоління громадян, є їх спрямованість на персональний розвиток, соціальну адаптацію і збереження активної життєвої позиції лю-

дей віку (55+) та зрілого віку (75+). Тож, навіть міжнародне об'єднання університетів третього віку діє під гаслом: «Найбільшим культурним досягненням народу є його щасливі люди похилого віку» [2]. І це не дивно, адже, соціальна і цифрова трансформація, що має місце в сучасному світі, ставить нові виклики перед громадянами всіх вікових категорій, у тому числі – дорослих.

Слід зазначити, що значну зацікавленість студенти 55+ виявляють до правового захисту, краєзнавства та іноземних мов, багато охочих навчатися комп'ютерним технологіям. Разом з тим, як чоловіки, так і жінки із окресленого вікового діапазону визнають значущість здобуття навичок з психології та здорового способу життя, опанування техніки фізичних вправ для здорового довголіття.

Сучасні люди похилого віку все частіше прагнуть вести активне життя, в тому числі, зміцнюючи своє здоров'я заняттями спортом та потребують більше інформації й підтримки щодо формування й інтеграції у повсякденні справи корисних звичок. Крім того, спільні тренування в групах здоров'я, фізкультурно-рекреаційних закладах клубного типу дозволяють пенсіонерам почуватися комфортно, вільно знаходити співрозмовників, розраховувати на підтримку, співчуття та розуміння від ровесників, при цьому почувати себе частиною єдиного колективу [3, с.76].

Тож, маємо стійке переконання, що популяризація філософії навчання впродовж життя є невід'ємною складовою успішної реінтеграції літніх осіб до соціальних процесів, суспільних заходів, персональної активності шляхом реалізації.

Список використаних джерел:

1. Постанова КМУ «Про організацію надання соціальних послуг» від 01.06.2020 р. №587 [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/587-2020-%D0%BF>.

2. Наказ Мінсоцполітики України «Про впровадження соціально-педагогічної послуги «Університет третього віку»» від 25.08.2011р. №326. [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/rada/show/v0326739-11>.

3. Гриньків М. Я. Спортивна морфологія з основами вікової морфології : навч. посіб. / Мирослава Гриньків, Любомир Вовканич, Федір Музика. – Львів : ЛДУФК, 2015. – 304 с. [Електронний ресурс]. – Режим доступу: <https://hromadske.ua/posts/reformu-inkliuzyvnoi-osvity>.

Зінчук Д.О.

студентка КПП ім. Ігоря Сікорського

Науковий керівник: **Головко О.М.**

к.ю.н., ст. викладач КПП ім. Ігоря

Сікорського

ПРАВОВІ ПЕРСПЕКТИВИ МЕДІАЦІЇ З ВИКОРИСТАННЯМ ЦИФРОВИХ ТЕХНОЛОГІЙ

Розкриття проблеми дистанційної медіації є важливим в умовах сьогодення, адже в умовах карантину повноцінна діяльність медіаторів суттєво ускладнюється. Сам процес медіації є дійсно важливим та корисним, але відносно незвіданим у нашій країні. Зазвичай, сторони звикли вирішувати свій спір у судовому порядку, витрачаючи велику кількість коштів у ході судового розгляду, не використовуючи свого права на досудове врегулювання конфлікту. Деякі науковці наголошують на обов'язковості застосування процедур з примирення перед зверненням до державного суду [3, с. 63]. Дійсно, особі має бути забезпечена можливість застосування медіаційних практик. Однак, на думку Головко О. М., не застосування нею такої можливості не повинно унеможлилювати її право на звернення до суду [1, с. 146].

Медіатор виступає саме тим посередником, який є необхідним для мирного знаходження консенсусу між сторонами під час вирішення проблеми в ситуації, з якою до нього звертаються. Завдяки своїм навичкам медіатор здатний аналізувати конфлікт та стимулювати сторін до пошуку можливих варіантів домовленостей з урахуванням їхніх інтересів та потреб.

Чому ж тоді виникає проблема застосування такої практики? По-перше, медіація є доволі незвичним способом досудового ви-

рішення спорів між особами в Україні, оскільки деякі громадяни про неї просто не знають.

По-друге, виникнення проблеми з пандемією спричинило низку проблем, які тепер постають у медіаторів. Наразі дедалі важче проводити повноцінну процедуру медіації. Наприклад, під час заслуховування сторін важливо мати не лише зоровий контакт, але і певні довірительні відносини зі сторонами задля вдалого проведення медіації. На цьому ж етапі діяльність медіатора характеризується ставленням уточнюючих питань, які допоможуть сторонам краще зрозуміти один одного.

Одним із важливих принципів медіації є конфіденційність. Конфіденційність полягає у тому, що медіатор повинен тримати у таємниці і не розголошувати інформацію, яку він отримав під час спілкування зі сторонами або в процесі медіації. Крім того, він не може виступати в ролі свідка у суді щодо інформації, отриманої в процесі медіації [2, с.104].

На мою думку, не менш вагомою проблемою здійснення дистанційної комунікації є використання технічних засобів – тому що не завжди є можливість доступу до мережі або пристрою, що міг би вдало виконувати своє призначення. Тому для медіатора режим он-лайн роботи є досить великим викликом, який покладає більшу відповідальність та навантаження під час здійснення своєї роботи.

Підводячи підсумок, хочу зазначити: в сучасному світі (в епосі розвитку науково-технічного прогресу) є безліч варіантів, які могли б полегшити роботу медіаторів в здійсненні ними процедури медіації в дистанційній формі. Оскільки майже кожен має в своєму користуванні певний гаджет та доступ до мережі Інтернет.

Хоча перш за все, я вважаю, що необхідно розповсюдити інформацію про існування такого методу альтернативного вирішення спору як медіація. Саме через підвищення рівня обізнаності населення України і відбудеться стрімкий її розвиток. Таким чином і законодавець зможе врегулювати питання, які стосуються процесу медіації, шляхом прийняття відповідних нормативно-правових актів, які б безпосередньо містили основні положення, принципи та завдання медіаторів, а також роз'яснювали права та обов'язки

сторін. Тож, питання відносно перспектив проведення медіації в дистанційній формі все ж таки залишається відкритим і потребує правового врегулювання.

Список використаної літератури:

1. Головка О. М. Право на інформацію щодо альтернативних методів вирішення спорів. Інформація і право. 2019. Вип. № 1 (28). С. 144-151.
2. Землянська В.В. Відновне правосуддя в кримінальному процесі України: посібник. Київ: Видавець Захаренко В.О., 2008. 200 с.
3. Спектор О.М. Альтернативні способи вирішення цивільно-правових спорів: світовий досвід та перспективи застосування у правовій системі України: монографія. Київ: Фенікс, 2013. 160 с.

Радзієвська О.Г.

кандидат юридичних наук, старший дослідник, провідний науковий співробітник НДІ інформатики і права НАПрН України

ПРОБЛЕМИ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНИХ ПРАВ ЛЮДИНИ В УМОВАХ СОЦІАЛЬНИХ ТА ЦИФРОВИХ ТРАНСФОРМАЦІЙ

В умовах глобалізаційних процесів, що відбуваються у світі, прискореному розвитку технологій та значному збільшенні ролі інформації у всіх сферах життя сучасного суспільства інформаційні права та свободи людини набувають дедалі більшого значення в системі права, а їх реалізація стикається з новими викликами. Загострення інформаційного протиборства, яке відбувається на всіх рівнях, інформаційні війни, інформаційний тероризм і шахрайство в інформаційній сфері спонукають суспільство і державу до посилення системи заходів інформаційної безпеки. Нині жоден суб'єкт інформаційних відносин не є повністю захищеним від інформаційних загроз, а реалізація його прав часто залежить від забезпечення інформаційної безпеки.

Сьогодні інформаційні права людини доцільно розглядати у двох аспектах. З одного боку – це право на здійснення інформаційної діяльності, тобто права передбачені у статті 34 Конституції України. Зокрема, це передбачене в Основному Законі право на:

- інформацію (тобто збір, отримання інформації);
- дії з інформацією, що передбачає право на створення, перетворення, оброблення, систематизація, архівацію та інш.;
- поширення та обмін інформацією.

З іншого боку невід’ємною складовою інформаційних прав людини є право на захист в інформаційній сфері, що включає в себе:

- право на захист від негативних інформаційних впливів та інформаційного насилля;
- право на захист від маніпулювання свідомістю та від недостовірної (фейкової) інформації;
- право на захист особистої інформації та персональних даних.

Оскільки в інформаційному суспільстві особливого, ключового значення набувають інформація та знання, доступ до ресурсів, технологій та загальна обізнаність громадян, а також наявність техніко-технологічного забезпечення, то одним з ключових інформаційних прав громадян є право на доступ до інформації та знань і право на відсутність дискримінації в інформаційній сфері.

Ще на початку 2000-х років в Україні була введена в дію Національна програма інформатизації та був прийнятий Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки». Система заходів передбачала створення належних умов для функціонування інформаційного суспільства, забезпечення матеріально-технічною базою всіх соціальних об’єктів, у тому числі навчально-освітніх закладів.

Однак, не зважаючи на значні зрушення в інформаційно-інфраструктурній сфері нашої держави, цифровізації країни та впровадження нових технологій, на сьогодні велика кількість соціальних об’єктів, у тому числі навчальних закладів та медичних амбулаторій в невеликих населених пунктах залишаються без належного оснащення та без широкосмугового підключення до

мережі Інтернет. Таким чином, 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. Особливого загострення проблема набула в період пандемії COVID-19. Це ставить під сумнів належне забезпечення у державі одного з головних основоположних прав громадян – право на охорону здоров'я, а також допускає дискримінацію громадян за місцем проживання.

Іншою проблемою мешканців невеликих населених пунктів є 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 кількість дітей на сьогоднішній день позбавлена доступу до надбань національної та міжнародної спільнот та не мають 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 право на інформацію та знання, які необхідні для повноцінного та гармонійного розвитку дитини. Зважаючи на той факт, що інтелектуальний капітал – це основний капітал інформаційного суспільства, то така інформаційна нерівність може призвести до нового соціального розриву у майбутньому, коли частина громадян України не зможе себе повноцінно реалізувати в епоху нових технологій.

Наведені факти говорять про те, що в Україні все ще спостерігається таке явище як цифровий розрив, або інформаційна нерівність. Крім того, із лише двох зазначених проблемних аспектів стає зрозумілим, що недотримання прав в інформаційній сфері призводить до порушення функціонування інших важливих сфер життя суспільства, що тягне за собою порушення основоположних прав людини в Україні.

Не менш важливим є право людини на захист в інформаційній сфері. Загрози інформаційній безпеці сьогодні є суттєвими, постійно видозмінюються та посилюються. Якщо ще декілька років назад однією з основних проблем інформаційної безпеки в соціальних мережах вважався неконтрольований обіг особистої інформації громадян, розміщеною ними власноруч, то сьогодні слід говорити про масовий збір інформації про користувача в мережі на основі спостережень за його діяльністю. Такий збір інформації є частиною функцій адміністрування мережі. Автоматично зібрана інформація про користувача, або великі дані (BIG DATA), стає цінним товаром, ф'ючерсом на ринку, як раніше були сировина чи енергоносії, а компанії які володіють такою інформацією (Facebook, Instagram, Google і т.д.) очолюють списки найдорожчих компаній світу. Ця інформація використовується в комерційних цілях та стає надзвичайно цінним ресурсом знань для будь-якої компанії, у тому числі й для створення персоналізованої (таргетованої) реклами. З іншого боку великі дані (BIG DATA) є незамінним інструментом у політичній сфері, яка нині активно використовує сучасні інформаційні технології. Політичні перегони сьогодні перетворюються на інформаційні війни, а політична реклама від головної мети інформування виборця переходить до маніпулювання з інформацією та його свідомістю. Це збільшує об'єми недостовірної, фейкової інформації в інформаційному просторі, підвищує кількість негативних та маніпулятивних впливів на свідомість громадян, що порушує його право на захист від маніпулювання свідомістю та від недостовірної (фейкової) інформації.

Крім того, у бажанні взяти верх над конкурентом в процесі політичних перегонів знищується довіра та повага до державних інституцій, що порушує цілісність усієї системи, призводить до трансформації поглядів і цінностей у суспільстві та становить загрозу повноцінному функціонуванню і гармонійному розвитку нашої держави.

Це далеко не повний перелік загроз, які виникають в умовах соціальних та цифрових трансформації сучасного інформаційного суспільства в Україні. Проте навіть окремі аспекти проблемних

питань таких перетворень викликають занепокоєння та підтверджують необхідність проведення ґрунтовного аналізу цих трансформацій, характерних для сучасного стану розвитку суспільства, та розроблення методів протидії загрозам, які їх супроводжують. Це є необхідною умовою для того, щоб громадяни України могли повноцінно реалізовувати свої права у будь-якій сфері та бути конкурентноздатними в сучасному інформаційному світі.

Гуменюк І.О.

кандидат юридичних наук, старший
науковий співробітник, завідувач
сектором Інституту законодавства ВРУ

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ВИКОРИСТАННЯ ІТ У СФЕРІ СОЦІАЛЬНОГО ЗАХИСТУ: ОКРЕМІ АСПЕКТИ

Розвиток інформаційно-комунікаційних технологій змінює засоби взаємодії основних суб'єктів суспільних відносин у сфері соціального захисту. Таке становище обумовлене збільшенням інформаційних потоків та процесами цифрової трансформації життєдіяльності кожної людини – адресата соціальних прав.

Правові передумови для використання інформаційно-комунікаційних технологій у соціальній сфері були передбачені у галузевому законодавстві ще наприкінці 90-х років минулого століття. Запровадження страхового стажу як юридичного факту – обов'язкової умови для призначення різних видів соціального забезпечення в рамках соціального страхування, а також для встановлення розміру цих виплат, вимагало організацію та ведення персоналізованого обліку [1].

Розвиток можливості інформаційних технологій обумовив генезу самого поняття «персоналізований облік», його змістовного розуміння та правового регулювання. Здійснення персоналізованого обліку за допомогою ІТ змінило систему гарантій соціально-захисних прав в соціальному страхуванні, особливо права на пенсію. Завдяки інформаційним технологіям забезпечено процес

переходу від загальної інформації (даних) про сплату страхових внесків та зарахування цих періодів до страхового стажу, до персоніфікованого обліку у загальнообов'язковому державному соціальному страхуванні за всіма його видами.

Система соціального забезпечення України є ширшою за систему соціального страхування. Вона охоплює різні види соціальних допомог, в тому числі і соціальні послуги. Використання інформаційних технологій у сфері надання соціальних послуг особам і сім'ям, які перебувають у складних життєвих обставинах; дозволяє максимально забезпечити дотримання принципу адресності; підвищити якість соціальних послуг, скоординувати діяльності місцевих органів влади, надавачів соціальних послуг (фізичних та юридичних осіб) і отримувачів соціальних послуг щодо профілактики складних життєвих обставин, подолання або мінімізацію їх негативних наслідків. Реєстр надавачів та отримувачів соціальних послуг – це автоматизована інформаційно-телекомунікаційна система, призначена для збирання, реєстрації, накопичення, зберігання, використання, знеособлення і знищення інформації, необхідної для здійснення діяльності щодо надання соціальних послуг, які б задовольнили індивідуальні потреби отримувачів соціальних послуг відповідно до віку, статі, стану здоров'я, особливостей інтелектуального та фізичного розвитку, життєвого досвіду, родинної, культурної, етнічної та іншої належності, потреб та інтересів дітей, осіб з інвалідністю, осіб, визнаних недієздатними, осіб, цивільна дієздатність яких обмежена, осіб похилого віку, а також з урахуванням думки отримувачів соціальних послуг, якщо вони за віком, рівнем розвитку та станом здоров'я можуть її висловити.

Успішним прикладом застосування ІТ у механізмі забезпечення реалізації пенсійних прав громадян стало створення у територіальних відділеннях Пенсійного фонду України інформаційних кіосків для доступу громадян до відомостей, які зберігаються в Інформаційному центрі персоніфікованого обліку Пенсійного фонду України, запровадження нової системи обслуговування громадян та обробки пенсійної документації на базі централізованих

інформаційних технологій, створення web-порталу електронних послуг Пенсійного фонду.

На сьогоднішній день, у своїй діяльності державні органи, до повноваження яких віднесено здійснення заходів щодо соціального захисту населення, можуть використовувати автоматизовані інформаційні системи: *«Наша сім'я»* для обліку на місцевому рівні соціального стану багатодітних та малозабезпечених сімей, осіб з інвалідністю та їх сімей, одиноких непрацездатних та малозабезпечених громадян для організації соціальної допомоги; *«Єдиний державний реєстр осіб, які мають право на пільги»* для обліку осіб, які мають право на пільги за соціальною ознакою [2] згідно із Законами України. Розроблені для використання програмні комплекси: *«Житлові субсидії»* для автоматизації процесів призначення, перерахунку житлових субсидій, формування звітності у відповідності до чинних законодавчих та нормативних актів України; *«Статистичний моніторинг бідності»*, що забезпечує оброблення регламентних запитів Мінсоцполітики до баз даних регіонального (обласні управління соціального захисту населення) та районного рівнів та формування звітів [3].

Законодавчого врегулювання потребує здійснення постійного моніторингу реальної нужденності осіб в рамках соціальної допомоги та організації інформаційно-аналітичної бази щодо цільового використання соціальних коштів на місцевому рівні. Суттєвим кроком у цьому напрямку є реалізація положень Закону України «Про верифікацію та моніторинг державних виплат». Верифікація – це комплекс заходів щодо збору та перевірки достовірності інформації, що визначена законодавством для призначення, нарахування та/або здійснення державних виплат (пенсії, допомоги, пільги, субсидії, соціальні стипендії та ін.) і, яка впливає на визначення права на отримання та розмір таких виплат, а також виявлення невідповідності даних у автоматизованих інформаційних системах, реєстрах, базах даних [4]. Верифікація державних виплат здійснюється в інформаційно-аналітичній платформі, за кожним реципієнтом з подальшим визначенням відповідності інформації вимогам, визначених законодавством про соціальний

захист. Доцільним, на наш погляд, є врегулювання організаційно-правових засад порядку здійснення контролю за використання коштів отримувачами соціальної допомоги за окремими його видами, що мають цільове призначення (допомога по нагляду за дитиною, монетизовані житлові субсидії та ін.). Застосування ІКТ у вищезазначених заходах є визначальним.

На стан правової регламентації використання засобів інформаційно-комунікаційних технологій у сфері соціального захисту впливає розвиток загального законодавства про інформацію та її захист. Вказаний аспект має суттєве значення, оскільки належне правове регулювання питань доступу до інформації, захисту персональних даних, вимог до електронних документів та електронного документообігу дозволяє забезпечити взаємодію між центральним органом виконавчої влади, що реалізує державну податкову політику, державну політику з адміністрування єдиного внеску на загальнообов'язкове державне соціальне страхування, та Пенсійним фондом, що ведуть Державний реєстр, та фондами загальнообов'язкового державного соціального страхування, органами виконавчої влади, що здійснюють державними соціальну політику щодо обміну інформацією з питань соціального захисту на безоплатній основі.

Іншим не менш важливим аспектом використання ІТ, який слід зазначити, це реальна можливість підвищити ефективність боротьби з несвоєчасною сплатою єдиного соціального внеску, а також подолання проблеми застосуванням праці неоформлених належним чином працівників (тіньова зайнятість).

Використання інформаційних технологій складний соціальний процес. Він потребує значних зусиль організаційного та економічного характеру для задоволення потреб і забезпечення реалізації прав людини [5]. У сфері соціального захисту він ускладнюється не тільки особливістю та широким колом суб'єктивного складу соціально-забезпечувальних відносин, а й обсягом прав, які передбачені законодавством України про соціальний захист. У зв'язку з цим, ідея створення єдиного інформаційного простору у соціальній сфері, то б то, сукупності баз та банків даних, техноло-

гій їх ведення і використання, інформаційно-телекомунікаційних систем та мереж, що забезпечують інформаційну взаємодію всіх суб'єктів, яка тривалий час дискутується у науковому колі, стає все більш актуальною.

Самі інформаційні технології потребують відповідної підготовки, ефективної праці співробітників органів соціального захисту, фондів соціального страхування, зайнятих обробкою та зберіганням інформації, значних початкових витрат і наукомісткої техніки, розробки нових методів організації та взаємодії набувачів соціальних благ і суб'єктів, зобов'язаних їх надавати. Питанню застосуванню у професійній діяльності соціальних працівників ІКТ, розуміння можливостей і переваг використання комп'ютерних технологій присвячено багато наукових праць. Слід погодитись з аргументами фахівців щодо переваг ІКТ у соціальній сфері під час надання допомоги особам, які опинилися у складній життєвій ситуації; з необхідністю створення спеціалізованих інтернет-ресурсів, оскільки розміщення достовірної інформації на подібних ресурсах буде корисною як для спеціалістів, так і для осіб, які потребують консультативної допомоги; поширення у суспільстві знань і формування навичок із профілактики соціально небезпечного становища та самодопомоги і взаємодопомоги [6], то б то тих аспектів, забезпечення яких виключно у правовий спосіб не дає бажаного ефекту.

Список використаних джерел.

1. Основи законодавства України про загальнообов'язкове державне соціальне страхування: Закон України від 14 січня 1998 року. *Відомості Верховної Ради України*. 1998. №23. Ст. 121
2. Про Єдиний державний автоматизований реєстр осіб, які мають право на пільги: Постанова Кабінету Міністрів України від 29 січня 2003 р. № 117 (в редакції від 21.05.2020 р.) URL: <http://www.zakon.rada.gov.ua>
3. Продукти Інформаційно-обчислювального центру. URL: <http://www.mlsp.gov.ua/labour/control/uk/publish/>
4. Про верифікацію та моніторинг державних виплат: Закон України від 3 грудня 2019 року № 324-IX. URL: <http://www.zakon.rada.gov.ua>

5. Пожуєв В.І. Розвиток концептуальних засад інформатизації сучасного українського суспільства. *Гуманітарний вісник ЗДІА*. 2010. Випуск 41. С. 4-17

6. Дітковська Л.А. Місце інформаційно-комунікаційних технологій у професійній діяльності соціальних працівників. *Збірник наукових праць Хмельницького інституту соціальних технологій Університету «Україна»*. 2013. № 2(8). С.78-82

Дранник В.А.

викладач КПП ім. Ігоря Сікорського

ЩОДО ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СОЦІАЛЬНОЇ СФЕРИ

Сьогодні дедалі актуальнішим стає питання трансформації соціальної сфери для роботи в умовах соціальної та цифрової інформатизації. Якісна та ефективна підготовка соціальної сфери для роботи в умовах нових трансформаційних процесів, повинно бути одним із головних пріоритетів будь-якої держави.

В цій сфері основоположним є розпорядження кабінету міністрів України від 28 жовтня 2020 року «Про схвалення Стратегії цифрової трансформації соціальної сфери». В цьому документі визначено основні напрями та важливі завдання цифрової трансформації соціальної сфери, а саме системи соціального захисту громадян України на основі єдиних стандартів.

Розвиток цифрової трансформації соціальної сфери повинен підвищити ефективність соціального захисту населення. Для найбільш вразливих верств населення дуже важливо, щоб соціальний захист громадян відбувався ефективно і скоординовано.

В Єдиному соціальному реєстрі буде акумулюватися уся інформація про громадян, які отримують соціальну допомогу. Все буде знаходитись в одному місці і це полегшить роботу працівників соціальної сфери, а також, заощадить час отримувачам допомоги в зборі всіляких документів. Тому, що в багатьох випадках, куди б людина не звернулася, вона повинна заповнювати стоси паперів, долати бюрократичні перешкоди щодо заповнення, отримання документів або

послуг. Наявність автоматизованих сервісів не тільки зробить роботу ефективнішою, а й знизить корупційну складову. Впровадження електронного документообігу знизить помилки людського фактору.

Треба наголосити, що запровадження цифрової трансформації соціальної сфери несе в собі такі зміни:

- автоматизована система контролю і управління;
- електронний документообіг;
- ефективний соціальний захист громадян;
- захист персональних даних громадян;
- існування єдиної інформаційної бази соціальної сфери;
- контроль фінансових надходжень у соціальній сфері;
- підвищення ефективності якості обслуговування у соціальній сфері;
- подолання бюрократичної складової у соціальній сфері;
- подолання дублювання процесів, пов'язаних із соціальним захистом;
- скорочення працівників установ соціального захисту.

Таким чином, цифрова трансформація соціальної сфери дуже важлива для громадян України сьогодні і її впровадження несе в собі більше позитивні моменти. Дуже важливо, що уряд вбачає в цьому один із головних пріоритетів вдосконалення соціальної сфери тому, що завданням будь-якої держави є законодавчо і практично підтримувати громадян, які потребують допомоги.

Щодо скорочення працівників установ соціального захисту, то виникає питання: якщо відбувається глобальна соціальна та цифрова трансформація внаслідок якої скорочують працівників, то де вони згодом будуть працювати?

І, якщо увесь документообіг перейде у цифрову форму, то, що робити у випадках цифрових атак і, як захистити данні від хакерських атак чи збою системи?

Подальші напрями розвитку цієї теми можуть бути направлені на усунення недоліків, які несе в собі цифрова трансформація соціальної сфери.

Також, треба пам'ятати про важливість громадських обговорень нових введень у цій сфері.

Капіца Ю.М.

доктор юридичних наук, директор
Центру досліджень інтелектуальної
власності та трансферу технологій
НАН України

ПИТАННЯ ІМПЛЕМЕНТАЦІЇ ДИРЕКТИВИ 2019/790 ПРО АВТОРСЬКЕ ПРАВО В ЄДИНОМУ ЦИФРОВОМУ РИНКУ В ЄВРОПЕЙСЬКОМУ СОЮЗІ

Директива 2019/790 про авторське право в єдиному цифровому ринку в ЄС, ухвалена 17.04.2019, стосується низки актуальних питань розвитку цифровому ринку: діяльність провайдерів он-лайн послуг та захист авторського права у мережі Інтернет; нові права видавців; виплата винагороди авторам та виконавцям; використання творів, що знаходяться поза комерційним обігом; аналізування даних та тексту в цілях наукових досліджень, використання творів у цифровій навчальній діяльності; діяльності бібліотек та архівів тощо.

Відсутність консенсусу при прийнятті директиви призвело до викладення її більш як концептуального документу з відсутністю механізмів реалізації та перекладення невіршених питань на майбутню практику Суду ЄС та практику імплементації директиви державами-членами ЄС. Аналіз директиви здійснено нами у ряді публікацій з загальним висновком доцільності перед адаптацією її положень в Україні очікування вироблення в ЄС однакової практики імплементації [1]. З урахуванням більш ніж півтора року з моменту ухвалення директиви у цій публікації досліджується стан та основні проблеми імплементації директиви 2019/790 в ЄС.

На 18.11.2020 з 27 держав-членів ЄС окремі положення директиви були імplementовані лише у Франції (ст. 15, право видавців, 23.07.2019, LOI n° 2019-775 du 24.07.2019). Положення з застосування у Франції норм ст. 17–22 щодо вплати винагороди та захисту прав у мережі Інтернет (без деталізації механізму застосування) ухвалені 17-18.11.2020 Сенатом та Національною асамблеєю. У Нідерландах акт, що стосується ряду статей директиви схвалено

Палатою представників 17.11.2020 та передано до Сенату. Інші держави члени ЄС знаходяться на стадії консультацій або підготовки (обговорення) законопроектів. Кінцевий термін імплементації директиви у законодавстві держав-членів ЄС, визначений ст. 29 директиви, – 7.07.2021.

Найбільш дискусійними при імплементації директиви з'явилися ст. 15 щодо прав видавців та ст. 17 стосовно захисту авторського права у мережі Інтернет. В Україні особливий інтерес викликають підходи до імплементації ст. 18–22 стосовно виплати належної винагороди авторам та виконавцям, у тому числі з врахуванням використання їх творів у мережі Інтернет.

Щодо ст. 17 зазначимо, що недосконалість норм директиви, що стосуються захисту прав ІВ у мережі Інтернет, призвело ще на стадії прийняття директиви до включення до статті положення про зобов'язання Європейської комісії організувати діалог із зацікавленими сторонами для обговорення найкращих практик співпраці між постачальниками послуг з обміну контентом в Інтернеті та особами, яким належать права інтелектуальної власності, та підготувати Керівництво з застосування цієї статті. Комісія мала намір опублікувати Керівництво у першій половині 2020 року. Незважаючи на 6 проведених обговорень та оприлюднення консультаційного документу на грудень 2020 р. Керівництво не було підготовлено [2].

Істотним, що стосується як Закону Франції № 2019-775 від 24.07.2019, так і зазначеного вище законопроекту Нідерландів, – в них не визначено кількість слів або іншим чином не визначено, що має розумітися під «дуже короткими витягами з публікацій преси» (част. 1 ст. 15 директиви). Саме перевищення обсягу «дуже коротких витягів» має наслідком застосування норм директиви з зобов'язань із сплати винагороди видавцям з боку провайдерів інформаційних послуг. Таким чином держави-члени ЄС не взяли на себе визначення у законі допустимої кількості слів з перекладанням вирішення цього питання на Суд ЄС.

Стосовно ст. 18-22 щодо виплати винагороди авторам та виконавцям; зобов'язань набувачів прав повідомляти про дохід від

використання творів, а також виплати додаткової винагороди при непропорційно низькій узгодженій винагороди порівняно з наступними доходами, зазначимо рекомендації Європейського товариства з авторських прав 2020 р. [3]. Рекомендації відзначають, що:

- зобов'язання директиви з виплати винагороди є обов'язкові та не можуть бути змінені контрактом. Положення ст. 18-22 як принципи мають застосовуватися для діючих контрактів;
- звертається увага на доцільність укладання колективних договорів, прийняття секторальних кодексів практики, стандартних умов щодо виплати винагороди;
- отримання авторами належної та пропорційної винагороди передбачає періодичні виплати за використання творів. Заміна періодичних виплат разовою фіксованою сумою може мати місце лише у обмежених та визначених випадках.

Слід вказати на корисні напрацювання деяких держав-членів щодо визначення у законопроектах особливостей та механізмів застосування окремих статей директиви. Так, в Італії у проекті Закону щодо імплементації директив ЄС (Disegno di Legge N.1721, 14.02.2020) зазначається, які додаткові уточнення та механізми мають бути запроваджені для ефективної імплементації директиви на національному рівні. Вказане стосується, зокрема, уточнення критеріїв віднесення твору до таких, що є поза комерційного обігу (ст. 8(5)); дій, якщо твір поза комерційного обігу є також сирітським твором (ст. 8); визначення поняття «дуже короткі витяги», щоб не створювати перешкод вільному руху інформації; визначення частки доходу, які отримують видавці від використання видань он-лайн, що мають отримувати автори (ст. 17(4)); визначення процедур взаємовідносин он-лайн провайдерів та користувачів щодо захисту авторського права та суміжних прав (ст. 17(9)); визначення процедур зміни контрактів стосовно виплати винагороди, відкликання прав (ст. 20–22) тощо.

В цілому зазначимо, що на цей час в державах-членах ЄС відсутній досвід імплементації та застосування положень директиви 2019/790. Деякі прийняті та розроблені акти переважно сто-

суються окремих статей директиви. Певний досвід застосування ст. 15 директиви щодо прав видавців наявний лише у Франції [4]. Разом з тим урядами, парламентськими комісіями нараблено цінний досвід з визначення питань, які мають бути врегульовані при імplementації директиви. Також організаціями, які представляють різні групи авторів, виконавців та набувачів прав інтелектуальної власності, підготовлені рекомендації, керівництва з застосування положень директиви, які варто взяти до уваги.

З врахуванням важливості положень директиви для вдосконалення законодавства України та розвитку цифрового ринку актуальним є відстеження наробок держав-членів ЄС з розробки законодавчих актів та порівняння їх між собою, дослідження практики застосування, що дозволить більш виважено підійти до імplementації положень директиви 2019/790 у право України.

Література

1. Капіца Ю.М. Директива ЄС про авторське право в єдиному цифровому ринку: нові виміри чи нові випробування? Інтелектуальна власність. № 8, 2019. С. 6–22.

2. Directive on Copyright in the Digital Single Market: Commission seeks the views of participants to the stakeholder dialogue on Article 17. European commission. 27.07.2020. URL: <https://ec.europa.eu>

3. Comment of the European Copyright Society addressing selected aspects of the implementation of articles 18 to 22 of the Directive (EU) 2019/790 on Copyright in the Digital Single Market. 8 June 2020. URL: <https://europeancopyrightsociety.org/opinions/>

4. Google reaches agreement with some of the French publishers. 19 November 2020: URL: <https://france.googleblog.com/2020/11/-droits-voisins.html>

Муханов В.М.

кандидат історичних наук, старший
викладач Вінницького державного
педагогічного університету імені
Михайла Коцюбинського

Голюк М.В

студентка Вінницького державного
педагогічного університету імені
Михайла Коцюбинського

ПОРУШЕННЯ АВТОРСЬКИХ ПРАВ У МЕРЕЖІ ІНТЕРНЕТ

Важливою умовою формування позитивного іміджу будь-якої країни є забезпечення належного рівня захисту інтелектуальної власності. На даний час спостерігається швидкий та невпинний розвиток інформаційних технологій, особливо глобальної Інтернет-мережі, що стало причиною збільшення кількості правопорушень пов'язаних з використанням об'єктів авторських прав.

Найбільш розповсюдженим порушенням авторського права у наш час є незаконне використання творів та їх незаконне розповсюдження, тобто без згоди автора. Прикладом даного правопорушення є розміщення наукових робіт без згоди автора (або авторів) на Інтернет-сайтах, де даною роботою може скористатися кожен хто має доступ до мережі, оприлюднення творів у громадських закладах за плату або ж завантаження роботи в пам'ять мобільного телефону, планшета, ноутбука [2, с 117].

Викладення роботи без дозволу, тобто недотримання авторських прав в будь-якій соціальній мережі або на різних сайтах виражається насамперед в незаконному відтворенні та копіюванні будь-яких музичних, художніх, літературних, наукових робіт чи навіть комп'ютерних програм без попереднього надання дозволу автора [4, с 5].

Порушенням авторського права у мережі Інтернет є плагіат, що широко розповсюджене на території не лише України але й інших країн. Особливо даний вид правопорушення є популярним

явищем серед наукових робіт і досить часто має вигляд немотивованого відтворення. Виділяють академічний, тобто оприлюднення наукових результатів іншої людини під власним прізвиськом, що вважається академічною не доброчесністю. Самоплагіат: оприлюднення власних наукових результатів у якості нових [2 с 118]. Термін кіберплагіат вживається давно і певною мірою двояко, тобто запозичення праць інших авторів, без їхнього дозволу, із використанням Інтернет технологій, тут мається на увазі загальне використання Інтернету для власних цілей, тобто копіювання тексту, створення однієї роботи із маленьких шматочків різних наукових робіт [3, с 142].

Окремим видом неправомірної діяльності серед об'єктів авторського права є Інтернет – піратство. Термін означає порушення прав інтелектуальної власності. Суть даного правопорушення полягає у відтворенні та розповсюдженні мережею фільмів, музичних композицій, комп'ютерних програм та інших об'єктів без дозволу автора. Наразі із піратством намагаються боротися у кожній країні світу. Основними видами Інтернет-піратства є: аудіо піратство – копіювання та розповсюдження копій музичних композицій, також виділяють відео піратство тобто розповсюдження та копіювання відео, фільмів. Досить розповсюдженим є піратство літературних творів розповсюдження авторських творів без згоди автора, тобто незаконне. Піратство комп'ютерних ігор, також користується популярністю як в Україні так і закордоном. В Україні даний термін був використаний уперше в Законі України «Про авторське право і суміжні права» там же згадується термін «плагіат» [1, с 64] .

Власники онлайн платформ на яких було розміщено ту чи іншу статтю мають насамперед значний перелік зобов'язань щодо авторів та правовласників, законодавство України містить низку ефективних норм щодо способів захисту авторського права [5, с 128-129].

Держава вживає певні заходи щодо інформування користувачів мережі Інтернет про недопустимість порушення авторських прав, контролювати порядок розміщення твору [6, с 88]. Тягар захисту

авторських прав, часто лежить, як правило, на самому автору, тому вони, перш ніж розміщувати твір на різних сайтах, мусять вживати певні додаткові дії із захисту авторських прав. Виявлене конкретне порушення авторських прав передбачає конкретні дії із захисту прав автора [7, с 368].

Непідготовленість державних службовців у сфері захисту прав автора, також створює проблему у боротьбі з плагіатом, кіберпіратством. Низький рівень підготовки, відсутність досвіду і знань у цій сфері викликають недовіру у суспільства. Це є величезною проблемою, адже право інтелектуальної власності заповнило кожен сферу людського життя, воно присутнє повсюди. Особливо це помічається в Інтернет ресурсах, адже весь контент складається із авторського права [8, с 3-12].

Отже, порушенням авторських прав в мережі Інтернет можна вважати будь-які прямі чи непрямі дії особи, спрямовані на порушення прав та інтересів суб'єктів авторського права. Основними видами порушення прав автора є, піратство та плагіат, останній є більш розповсюдженим серед наукових робіт. Основними видами плагіату є кіберплагіат та само плагіат, у першому це використання Інтернет сайтів з власної вигоди, тобто копіювання робіт інших авторів, і створення з маленьких частин однієї повної роботи, само плагіат навпаки означає використання власних дослідження проте в іншій роботі.

Список використаних джерел

1. Про авторське право і суміжні права: закон України від 23.12.1993 р. // Відомості Верховної Ради України (ВВР). – 1994. – N 13. – ст. 64.
2. Кирилюк А. В. Правопорушення авторських прав у мережі інтернет: поняття та види / А. В. Кирилюк. – С. 117–120.
3. Рижко О. Поняття, види, класифікації плагіату / О. Рижко. – 2016. – С. 134–150.
4. Орлова А.В. Проблеми захисту авторського права в Україні / А.В. Орлова, Л.В. Первалова. Вісник НТУ «ХПІ». 2014. № 37(1080). С. 4–8.
5. Кирилюк А.В. Проблеми захисту авторських прав в мережі Інтернет. Часопис цивілістики. 2014. № 16. С. 126–130

6. Жаров В.О. Захист права інтелектуальної власності в Україні : навчальний посібник. Київ : Інст. інт. власн. і права, 2005.

7. Шишка Р.Б. Охорона права інтелектуальної власності: авторсько-правовий аспект : моногр. / Р.Б. Шишка – Х. : Видавництво НУВС. – 2002. – 368 с.

8. Штефан А.О. Дещо до питання про порушення у сфері авторського права / А.О. Штефан // Теорія і практика інтелектуальної власності. – 2009. – №6. – С.3-12.

Войтко А.А.

студентка КПП ім. Ігоря Сікорського

Науковий керівник: **Дубняк М.В.**

к.ю.н. старший викладач КПП ім. Ігоря Сікорського

РИЗИКИ ПОРУШЕННЯ ПРАВА НА НЕ ВТРУЧАННЯ В ОСОБИСТЕ ЖИТТЯ ПРИ ВИКОРИСТАННІ ДАНИХ СОЦІАЛЬНИХ МЕРЕЖ

Уявити сучасний світ без соціальних мереж стає дедалі складніше або й практично неможливо, це свідчить про те, що мережа Інтернет стала частиною нашого життя, його невід’ємною складовою. Понад мільярд людей активно використовують прямі мобільні платформи обміну повідомленнями, зокрема WhatsApp, Instagram, Facebook Messenger, Skype, Telegram. Наразі майже кожен має акаунт для доступу до сторінки в певну соціальну мережу. У звіті «Цифрові технології 2020» зазначено, що наймасовішою платформою є Facebook – у неї 2,449 млрд. активних користувачів на місяць. На другому місці YouTube (2 млрд.), на третьому – WhatsApp (1,6 млрд). На четвертому – TikTok (800 млн.) [1].

У зв’язку із збільшенням кількості користувачів та часу використання таких сервісів доцільно дослідити: ризики використання даних, які порушують право на не втручання в особисте і сімейне життя; міжнародний досвід протидії злочинам, які скоєні за допомогою використання даних з соціальних мереж; сформулювати

перелік ефективних заходів, для протидії порушенню права на невтручання в особисте життя.

Соціальна мережа – інтернет-співтовариство користувачів, об'єднаних за будь-якою ознакою на базі одного сайту [2]. Кожна із сторінок користувача – легкодоступний архів його персональних даних. Аналізуючи загрози для користувачів соціальних мереж, необхідно зазначити, що дані, які там розміщено можуть активно використовуватися з протиправною метою.

7. Як засіб та місце вчинення злочину, наприклад, гра під назвою «Синій кит», яка поширювалась серед користувачів соціальної мережі Вконтакте. Це історія про серію самогубств серед підлітків вчинених під впливом стороннього навіювання та заохочення. Умовами доступу до гри було виконання ряду завдань, в основному пов'язаними із нанесенням користувачем собі тілесних ушкоджень.

8. Як знаряддя вчинення злочинів, наприклад, дані громадян України, які були у додатку «Дія» (електронне посвідчення водія, паспортні дані), були розповсюджені та перебували у відкритому доступі на Telegram-каналі.

У політиках використання даних соціальних мереж визначено, які обсяги даних збираються та з якою метою. Наприклад, політика використання даних Instagram стверджує: «Ми збираємо контент, повідомлення та іншу інформацію, яку ви надаєте нам під час використання наших Продуктів, зокрема, коли ви реєструєте обліковий запис, створюєте або поширюєте контент або повідомлення, коли спілкуєтесь з іншими користувачами. Сюди може входити інформація про контент, який ви публікуєте (така як метадані), наприклад місце, де зроблено фотографію, або дата, коли було створено файл. Така інформація також може включати в себе те, що ви бачите завдяки наданим вам функціям, таким як, наприклад, наша камера, за допомогою чого ми можемо запропонувати вам маски та фільтри, які вам можуть сподобатися, або надати вам підказки щодо того, як використовувати формати камери» [3].

Враховуючи обсяг даних, які збираються про кожного користувача можемо відзначити ризики та сфери їх протиправного використання:

1. відкрите поширення конфіденційної інформації;
2. можливість зіткнутися з неналежним контентом (насильство, образи, тощо);
3. ймовірність використання особистої інформації третіми особами з метою отримання вигоди;
4. умисне створення негативного іміджу певної особи іншими учасниками спільноти (кібербулінг) [4].

Варто звернути увагу, що в протиправних цілях можуть бути використані дані із соціальних мереж які, на перший погляд, не є важливими. Наприклад, користувач публікує допис про перебування на відпочинку який може супроводжуватися світлиною з геолокацією його місцязнаходження, цими даними можуть скористатися зловмисники при вчиненні квартирної крадіжки.

Хоча Конституція України гарантує, що ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [5]. А Закон України «Про захист персональних даних» регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних» [6]. Однак, наявність такого правового регулювання не мінімізує ризиків порушення права на не втручання в особисте життя при використанні даних соціальних мереж. У зв'язку з цим далі необхідно навести аналіз міжнародного досвіду, щодо ефективних заходів протидії втручання в право на недоторканість особистого і сімейного життя.

Міжнародною асоціацією керівників поліції розроблено рекомендації щодо використання соціальних мереж з метою запобігання злочинності, в яких вказується напрями цієї роботи шляхом безпосереднього розміщення в соціальних мережах інформації щодо запобігання злочинності; розробка блогів та організація ча-

тів з цієї тематики; створення цифрових медіа-файлів, наприклад, у вигляді лекцій; розповсюдження в соціальних мережах інформації щодо різноманітних заходів із запобігання злочинності [7]. Тобто збільшувати поінформованість суспільства про ймовірні злочинні дії та способи протидії їм. Таким чином, держава підвищує правову свідомість громадян.

У доповіді американського аналітичного центру RAND (Research and Development) зазначено, що аналіз соціальних мереж має великий потенціал використання в інформаційних операціях американськими військовими, оскільки дозволяє провести дослідження, яке стосується ставлення, світогляду та спілкування широкого кола осіб. Наприклад, контент-аналіз може бути використаний для пошуку осіб в процесі радикалізації, оцінити ступінь підтримки екстремістських поглядів у певній групі. Завдяки аналізу мереж можливо або сприяти, або навпаки, протидіяти, поширенню окремих ідей або інформації [8, с.111].

Прикладом участі громадських організацій у пошуку в мережі Інтернет контенту, який може нести загрозу для молоді та підлягає кримінальному переслідуванню, може слугувати німецька організація із захисту молоді (jugendschutz.net.), що фінансується всіма федеральними землями Німеччини.

Якщо інспектори цієї організації знаходять протиправний контент, вони намагаються зробити так, щоб його видалили. У 2011 р., за підрахунками та з ініціативи jugendschutz.net, понад 970 разів було видалено неонацистські матеріали в різних соціальних мережах.

У Британії правоохоронці також використовують соціальні мережі як засіб зв'язків із громадськістю. Так, поліція графства Великий Манчестер створила обліковий запис мережі Twitter. У мікроблозі даного ресурсу публікують важливі повідомлення, кримінальні відомості, дані про осіб, оголошених у розшук. При цьому британські правоохоронці визнали важливу роль соціальних мереж у попередженні та розкритті злочинів і включили відповідний курс у програму підготовки молодих співробітників [9].

Сьогодні у багатьох країнах налагоджена система співробітництва, що обумовлюється необхідністю обміну досвідом на міжнародному рівні. Ці питання координуються кожною країною відповідно до розробленої та діючої стратегії кібербезпеки: США та більшість країн-учасниць ЄС у своїх стратегіях виносять питання боротьби з кіберзлочинністю на передові позиції. В ЄС створений необхідний нормативно-правовий фундамент з питань захисту кіберпростору. Особливістю стратегії кібербезпеки ЄС є те, що в цьому акті охоплено різні аспекти кіберпростору, зокрема, внутрішній ринок, правосуддя, внутрішня та зовнішня політика [10].

На основі вищевикладеного та проаналізувавши досвід зарубіжних країн можна дійти до висновку, що найоптимальнішими програмами для зменшення ризиків втручання в право на особисте і сімейне життя при використанні даних соціальних мереж є проведення власної інформаційної політики держави, яка буде виражатися у забезпеченні поінформованості громадян. На нашу думку, основною цільовою групою повинні стати школярі та підлітки, оскільки вони є найбільшою групою ризику.

Таким чином, доцільно було б проводити для них уроки-тренінги, запроваджувати навчальні програми та платформи навчально-ігрового формату з метою закріплення знань, проводити соціальні опитування. Ці заходи стануть превентивними способами запобігання поширення про себе даних, які можуть бути протиправно використані третіми особами та порушити право на не втручання в особисте і сімейне життя.

Список використаних джерел

1. Simon K. (2020) Digital 2020: global digital overview report URL: <https://datareportal.com/reports/digital-2020-global-digital-overview> (дата звернення: 05.12.2020)
2. SEO словник iGroup URL: <https://igroup.com.ua/seo-articles/sotsialna-merezha/>. (дата звернення: 05.12.2020)
3. Політиках використання даних Instagram URL: <https://www.facebook.com/help/instagram/833836199971426?helpref=related> (дата звернення: 05.12.2020)

4. Беркій Т.М. Соціальні мережі: різні аспекти впливу на людину. URL: http://ukrainepravo.com/legal_publications/essay-on-itlaw/it_law_berkiy_Soci_networks_and_there_involves/ (дата звернення: 05.12.2020)
5. Конституція України URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>. (дата звернення: 05.12.2020)
6. Закон України «Про захист персональних даних» URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.
7. Social Media and Crime Prevention URL: <https://www.nnw.org/publication/social-media-and-crimeprevention> (дата звернення: 05.12.2020)
8. Бугера О. І. Соціальні Інтернет-мережі та запобігання злочинності: сучасні тенденції. *Вісник НТУУ “КПІ” політологія, соціологія, право*. 2018. №2. С. 110–113.
9. Гавловський В. Д. Щодо використання соціальних мереж для виявлення, розкриття та попередження злочинів. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. № 2. С. 271-282
10. Youtsen M. Research on European Juvenile Delinquency // HEUNI Publication Series. 1987. № 7. С. 57-62

Ніжнік В.В

студент КПІ ім. Ігоря Сікорського
Науковий керівник: **Солончук І. В.**
старший викладач КПІ ім. Ігоря
Сікорського

МЕДІАЦІЯ В СУДОЧИНСТВІ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Всі люди між собою є різними за характером, думками, уподобаннями та почуттями, а тому який би спосіб життя людина не вела, вона все одно не зможе уникнути непорозуміння із оточуючими, тобто вони є невід’ємною складовою нашого спілкування і потребують врегулювання. Традиційною і наразі провідною формою вирішення спорів між людьми є звернення до суду. Але на сьогодні суспільство недостатньо ознайомлене із альтернативним методом вирішенням спору – медіацією. Актуальність дослідження даної теми обумовлена правовою неврегульованістю медіації

у законодавстві України, непоінформованістю населення, а також проблемами, які можуть виникнути у людей, які бажають звернутися до послуг медіатора.

Метою дослідження є висвітлення проблеми непоінформованості щодо інституту медіації серед населення України та проблем із зверненням громадян до послуг сфери медіації та пошуком медіатора шляхом використання мережі Інтернет.

Як вже зазначалося, один із способів вирішення спору, окрім, судового є медіація. Медіація – це переговорний процес, що здійснюється за допомогою незалежного нейтрального кваліфікованого посередника – медіатора, який допомагає сторонам спору проаналізувати конфліктну ситуацію таким чином, щоб вони змогли самостійно обрати той спосіб вирішення суперечки, що відповідатиме інтересам обох сторін [1, с.57]. А медіатор (посередник) – це незалежна, неупереджена фізична особа, яка проводить медіацію і не має повноважень щодо прийняття рішення по суті конфлікту(спору) [2].

На сьогоднішній день провідним способом вирішення конфліктів і спорів залишається саме звернення до суду, оскільки кожен знає про таке правило: якщо порушили твоє право – звертайся до суду. Але не кожен знає про медіацію, що це таке і для чого вона потрібна. Провівши опитування серед своїх знайомих та родичів, чи знають вони що таке медіація і для чого вона, ми одержали неоднозначні результати: ні один з опитаних не знає про медіацію і взагалі ніколи не чули такого поняття. На цій підставі цього можна зробити висновок, що у разі порушення, невизнання чи оспорювання їхніх прав вони звернуться до суду, а не до послуг медіатора. Причиною необізнаності про медіацію і про її існування в Україні є недостатня реклама медіації, як альтернативного способу вирішення спору. Внаслідок цього громадяни і далі продовжують звертатися до суду із приводу конфліктів, у той час як їхні проблеми можна було б простіше врегулювати шляхом медіації [3, с.261].

Проблема непоінформованості населення про медіацію, як одна із проблем медіації, була наведена суддею Полтавського

окружного адміністративного суду І. Г. Ясиновським ще у 2015 році. «У судах немає інформаційно-довідкових відділів або бюро з питань медіації, відповідальних за надання інформації широкій публіці. Окрім брошур про медіацію, випущених деякими неурядовими організаціями, інших інформаційно-реklamних матеріалів (плакатів, рекламних листків, різних звітів, інформаційних бюлетенів, відео) не існує», – зазначав у своїй статті І. Г. Ясиновський [3, с.262]. З 2015 року ситуація дещо змінилася: з'явилися сайти, де можна детальніше прочитати про процедуру медіацію та обрати собі медіатора, декілька відео про медіацію в Україні, два звіти від Української Академії Медіації та плакати, які вивішені в деяких державних установах. Але це та кількість, якої замало для того, аби популяризувати цю процедуру.

Медіація в Україні є і вона практикується, не дивлячись на те що, її законодавчого врегулювання досі не існує. У випадку, коли людина дізналася про процедуру медіації, то тепер перед нею стоять наступні питання: де знайти медіатора, який допоможе врегулювати конфлікт і яким чином до нього звернутися. Особа може скористатися послугами медіатора як до звернення до суду та під час провадження, так і на стадії виконання рішення суду [4].

На прикладі реєстру медіаторів дослідимо проблему пошуку медіатора. Для того, щоб звернутися до медіатора, особі необхідно у будь-якому пошуковому сервісі здійснити пошуковий запит реєстру медіаторів. Першим же посиланням буде реєстр медіаторів – членів НАМУ (Національної асоціації медіаторів України). На цьому сайті особа може здійснити пошук вже відомого їй медіатора, знаючи ім'я, прізвище та по-батькові або обрати медіатора за регіоном роботи, за сферою врегулювання конфлікту та за робочою мовою і обрати вподобаного. На сьогодні на вищезазначеному сайті представлено 172 кваліфікованих медіатори, які допоможуть врегулювати спір. Перейшовши на профіль вподобаного медіатора, можна написати йому безпосередньо, можна також переглянути, на яких справах він спеціалізується, його науковий ступінь, регіони, в яких він працює, мови, якими він володіє та його підготовку. У зв'язку із пандемією COVID-19 більшість ме-

діаторів перейшли в онлайн-формат, що буде безмежно зручно для людей, які обмежили свої контакти із оточуючим світом. Тому не дивуйтеся, якщо в графі регіон роботи зазначено «on-line».

У підсумку хотілося б зазначити, що медіація досі перебуває у стані розвитку і свого запровадження на території України. Однією із основних проблем медіації в судочинстві інформаційного суспільства є недостатня поширеність цієї процедури серед населення, в тому числі у мережі інтернет. Необізнаність громадян щодо медіації спричинена багатьма факторами, основним із яких є неприйняття Закону України «Про медіацію». На нашу думку, прийняття Закону допомогло б поширити процедуру мирного врегулювання спору серед населення шляхом банальної реклами у соціальних мережах, газетах, метро, рекламних щитах, тощо. Вважаємо, що ця функція може бути покладена на засоби масової інформації, громадські організації та державу.

Список використаної літератури:

1. Новосад А. С, Сойка Ю. Ю, Семенкова Н. І Проблематика медіації як альтернативної форми врегулювання спору за участю судді чи адвоката. Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. Том 30 (69), № 2, 2019. 5 с. URL: http://www.juris.vernadskyjournals.in.ua/journals/2019/2_2019/11.pdf (дата звернення: 07.12.2020).

2. Проект Закону України «Про медіацію»: Проект Закону України від 19 травня 2020 р. № 3504. База даних «Законодавство України»/ ВР України. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/JI02134A.html (дата звернення: 07.12.2020).

3. Ясинівський І. Г. Полтавський окружний адміністративний суд. Проблеми впровадження та проведення медіації в Україні. Актуальні проблеми політики. 2015. Вип. 55. 8 с. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/3250/%25D0%25AF%25D1%2581%25D0%25B8%25D0%25BD%25D0%25BE%25D0%25B2%25D1%2581%25D1%258C%25D0%25BA%25D0%25B8%25D0%25B9%2520APP_55-31.pdf?sequence=1&isAllowed=y (дата звернення: 07.12.2020).

4. Потьомкіна Ю. Медіація: інструкція з використання. URL: <https://thepage.ua/ua/experts/mediaciya-instrukciya-z-vikoristannya> (дата звернення: 08.12.2020).

Воронько М.А.

студентка КПП ім. Ігоря Сікорського

Науковий керівник: **Головко О.М.**

к.ю.н., ст. викладач КПП ім. Ігоря

Сікорського

КОНФІДЕНЦІЙНІСТЬ В ОНЛАЙН МЕДІАЦІЇ

Усвідомлення безпеки особистої інформації дозволяє клієнту говорити про свої проблеми вільно, що є вкрай важливим для виявлення справжніх потреб сторін. В умовах пандемії основним форматом роботи є онлайн формат, але практика проведення медіації показує, що забезпечення конфіденційності у такому форматі має проблеми реалізації.

Проблема недовіри людей до збереження даних у інтернет просторі частково полягає у некомпетентності учасників медіації щодо забезпечення інформаційної безпеки. Ми знаємо як захистити себе від підслуховування в реальному житті, проте ми не завжди знаємо як зробити це в мережі. Тому дуже важливо як надавачу медіаційної послуги, так і її споживачу мати високий рівень інформаційної культури. Проведення медіації в режимі відеоконференції може бути незвичним для сторін, до того ж, уміння працювати з програмами відеозв'язку напряду визначає можливість доступу особи до медіації та якості, своєчасності наданих нею коментарів при обговоренні проблем. Як зазначає Головко О. М., “цифрові компетенції – це уміння використовувати цифрові технології, ключову роль з яких надають цифровій грамотності” [1, с. 39].

Дійсно, в умовах сьогодення питанню інформаційної грамотності потрібно приділяти значну увагу, зокрема, задля створення умов надання послуг онлайн та їх юридичного визнання. Треба враховувати, що альтернативні процедури врегулювання спору спрощують життя як окремій людині, так і представникам судової влади, особливо в умовах пандемії. За даних умов у медіатора з'являються нові виклики, адже при проведенні онлайн медіації саме на нього покладається обов'язок забезпечення умов для на-

лежної роботи. Медіатор має приділяти увагу вміню сторін користуватися програмою, в якій він пропонує провести медіацію.

На сьогодні існує необхідність навчання інформаційній грамотності медіаторів або додаткове залучення спеціаліста з електронних комунікацій, створення онлайн курсів чи коротких відео-презентацій для ознайомлення сторін з важливими питаннями роботи з платформами онлайн зв'язку.

Лише через залучення експертів, які можуть надати сторонам висновок щодо рівня інформаційної безпеки майбутньої відеоконференції та інформацію щодо специфіки користування функціоналом програм, можна подолати бар'єр небажання людей переходити у онлайн медіацію. На підготовчому етапі дистанційної медіації медіатор обов'язково повинен дізнатися чи вміють сторони користуватись обраною програмою. У разі, якщо ні – він зобов'язаний ознайомити їх з цим персонально, через надання доступу до відповідних інформаційних ресурсів або запросити для цього спеціаліста. У разі побоювань сторони щодо безпечності збереження даних медіатор має роз'яснити, чому режим роботи, який він використовує є безпечним та відповісти на запитання. Лише таким чином, коли не залишиться відкритих питань або незрозумілих моментів щодо формату проведення процедури, можна досягти сприятливих умов для вільної побудови діалогу. Окрім цього, виключно сторони при узгодженні між собою мають можливість визначити чи буде інформація з медіаційної процедури конфіденційною або публічною, окрім випадків, встановлених законом [2, с. 133].

З іншого боку, причини недовіри виникають не безпідставно, тому що реальна загроза викрадення особистих даних насправді існує. Це напряму пов'язано з дотриманням принципу конфіденційності медіації, оскільки як медіатор, так і сторони мають докладати зусилля для підтримки безпечного середовища під час медіаційної процедури. Вирішенням даної проблеми може бути лише ретельний відбір програм, що надають послуги відеозв'язку за визначеними критеріями, які направлені на забезпечення інформаційної безпеки як сторін медіаційної процедури, так і медіато-

ра. Окрім цього, медіатори мають бути обізнані з базових правил запобігання порушенню конфіденційності та мати швидку технічну підтримку у разі виникнення складнощів.

Другою проблемою, ймовірність настання якої не менше відштовхує людей від онлайн медіації – це вірогідність порушення принципу конфіденційності другою стороною, або самим медіатором. При проведенні онлайн медіації людина обмежена у можливості візуального сприйняття кутом огляду веб камери. Ми не знаємо, де знаходиться людина, що відбувається у тих «сліпих зонах», які технічно не можемо перевірити. Тому можливість підслуховування чи незаконного запису розмови абсолютно реальна.

У таких випадках медіатори найчастіше висловлюють прохання продемонструвати кімнату, в якій знаходиться людина з усіх боків, та підтвердження з її боку, що вона знаходиться за закритими дверима. Таке рішення справді має сенс і практичну користь, але, як визнають і самі медіатори, – це не є абсолютною гарантією, що особа не вчиняє спроб порушити принцип конфіденційності.

В цілому, при будь-яких зовнішніх перевірках завжди залишається можливість обійти правила (приховати від камери звукозаписувальну техніку, не відслідковування чи не вчиняється спроб підслухати розмову іншою особою за дверима), тому справді дієвим варіантом є спонукання особи до відмови вчиняти такі дії, що ґрунтується на її внутрішньому переконанні. Окрім цього, доречним вважаємо передбачити обов'язок сторін угоди про надання медіаційних послуг створити всі можливі умови для унеможливлення витоку відомостей, отриманих в процесі медіації. Заборона на вчинення дій пов'язаних з намаганнями скопіювати розмову чи її частину для подальшого відтворення під час онлайн медіації має бути акцентована серед загальної вимоги не порушувати принцип конфіденційності.

Доречним буде детальне визначення переліку недопустимих дій, які б забезпечили конфіденційність медіації одразу в угоді про медіацію. При чому такий перелік має бути пристосований саме до онлайн медіації, адже в такому випадку він буде значно ширший, ніж при очній зустрічі.

Формат онлайн медіації не можна пов'язувати лише з пандемією. Він є зручним у випадках неможливості обом сторонам бути присутніми в одному приміщенні; з причин великої різниці у відстанях; через місцезнаходження сторін у різних державах; через специфіку особистого графіку тощо. Закріплення вимог дотримання принципу конфіденційності та відповідальності за його порушення, особливо при дистанційній медіації має бути враховано при підготовці проекту закону про медіацію. Встановлення і закріплення справедливої відповідальності стримуватиме людей від бажання порушити встановлені на законодавчому рівні правила.

Отже, забезпечення принципу конфіденційності онлайн медіації є важливим чинником для створення безпечних умов побудови діалогу, і як наслідок – збільшення ймовірності успішного врегулювання конфлікту. На сьогодні, проблемним питанням є взаємодія людей з програмами відеозв'язку, а також низький рівень безпеки даних у Інтернет просторі.

Отже, сторони мають розуміти наявність заборони на вчинення дій, що порушуватимуть принцип конфіденційності. Сприяти відмові сторін від вчинення таких дій може їх визначення та пряма заборона в угоді про надання медіаційних послуг, а також встановлення юридичної відповідальності у законопроекті про медіацію. Виключення наявних проблем зробить медіацію більш привабливою та доступною для потенційних учасників, що звичайно призведе до поширення практики її застосування.

Література

1. Головка О. М. Цифрова культура та інформаційна культура: права людини в епоху цифрових трансформацій. Інформація і право. 2019. № 4 (31). С. 37-44.
2. Головка О.М., Друзь В.Д. Право на правосуддя та право на доступ до інформації: кореляція та взаємозалежність. Інформація і право. 2020. № 1(32). С. 130-137.

Гуменюк А.О.

студентка КПІ ім. Ігоря Сікорського

Науковий керівник: **Головко О.М.**

к.ю.н, ст. викладач КПІ ім. Ігоря

Сікорського

ЕФЕКТИВНІСТЬ ДИСТАНЦІЙНОЇ РОБОТИ МЕДІАТОРА В УМОВАХ ПАНДЕМІЇ

В умовах пандемії, коли люди ізольовані один від одного, ускладнився і процес налагодження взаємовідносин, особливо в частині врегулювання конфліктів між сторонами. Так, виникла потреба дистанційного врегулювання суперечок, одним із варіантів якого є онлайн медіація.

Дистанційна медіація – це нові можливості для вирішення спорів у досудовому порядку, але варто зазначити, що викликів та ризиків, які потрібно продумати та вирішити теж досить багато.

Посилаючись на думку науковця Розумної М. М., законодавче врегулювання медіації та врегулювання питання онлайн-правосуддя та використання онлайн способів альтернативного вирішення спорів може мати наслідком значне зменшення навантаження на судову систему та забезпечення доступу до правосуддя всім верствам населення в умовах нової реальності [1, с. 147].

Варто розглянути як приклад той факт, що під час пандемії в рази збільшився відсоток розлучень по всьому світу. Перебуваючи в умовах самоізоляції багато пар зрозуміли, що бажають припинити спільне проживання. Таке рішення, ймовірно, прийняте на емоціях в першу чергу потрібно обдумати та проговорити, і вже потім звертатись до суду.

Варто зазначити, що українське суспільство за час панування пандемії стало свідком збільшення строків розгляду спорів в судах, перенесення судових засідань через неможливість застосування відеоконференції у зв'язку із технічними обмеженнями чи навантаженням [2, с. 148].

Тому постає той факт, що в умовах пандемії, локдауну більшість установ зачинено, суди не працюють (або розглядають мак-

симально обмежену кількість справ), тому дистанційна mediaція – це найкраще вирішення такого роду труднощів. За допомогою медіатора та проведення переговорів є великий шанс врегулювати конфлікт із збереження стосунків між сторонами.

В теперішніх умовах суди потребують роботи медіаторів більше, ніж будь-коли, а отже з'явилися можливості дистанційної співпраці з судами інших регіонів. Тому можна визначити, що роль дистанційної mediaції при реалізації права на доступ до правосуддя в період карантину – надзвичайно важлива. Більшість медіаторів працюють на волонтерській основі, надаючи послуги безкоштовно. Можемо привести у приклад Київський районний суд м. Одеси, при якому працюють медіатори на громадських засадах.

Оскільки в нашій країні напрям mediaції на законодавчому рівні ще не закріплено, то медіаторами в більшості випадків здійснюють свою діяльність на громадських засадах задля того, щоб в майбутньому до медіаторів зверталось більше людей, а отже розвантажувалась робота судів.

Але варто зазначити, що при здійсненні дистанційної mediaції виникає достатня кількість труднощів, про які необхідно написати. По-перше, ставиться під сумнів конфіденційність процедури mediaції. Одна справа, коли сторони та медіатор перебувають в одній кімнаті і на безпечних умовах відбувається діалог, але коли все проходить дистанційно, за допомогою електронних пристроїв забезпечити цілковиту конфіденційність в разі складніше.

По-друге, варто взяти до уваги психологічний фактор: коли люди зустрічаються особисто в кабінеті медіатора, ймовірність вирішення конфлікту більша, оскільки медіатору легше слідкувати за швидкими реакціями, аргументами, а у разі виникнення непорозуміння – надання швидкого роз'яснення. Над цими завданнями ще необхідно попрацювати, та, можливо, розробити нові механізми роботи медіатора, враховуючи дистанційну специфіку процедури.

Тому, беручи до уваги всю вище зазначену інформацію, хочемо наголосити, що саме зараз, в умовах пандемії у людей є можли-

вість звернутись до медіатора та вирішити свій конфлікт швидко, не витрачаючи великі кошти.

Отже, підводячи підсумок: дистанційна медіація – це чужа можливість вирішення конфліктів та перегляду сторонами рішень, які вони приймають під впливом емоцій. Умови пандемії створили нові реалії для розвитку медіації, оскільки в цей період все більше людей звертаються за допомогою до медіатора. Важливо продовжувати працювати над недоліками дистанційного формату медіації та покращувати слабкі сторони дистанційної медіації – за таких умов вона стане популярнішою, більш доступною та потрібною для українського народу.

Список використаної літератури

1. Розумна М. М. Актуальні проблеми та перспективи розвитку альтернативних способів врегулювання спорів в Україні: онлайн медіація та посередництво. Підприємництво, господарство і право. 2020. № 9. С. 147-153.
2. Спектор О. М. Альтернативні способи вирішення цивільно-правових спорів: світовий досвід та перспективи застосування у правовій системі України: монографія. Київ. Нац. ун-т ім. Т. Шевченка. К.: Фенікс, 2013. с. 146-159.

Данілевич Д.Р.

студентка КПП ім. Ігоря Сікорського

Науковий керівник: **Головко О.М.**

к.ю.н., ст. викладач КПП ім. Ігоря

Сікорського

ДИСТАНЦІЙНА РОБОТА МЕДІАТОРА

Правові спори та конфлікти є невід’ємною частиною життя суспільства. І завдання держави – створення умов для вирішення спорів та захист охоронюваних законом прав та інтересів громадян. Найбільш відомим у суспільстві є традиційне звернення до

суду. Однак, існують й альтернативні методи вирішення спорів. Серед них найбільш відомою є медіаційна процедура.

Медіація є поширеним методом вирішення конфліктів за кордоном, який в багатьох державах закріплено на законодавчому рівні. Це зумовлено тим, що медіація має багато переваг. Це прямий спосіб запобігти судового процесу і зберегти взаємовідносини між сторонами спору. Деякі вчені вважають, що Україні медіація ще не поширена у масштабах всієї країни, тому що для цього існують перешкоди, через які такий метод врегулювання відносин не буде популярним і ефективним [1, с.276].

Медіація є перспективним способом вирішення спорів як у публічно-правовій, так і в приватноправовій сфері. Необхідність подальшого розвитку і вдосконалення діяльності інституту медіації сьогодні настійно диктується особливістю інтеграційних процесів, що відбуваються на сучасному європейському просторі [2].

В Україні на рівні законодавчих ініціатив сформовані підвалини для запровадження медіації та медіаційних процедур, проте зазначені законодавчі новели потребують формування чіткого теоретичного підґрунтя до:

- тлумачення термінів (медіація, медіатор, медіативна угода тощо);
- з'ясування суті та меж поняття юридичних спорів, що можуть бути вирішені за допомогою процедури медіації, адже, наприклад, включення до цієї категорії кримінальних проваджень та справ про адміністративні правопорушення потребує внесення змін до чинного законодавства України;
- відповідальності учасників процедури медіації за порушення вимог конфіденційності [3].

Тому ці законопроекти мають стати предметом громадського обговорення із залученням також суб'єктів зовнішньоекономічної діяльності, яким варто знати та вміти користуватися послугами медіаторів при вирішенні спорів, що виникатимуть у відносинах із європейськими партнерами. Як свідчить досвід іноземних країн, варто звернути увагу на фінансування інституту медіації,

підготовку фахівців, міжнародне співробітництво, прийняття відповідних законодавчих норм і залучення провідних спеціалістів.

Запровадження інституту медіації є конче необхідним для зменшення навантаження на судову систему та суддів безпосередньо, адже за великої кількості зареєстрованих справ найчастіше з'являється така сукупність соціальних якостей, як «людський фактор», який проявляється в порушенні правил застосування норм матеріального та процесуального права. Українській державі як учасниці інтеграційних і глобалізаційних процесів варто сприяти поглибленню міжнародного співробітництва та наслідуванню міжнародної практики в процесі створення не тільки судової, а й приватної медіації. Законодавчо врегульований процес медіації сприятиме швидкому вирішенню спорів у приватному порядку в різних галузях права, тим самим підвищуючи авторитет суду та органів державної влади в очах суспільства загалом [5, с.12].

В умовах сьогодення все більшої популярності набувають сучасні методи спілкування та навчання, а саме: онлайн-лекції, вебінари, чат-конференції, онлайн-наради, тощо. Не виключенням є і медіація, яку почали практикувати в дистанційному форматі. Природно, що ефективність вжитих зусиль в цьому напрямі багато в чому буде залежати від безпосередньої ініціативи, правового підґрунтя в даній сфері і з боку самої держави. Це, в першу чергу, стосується широкого інформування населення про існування медіації як способу мирного врегулювання суперечок в різних сферах життя людей. Таке інформування може проводитися через соціальні мережі, месенджери та інші засоби зв'язку, які наразі є найбільш ефективними для отримання інформації.

В цьому плані громадські організації, що займаються проблемами розвитку інституту медіації в Україні, готові представити свої пропозиції до законодавчого органу і взяти активну участь у підготовці та проведенні Національної конференції медіаторів, тим більше, що партнерські зв'язки з організаціями інших країн, в яких медіація працює ефективно, вже існують і є їх досвід, який необхідно використовувати.

Однак, як і будь-який процес, дистанційна медіація має і свої недоліки. Одним з них можна назвати технічні проблеми, а саме: відсутність інтернет зв'язку; технічні збої; неможливість встановити зв'язок зі сторонами тощо. Дані проблеми можуть мати наслідком затягування процесу медіації, а також викликати незадоволення сторін спору, спровокувати новий конфлікт та стрес. Крім того, щоб скористатися онлайн медіацією особа повинна мати достатні навички для роботи із відповідним програмним забезпеченням та доступ до нього, що не завжди можливо забезпечити.

Ще одним із недоліків використання онлайн медіації є неможливість використати такі навички медіатора як аналіз мови тіла в повній мірі. Тобто, медіатор не може проаналізувати міміку, вираз обличчя, пози сторін тощо, що зумовлює обмеженість технік та прийомів, які можуть бути використані.

Також, недопрацьованим на даний момент є забезпечення конфіденційності як від третіх осіб, адже можливі хакерські атаки та втручання у канали зв'язку, так і від самих сторін, адже вони можуть записувати медіацію на відео або дублювати чати, і в подальшому намагатися їх використати для судового провадження.

Отже, зазначені недоліки та виклики, які наразі стоять перед дистанційною медіацією породжують широке поле для дискусії щодо доцільності та ефективності її використання в Україні, однак, на мою думку, переваг значно більше, а усі недоліки з часом та новітніми розробками можна вирішити.

Проте, дистанція медіація має і свої переваги. Так, першою перевагою такого способу медіації можна назвати те, що її проведення можливе незалежно від місця знаходження сторін. Особливо дана перевага відчутна під час вирішення міжнародних спорів, де сторони знаходяться на значній відстані одна від одної, а проведення офлайн зустрічі значно ускладнено.

Другим плюсом дистанційної медіації є економія фінансових ресурсів. Так, при такій формі медіації сторони не повинні витрачати грошові кошти наприклад на квитки, проживання в готелях, а також, на організацію цієї зустрічі, крім того, кожен із учасників

медіації може знаходитися у будь-якому зручному для них місці, а сама медіація може проводитися у зручний для всіх сторін час.

Третьою перевагою дистанційної медіації є те, що медіатор може пропонувати свої послуги не обмежуючись місцем свого проживання, і навіть країною проживання. Також, дана перевага є плюсом і для сторін спору, адже вони можуть обирати будь-якого медіатора, орієнтуючись не тільки на його місце проживання, а й на досвід та успішні практики.

Також, для онлайн медіації є перевагою той факт, що сторони відчувають менший стрес, оскільки не бачать один одного вживу, і можуть стримувати свої емоції, наслідком чого є швидке та правильне вирішення спору. Крім того, зарубіжні дослідження свідчать, що особи, які скористалися послугами онлайн медіації відчувають себе спокійніше, менш вороже налаштованими та більш впевненими у собі, порівняно з особами, які беруть участь у медіації віч-на-віч, це дозволяє їм більш зосередитися на конфлікті та пошуку варіантів рішення, аніж на сварках та суперечках один з одним [7].

Отже, дистанційна медіація набуває все більшої і більшої актуальності в умовах сьогодення. Зазначені недоліки та виклики, які наразі стоять перед дистанційною медіацією, породжують широке поле для дискусії щодо доцільності та ефективності її використання в Україні, однак, на мою думку, переваг значно більше, а усі недоліки з часом та новітніми розробками можна вирішити.

Список використаних джерел

1. Гаврилiшин А. П. Медіація як альтернативний спосіб вирішення спорів. *Науковий Вісник Херсонського державного університету*. Херсон. 2014. № 5. Т. 1. С. 275–278.
2. Гусейнова Р.З. Перспективи розвитку медіації в Україні. *Юридична газета*. 2014. №37-38. DOI: <http://jur-gazeta.com/publications/actual/perspektivi-rozvitku-mediatsiyi-v-ukrayini.html>
3. Про медіацію: проект закону України від 17 лютого 2010 року № 7481. *Законодавство України* : база даних / Верхов. Рада України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=44891

4. Про міжнародну комерційну примирювальну процедуру з настановами щодо її впровадження й застосування: типовий закон ЮНСІТРАЛ від 05 березня 2002 року. URL: [http:// www.uncitral.org/pdf/english/texts/arbitration/ml-conc/0390953_Ebook.pdf](http://www.uncitral.org/pdf/english/texts/arbitration/ml-conc/0390953_Ebook.pdf)

5. Резнікова В. В. Медіація (посередництво) як спосіб вирішення господарських спорів. *Вісник КНУ*. Київ. 2012. № 90. С. 10–15.

6. Бершеда Є. Р. Перспективи застосування медіації при вирішенні податкових спорів в Україні. *Голос України*. 2016. DOI: <http://www.golos.com.ua/article/265220>

7. Єрьоменко Г.І. Медіація як спосіб вирішення суперечок. DOI: https://www.training.com.ua/live/interview/Mediatsiya_yak_sposib_virishennya_superechok

Сорока М.М.

студентка КПП ім. Ігоря Сікорського

Науковий керівник: **Головко О.М.**

к.ю.н., ст. викладач КПП імені Ігоря Сікорського

ЗДІЙСНЕННЯ ДИСТАНЦІЙНОЇ МЕДІАЦІЇ: МОЖЛИВОСТІ ЧИ ВИКЛИКИ?

У сучасних умовах, коли весь світ поглинула пандемія доступ до правосуддя став більш обмеженим. У зв'язку з цим, судові засідання затримуються чи навіть призупиняються, а спори не можуть вирішуватися швидко.

Як наголошує Головко О.М., “взаємопроникнення права на правову допомогу, права на доступ до правосуддя та права на інформацію формує новий вид інформаційного права особи, що кореспондує обов’язку адвоката, а саме – право на інформацію про альтернативні види вирішення спорів” [1, с. 150]. У таких випадках, коли справа потребує негайного вирішення і вона є медіабельною, сторони можуть звернутися до процедури медіації. Однак, процедура медіації теж стала дистанційною через пандемію, що призвело до виникнення неабиякої проблеми – забезпечити *конфіденційність* інформації, що є основою для

якісного врегулювання спору, довіри до медіатора та даної процедури загалом.

Перш за все, медіація – це структурована добровільна та *конфіденційна* процедура позасудового врегулювання спору (конфлікту), у якій медіатор (посередник) допомагає сторонам у розумінні їхніх інтересів та пошуку ефективних шляхів досягнення взаємоприйнятного рішення [2, с. 55].

Аналізуючи дане визначення, ми можемо припустити, що забезпечити основні ознаки даної процедури, такі як структурність можливо, розробивши графік онлайн зустрічей для врегулювання спору. Це додатково підтвердить ознаку добровільності, адже особи щонайменше зафіксують таким чином рішення про обрання конкретного медіатора та приєднаються до онлайн зустрічей. Проте, виникає питання:

- як забезпечити конфіденційність процедури, якщо сторони та медіатор перебувають у різних приміщеннях;
- як перевірити відсутність засобів аудіо- та відеозапису.

Конфіденційність інформації повинна забезпечуватися усіма учасниками процедури медіації, тобто як самим медіатором, так і сторонами, а також спеціалістами та юристами (адвокатами сторін), які можуть запрошуватися для допомоги при вирішенні конфлікту за згодою сторін.

Так, на думку Землянської В.В., конфіденційність полягає у тому, що медіатор повинен тримати у таємниці і не розголошувати інформацію, яку він отримав під час спілкування зі сторонами або в процесі медіації. Крім того, він не може виступати в ролі свідка у суді щодо інформації, отриманої в процесі медіації [3, с. 104].

Більше того, засади конфіденційності передбачені й у міжнародних актах, а саме, згідно з п. 2 додатку до Рекомендації № R (99) 19, прийнятої Комітетом Міністрів РЄ 15 вересня 1999 року на 679-й зустрічі представників Комітету, – “будь-які обговорення під час зустрічі мають конфіденційний характер та не можуть використовуватися в майбутньому, за винятком випадків, коли наявна згода сторін”. Відповідно до п. 30 даного додатку, “незважаючи на узгоджений принцип конфіденційності, інформація про

можливу небезпеку злочинів, про яку може стати відомо під час зустрічі, передається медіатором відповідним зацікавленим особам чи органам” [4].

А також принцип конфіденційності медіації встановлено у програмах відновного правосуддя у кримінальних справах, які були прийняті 2002 р. Економічною і Соціальною Радою ООН. Відповідно до них конфіденційність процесуальних дій розглядається так: “обговорення у відновних процесах, що відбуваються не публічно, мають бути конфіденційними та не можуть розголошуватися у подальшому, за винятком тих випадків, коли сторони на це погодились, або ж коли цього вимагає національне законодавство” [5].

Отже, як ми бачимо, цей принцип конфіденційності закріплений у багатьох міжнародних актах. Однак, в державі має бути наявний правовий механізм забезпечення дотримання такого принципу в межах діяльності медіатора. Варто робити акцент на добросовісності усіх учасників процедури як на координаційній зустрічі, так і в процесі медіації. Окрім цього, необхідно наголошувати на обізнаності учасників щодо відповідальності за розголошення конфіденційної інформації без згоди на це особи, якої стосуються такі відомості.

Джерела:

1. Головка О. М. Право на інформацію щодо альтернативних методів вирішення спорів. Інформація і право. 2019. Вип. № 1 (28). С. 144-151.

3. Можайкіна О. С. Поняття та зміст основних принципів медіації в цивільно-правових відносинах. Актуальні проблеми вітчизняної юриспруденції. 2017р № 5.

2. Землянська В.В. Відновне правосуддя в кримінальному процесі України: посібник. Київ: Видавець Захаренко В.О., 2008. 200 с.

4. Рекомендація Комітету Міністрів Ради Європи державам-членам, які зацікавлені в організації медіації у кримінальних справах від 15.09.1999 р. № R(99)19. URL: https://zakon.rada.gov.ua/laws/show/994_828#Text (дата звернення: 19.03.2019).

5. Посібник з програм відновного правосуддя. Серія посібників з кримінального правосуддя / Упр. ООН з наркотиків та злочинності. Дитячий фонд ООН (ЮНІСЕФ). URL: http://www.unicef.org/ukraine/ukr/11Jvenal_Const.indd.pdf (дата звернення: 12.03.2019).

Томик В.В.

студентка КПП ім. Ігоря Сікорського

Науковий керівник: **Головко О.М.**

к.ю.н., ст. викладач КПП імені Ігоря
Сікорського

МЕДІАЦІЯ В ЦИВІЛЬНИХ СПРАВАХ: ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ В УМОВАХ ПАНДЕМІЇ

Механізм вирішення цивільних справ у судовому порядку заснований на принципі змагальності, що передбачає, однак, таку ситуацію, у якій з більшою ймовірністю задоволеними будуть позовні вимоги того, хто надасть більш переконливі докази чи краще обґрунтує свою правову позицію. Крім того, прийняття рішення у справі насправді досить нечасто задовольняє справжні інтереси й потреби сторін, не вичерпує спір, який існує між сторонами. Примирення або ж досягнення консенсусу, які є найкращими варіантами закінчення конфлікту, а особливо у сімейних, трудових, комерційних справах, не завжди можуть бути забезпечені судом у повному обсязі. Однак, саме для цього й існує медіація як один із видів альтернативного вирішення спорів.

Тож медіація, що за своєю природою є процедурою позасудового врегулювання спору і здійснюється медіатором, який надає допомогу сторонам конфлікту у розумінні їхніх інтересів та пошуку найбільш взаємоприйнятної рішення, є одним з найефективніших способів досягнення консенсусу між учасниками даної діяльності та має декілька безсумнівних переваг у порівнянні з судовим розглядом справи, які пояснюють зростання чисельності її використання та підвищену увагу до такої процедури [1, с. 59].

Особливостями медіації, що роблять її більш ефективною в певних спорах порівняно з судовим розглядом, є те, що предмет розгляду не обмежується, адже враховуються всі потреби та наявні у сторін інтереси, участь у процедурі завжди є взаємною та добровільною, а кожна зі сторін може відмовитися від неї у будь-який час; медіація є конфіденційною, навіть щодо факту її проведення; на відміну від суддівського розгляду, який може тривати

роками, медіація провадиться значно швидше, її час залежить у більшості випадків лише від сторін конфлікту; вартість цієї процедури також значно нижча, ніж судові витрати, а головною перевагою є те, що відносини між сторонами не руйнуються, вони спільно приходять до рішення, яке здатне задовольнити кожного з учасників конфлікту [2, с. 3].

Крім того, медіація сприяє покращенню рівня правосвідомості громадян, можливості доступу до правосуддя, адже останнє повинно включати й позасудові методи вирішення спорів, що стає можливим завдяки використанню медіації у спорах різних категорій справ [3, с. 145]. Вона суттєво зменшує навантаження на суди, а як наслідок і строки розгляду й вирішення справ та відсоток таких рішень, що оскаржуються.

Запровадження медіації в систему національного механізму правового захисту фізичних та юридичних осіб, їх прав, свобод та законних інтересів наразі характеризується існуванням двох підходів. Один з них – досудова медіація – передбачає, що така процедура повинна бути незалежним альтернативним способом вирішення спорів, не включеним у судовий процес та існувати з ним паралельно, не перетинаючись. На основі цього підходу в Україні існують як окремі медіатори, так і їх групи, що здійснюють таку діяльність відокремлено від судового розгляду. Інша концепція пов'язана з судовою (присудовою) медіацією й орієнтується на впровадження цієї діяльності як одного з елементів судового процесу [4, с. 182].

Чинний Цивільний процесуальний кодекс України (далі – ЦПК України) перебуває на шляху до підвищення ефективності наявного в Україні правового механізму здійснення правосуддя. А тому імплементація до нього правових норм, що стосуються процедури медіації є вагомим кроком. Зокрема, у ст. 16 ЦПК України зазначається, що “сторони можуть вживати заходів для досудового врегулювання спору, що виник між ними, за домовленістю між собою або у випадках, коли такі заходи є обов’язковими згідно із законом” [5, ст. 16]. Крім цього, такий принцип медіації як конфіденційність простежується в ст. 70 ЦПК України, у якій встанов-

лено, що “особи, які надавали послуги посередництва (медіації), не можуть бути допитані як свідки про відомості, які були отримані ними під час проведення такої процедури” [5, ст. 70].

Процедурою, що містить певні ознаки досудового врегулювання конфлікту, є врегулювання спору за участі судді (ст. 201-205 ЦПК України). Така діяльність здійснюється суддею виключно до початку розгляду справи по суті за взаємною згодою обох сторін та є націленою на мирне й добровільне врегулювання спору, тобто без прийняття судового рішення. Вона не є медіацією за своєю суттю, однак має певні спільні з нею риси, є засобом, що допомагає скоротити час на вирішення справи, зберегти стосунки між сторонами та забезпечує добровільність виконання рішення, адже останнє приймається сторонами свідомо та на власний розсуд.

Врегулювання спору за участю судді проводиться на основі принципу добровільності, тобто кожен з учасників має висловити свою згоду. Якщо заяву про врегулювання спору подає лише одна зі сторін, тоді суд відмовляє у проведенні такої процедури [6, с. 120].

Враховується і принцип конфіденційності: будь-яка інформація, отримана під час проведення цієї діяльності є конфіденційною, заборонено вести протокол врегулювання спору за участю судді, фіксувати процес технічними засобами, вести кінозйомку, фото-, відео-, звукозапис чи використовувати будь-які портативні пристрої. Особливостями цієї процедури є і те, що вона повинна здійснюватися у неформальній обстановці, де суддя не використовує свої атрибути й статус, а сидить з усіма іншими учасниками за одним столом [7, с. 399].

Про здійснення такого виду діяльності постановляється ухвала, а сама процедура проводиться у формі спільних та закритих нарад. Відповідно на спільних нарадах присутні усі учасники конфлікту, а на закритих – лише суддя й одна зі сторін. Відмінності ж полягають у тому, що хоча судді й заборонено надавати будь-які юридичні поради та рекомендації, проте він може запропонувати сторонам можливі варіанти вирішення конфліктної ситуації, медіатор же відповідає лише за комунікацію між сторонами й не наді-

лений таким правом (виключення становить оціночна медіація). Також медіація може проводитися на будь-якій стадії судового процесу, тривалість такої процедури не обмежена та може здійснюватися повторно. Натомість врегулювання спору за участю судді проводиться виключно до початку розгляду справи по суті, не більше тридцяти днів від дня постановлення ухвали та не може здійснюватися повторно [5, ст. 201-205]. Однак, незважаючи на це, таке врегулювання спору за участю судді є певним підтвердженням використання елементів процедури медіації загальними судами, що сприяють у перспективі підвищенню довіри населення до кожного судді окремо та до системи правосуддя загалом.

Як медіація, так і врегулювання спорів за участю судді може здійснюватися дистанційно. Відповідно до ст. 203 ЦПК України сторони можуть брати участь у такій процедурі в режимі відеоконференцій [5, ст. 203]. Настання пандемії та запровадження карантинних обмежень зумовили виникнення певних труднощів у практиці врегулювання спорів та судовому захисті прав, свобод та законних інтересів осіб. Будь-які процедури щодо здійснення такої діяльності були уповільнені та не унормовані, потребували досить великих затрат на їх упорядкування, не були достатньо ефективними.

Онлайн медіація, безсумнівно, є наступним ступенем розвитку звичної нам процедури медіації та може бути здійснена дистанційно, наприклад, з використанням відеоконференцій на платформі ZOOM або будь-якій іншій, подібній до цієї. Однією з переваг дистанційного врегулювання спорів є економія часу. Більше не потрібно призначати зустріч у якомусь місці, добиратися до нього певний тривалий проміжок часу та сподіватися, що кожен з учасників буде вчасно. Достатньо лише знайти місце у себе дома, де ви можете встановити конференц-зв'язок. Це також означає, що проведення медіації стає можливим навіть тоді, коли особи, що є сторонами конфлікту, знаходяться на відстані один від одного або навіть в інших частинах світу.

Ще однією перевагою онлайн медіації є її комфорт. Кожна особа, знаходячись вдома або ж в іншому місці, де її емоційний стан

близький до відчуття захищеності, відчуває себе впевненіше, більш розкуто, спокійно, вона здатна об'єктивно оцінювати аргументи протилежної сторони та більш схильна до прийняття взаємовигідного рішення. Будь-який психологічний тиск відповідно виключається. Це ж з іншого боку є і певним викликом для дистанційної медіації. Особиста зустріч, все ж таки, з психологічної точки зору створює кращі умови для врегулювання конфлікту. Сторони стають більш вимогливими один до одного, активними, а медіатору легше спрямувати їх позиції та поведінкова модель обвинувачення до визначення їх інтересів та потреб. Однак, процедура медіації є добровільною, сторони можуть обрати той варіант проведення даної процедури, який підходить та є оптимальним саме для них.

Також, угода за результатами медіації, що найчастіше все-таки укладається у письмовій формі відповідно до практики, яка склалася на даний момент (проте відповідно до принципу гнучкості медіації сторони можуть самостійно визначати форму домовленостей між ними, а отже, така угода може бути й усною), може бути укладена дистанційно і не потребує особистої участі її учасників. Наприклад, підписуватись дана угода може за допомогою електронного цифрового підпису.

Отже, у висновку варто зазначити, що карантинні обмеження, пандемія або інші схожі обставини, що складаються у суспільстві чи житті окремої особи, не є перешкодою для здійснення медіації цивільних спорів, адже вона цілком ефективно та з дотриманням усіх необхідних вимог її здійснення може проводитись дистанційно. Розвиток інформаційних технологій та зростання популярності їх використання є лише тим фактором, що ще більше спонукає сторін конфлікту використовувати онлайн медіацію та врегульовувати спори дистанційно.

Список використаної літератури

1. Мамницький В. Ю., Белей О. В., Дулепа В. П. Медіація в цивільному процесі: перспективи запровадження в Україні. *Актуальні проблеми вітчизняної юриспруденції*. 2019. №3. С. 59–63.

2. Медіація та судова система. Що? Як ? Навіщо? URL: http://namu.com.ua/ua/downloads/promomaterials/DODATOK_6_BROSHURA_MEDIATCHIA_TA_SUD.pdf.

3. Головка О. М. Право на інформацію щодо альтернативних методів вирішення спорів. *Інформація і право*. 2019. Вип. № 1 (28). С. 144-151.

4. Бондаренко-Зелінська Н. Л. Впровадження медіації у судовий процес як складова наближення законодавства України до європейських стандартів. *Міжнародне приватне право: розвиток і гармонізація*. 2011. С. 181–185.

5. Цивільний процесуальний кодекс України: Закон України від 18 березня 2004 р. № 1618-IV. *Відомості Верховної Ради України*. 2004. № 40. Ст. 492.

6. Дяченко С. В. Колокольна. Н. С. Запровадження медіації для вирішення сімейних спорів у цивільному судочинстві України: судова практика. *Юридичний науковий електронний журнал*. 2020. №2. С. 118–121.

7. Крестовська Н. Романадзе Л. Медіація у професійній діяльності юриста. Одеса: «Екологія», 2019. 454 с.

Брайчевський С.М.

кандидат фізико-математичних наук,
старший науковий співробітник НДІ
інформатики і права НАПрН України

ПРОБЛЕМА ПРИРОДНОЇ МОВИ В СИСТЕМАХ ІЗ ШТУЧНИМ ІНТЕЛЕКТОМ

Сучасний прогрес в галузі інформаційних технологій суттєво розширює наші можливості, але й породжує нові виклики і нові ризики, що потребують ретельного вивчення. Одним з важливих напрямів застосування сучасних технологій є соціальна сфера, при чому основну роль, очевидно, відіграватимуть інформаційні технології. Дійсно, в соціальній сфері постійно підтримується обмін величезними обсягами інформації і забезпечувати його традиційними засобами стає дедалі важче. Окремі спроби впровадження інформаційних технологій в ті чи інші ланки соціальних служб, з одного боку, продемонстрували їхню ефективність, але з другого боку, показали, що такий процес далекий від досконалості і

не дозволяє успішно вирішувати весь спектр задач. Тому виникла необхідність розробки і впровадження комплексних програм автоматизації соціальних служб, які б забезпечили необхідну системність відповідних заходів. З цією метою і Україні була розроблена Стратегія цифрової трансформації соціальної сфери, яка визначає “напрями та завдання комплексної цифрової трансформації всіх компонентів системи соціального захисту населення на основі єдиних підходів, стандартів і технологій”[1]. Зокрема, вона чітко формулює основні фактори, що зумовили необхідність її розробки та реалізації. І з цього видно, що реалізація Стратегії далеко не зводиться до використання простої комп’ютерної техніки, а передбачає застосування потужних апаратно-програмних комплексів з широким спектром функціональних можливостей.

Важливою особливістю інформаційних технологій є те, що вони розвиваються в плані вдосконалення наявних можливостей незалежно від галузі застосування. А це означає, що при реалізації Стратегії так чи інакше будуть використовуватися новітні розробки, що забезпечують максимальний рівень ефективності автоматизації виробничих процесів.

До таких розробок належать і системи з елементами штучного інтелекту (далі – ШІ)[2, 3], які останніми роками починають активно впроваджуватись в життя. Такі системи значно розширюють наші можливості, але й породжують нові виклики та загрози. Це повною мірою стосується і автоматизації процесів в соціальній сфері.

Ми обговоримо окрему категорію специфічних проблем, які можуть виникати при застосуванні комп’ютерних систем з елементами ШІ. Ці проблеми, взагалі кажучи, є універсальними з точки зору галузі застосування, але в соціальній сфері вони можуть призводити до серйозних ускладнень. Головна причина полягає в тому, що тут вкрай важливим є безпосереднє спілкування служб з громадянами. Тому, з одного боку, має бути забезпечене точне розуміння потреб громадян і прийняття відповідних адекватних рішень, а з другого боку, не менш важливим є зворотній зв’язок з громадянами, тобто вони повинні оперативно отримувати зрозумілі відповіді (в широкому розумінні слова).

Важливість цієї обставини підтверджується тим, що в згадуваній Стратегії цифрової трансформації соціальної сфери серед основних факторів, що зумовили необхідність її розробки та реалізації, безпосередньо зазначені такі [1]:

- складні процедури звернення за соціальною підтримкою, низький рівень сервісу, корупційні ризики;
- значна кількість звернень громадян, які не є автоматизованими, дублюють один одного або є зайвими;

Отже, одним з ключових напрямів реалізації Стратегії є вдосконалення процесу підтримки і супроводу звернень громадян.

В традиційному режимі громадянин може певний час спілкуватися з працівником соціальної служби, в ході чого вони крок за кроком пояснюючи одне одному сутність справи, кожний з свого боку. У випадку використання громадянином автоматизованої системи такий режим стає вкрай проблематичним. Дійсно, для отримання певного результату, громадянин повинен ввести в систему запит. Для опису складної ситуації, що є предметом спілкування, необхідно побудувати відповідно складний запит. Виконати це професійно, використовуючи формальні мови запитів, більшість широкого загалу не в змозі. Отже, потрібно звертатись по допомогу до фахівця, а це ускладнює процес. Так само виникають складнощі в розумінні вихідної інформації, яку видає машина, оскільки вона також генерується на формальній мові. Тут допомога фахівця, скоріше за все, не потрібна, але можуть виникнути проблеми з правильною інтерпретацією того, що видає машина (громадянин може просто неправильно зрозуміти незвичний для нього набір термінів).

Одним з напрямів вирішення подібних проблем є застосування систем з елементами ІІІ.

Поняття «штучний інтелект» є надзвичайно популярним і, разом з тим, доволі погано визначеним. В літературі з ним пов'язано багато різноманітних спекуляцій від технічних непорозумінь до відвертих фантазій в дусі футуризму та наукової фантастики. В дійсності існує дві основні точки зору на поняття «штучний інтелект»:

- технологія створення обчислювальних машин, здатних вирішувати завдання, що традиційно вважаються інтелектуальними [2];
- властивість обчислювальних машин вирішувати такі завдання [3].

Головна складність полягає в тому, щоб строго визначити, які задачі слід вважати інтелектуальними. Але ми не будемо занурюватись в подібні фундаментальні проблеми. Для нас інтерес становитимуть системи, здатні здійснювати обробку текстів, складених природною мовою[4]. Не торкаючись проблеми строгого визначення поняття “природна мова”, скажемо лише, що мається на увазі вживання в процесі спілкування з машиною звичайних мовних засобів, якими люди користуються в розмові між собою.

Отже, надання можливості громадянам звертатись до комп'ютерної системи за допомогою звичних мовних засобів (так само, як вони звертаються до працівників відповідних установ), безперечно не просто підвищить ефективність системи, а переведе взаємодію з нею на якісно вищий рівень. Звичайно, сказане стосується і зворотного зв'язку з машиною.

Але використання ІІІ може призводити до появи серйозних проблем, в тому числі і таких, що потребують правового регулювання (див., наприклад, огляд [5] і посилання, що містяться в ньому).

Ми зупинимось на одній, надзвичайно важливій проблемі, пов'язаній з розумінням машиною тексту, складеного на природній мові. Вона полягає в тому, що можливості машини щодо розуміння природної мови обмежені і ще довго лишатимуться обмеженими. Незважаючи на переконливі успіхи в цьому напрямі, повного розуміння довільного тексту досягти ще не вдалося. А це означає, що машина так чи інакше сприйматиме звернення громадянина приблизно і, що ще гірше, відповідно до особливостей закладених в неї алгоритмів, розроблених людиною. Ми отримуємо, власне, те ж саме, що й у випадку використання формальних мов запитів, але тепер неадекватність спілкування прихована від людини. Громадянин вводить до системи осмислений запит при-

родною мовою і отримує таку ж осмислену відповідь. І він навіть не здогадується, що відповідь побудована на зовсім іншому розумінні його звернення, і до того ж може не відповідати реальному стану справ (видане машиною виглядає фахово бездоганим, але не корелює з чинним законодавством).

Таким чином, ми бачимо, що застосування кібернетичних систем з ІІІ в соціальній сфері потребує значних зусиль в плані забезпечення повноцінної взаємодії з громадянами. В тому числі, необхідно враховувати, що можуть виникати ситуації, які потребують вирішення складних питань стосовно відповідальності за припущені помилки. Отже, цифрова трансформація, яка, безперечно, є вкрай актуальною, повинна супроводжуватися переосмисленням загальних принципів правового регулювання в соціальній сфері.

Література

1. Про схвалення Стратегії цифрової трансформації соціальної сфери. *Розпорядження Кабінету Міністрів України*. Київ 2020. № 1353-р URL: <https://zakon.rada.gov.ua/laws/show/1353-2020-%D1%80#Text> (дата звернення 27.11.2020)
2. What is Artificial Intelligence? *FAQ от Джона Маккарти*, 2007. URL: <http://www-formal.stanford.edu/jmc/whatisai/whatisai.html> (дата звернення 27.11.2020)
3. Аверкин А. Н., Гаазе-Рапопорт М. Г., Поспелов Д. А. *Толковый словарь по искусственному интеллекту*. 1992. – 256 с. URL: <http://www.raai.org/library/tolk/aivoc.html#L208> (дата звернення 27.11.2020)
4. Максимов В. Ю., Клышинский Э. С., Антонов Н. В. Проблема понимания в системах искусственного интеллекта Новые информационные технологии в автоматизированных системах. 2016. 18 с. URL: <https://www.keldysh.ru/pages/cgraph/articles/dep20/publ2016/16-04.pdf> (дата звернення 04.12.2020)
5. Баранов А.А. ИНТЕРНЕТ ВЕЩЕЙ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: ИСТОКИ ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ. *IT-право: проблеми та перспективи розвитку в Україні: збірник матеріалів II-ї Міжнародної науково-практичної конференції (Львів, 17 листопада 2017 р.)*. Львів. : НУ «Львівська політехніка», 2017. 318 с. (С. 18-42).

Гиляка Олег Сергійович

кандидат юридичних наук начальник
управління планування і координації
правових досліджень в Україні
Національної академії правових наук
України, кандидат юридичних наук

МІЖНАРОДНИЙ ДОСВІД ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В СУДОЧИНСТВІ

Розвиток нових технологій у світі, використання штучного інтелекту і робототехніки в різних сферах суспільного життя – одна з реалій сучасної епохи. Використання штучного інтелекту та роботів створило абсолютно новий напрямок в юридичній науці, а нові виклики суспільству від штучного інтелекту в контексті права і прав людини стають предметом нових досліджень. Крім того, системи штучного інтелекту, здатні самостійно узагальнювати і аналізувати законодавство, інші нормативно-правові акти, судову практику і виносити стандартні, незаперечні рішення, також стають частиною судочинства.

Передовими користувачами штучного інтелекту в судочинстві залишаються Сполучені Штати Америки, які використовують технології переважно в цивільних і кримінальних справах. Дослідники зі Стенфордського університету (Stanford Computational Policy Lab) розробили алгоритм, який асистує судді під час обрання запобіжного заходу для підсудного: тримання під вартою або застави. Розглянувши близько 100 тисяч процесуальних документів, пов'язаних з обранням запобіжних заходів, розробники виявили, що одні судді в 90% випадків дозволяють громадянам виходити під заставу, тоді як інші – тільки в 50%. Програма дає змогу справедливо оцінити ризики й тримати під вартою значно меншу кількість осіб, не наражаючи на небезпеку громадськість.

Як показав досвід Сполучених Штатів Америки, обрання запобіжного заходу може бути ефективнішим за допомогою штучного інтелекту. Проте стосовно цивільних справ тенденція до залучення алгоритмів поки не зустрічається. Варто зазначити, що

основною причиною тут є те, що, наприклад, розгляд клопотань часто відбувається в короткий проміжок часу і великої потреби пришвидшувати процес нема. Проте присутній також фактор непевності за результати застосування штучного інтелекту, пов'язаний передусім з індивідуальними властивостями кожної справи.

За звання лідера з використання технологій із США може поборотися Китай, який є її прямим конкурентом на технологічній арені. Китай з 2017 року відправляє судочинство по розгляду справ, пов'язаних з інтернет порушеннями (фінансові позики, інтернет торгівля, захист авторських прав) в рамках цифрового суду. Всі дані вносять самі сторони, слухання відбуваються по відеочату, попереднє рішення виносить штучний інтелект. На базі найбільшого месенджера створений сервіс, що дозволяє користувачам брати участь в судових засіданнях без відвідування суду. Такий чат-бот завдяки технології штучного інтелекту розглянув понад мільйон цивільних справ. Першим цифровим судом став суд Ханчжоу, далі уряд КНР створив аналогічні суди в Пекіні і Гуанчжоу. Разом суди розглянули близько 119 тисяч справ й ухвалили рішення щодо 88 тисяч справ. Суд наділений повноваженнями розглядати спори у сфері авторського права, господарські спори в Інтернеті й порушення в сфері електронної комерції.

За словами директора інформаційного центру Верховного народного суду Сюй Цзяньфена, народні суди в країні будуть використовувати додатки для електронної подачі заяв, просувати мобільні електронні судові процеси, а також створювати мобільні мікросуди, що дозволяють інтелектуальним програмам охоплювати всі аспекти судових процесів.

Що стосується створення «розумних» судів, народні суди будуть зосереджені на точному виконанні судових рішень, створення голограм людей, які перебувають під слідством, а також формуванні зв'язку з системою соціального кредитування. Одночасно за допомогою технології розпізнавання осіб народні суди Китаю будуть удосконалювати комплексні послуги і створювати базу даних для надання послуг з перевірки особи і спільному використанню інформації про громадянство, адвокатів, підприємства і суддів.

Китайська онлайндова судова система, одна з публічних судових платформ країни, оприлюднила більше 60 мільйонів судових документів. На платформі зареєстровано до початку 2020 року понад 20 мільярдів відвідувань.

В Аргентині прокуратура округу Буенос-Айрес в 2019 році підвела проміжні підсумки експерименту з використання штучного інтелекту по ряду категорій цивільних і адміністративних справ. Виявилось, що місцевими суддями були затверджені 100% рішень, прийнятих за допомогою штучного інтелекту.

Додаток Prometea – двомовна програма (розпізнає англійську та іспанську мови), яка використовує цифрову бібліотеку документів. Prometea проаналізувала близько 300 тис. відсканованих судових рішень з 2016-го по 2018 рік, в тому числі 2000 постанов (в Аргентині окружні прокурори складають рішення, а головуючі судді у справах або відхиляють їх і пишуть власні, або просто схвалюють їх).

Тепер, як тільки нова справа потрапляє в прокурорську систему, Prometea зіставляє фактуру з найбільш релевантними рішеннями у своїй базі даних, що дозволяє програмі приблизно за 10 секунд вгадати, як суд відреагує на ситуацію. Мова поки йде про відносно прості справи, наприклад, суперечки про видачу ліцензії на перевезення таксі, відмову у виплаті компенсації вчителям, які купили шкільне приладдя за свій рахунок тощо. В результаті застосування програми прокурорські працівники виявилися звільнені від великих масивів рутинної діяльності. За словами глави офісу, 15 його юристів зараз за шість тижнів справляються з таким обсягом роботи, на який раніше їм було потрібно близько шести місяців, помилки при перегляді згенерованих комп'ютером файлів зустрічаються досить рідко. Окружний прокурор відзначив, що його співробітники для подачі рядової скарги на водіння в нетверезому вигляді повинні були внести в неї масу уточнень велику кількість разів. Тепер, формуючи подібний документ у новій програмі, вони вносять всі дані тільки один раз.

Високо оцінили додаток і судді, якими до теперішнього часу схвалено усі з запропонованих ним рішень. Однак програму не

можна вважати повноцінною заміною інтелекту судді-людини, проте вона дуже допомагає служителям Феміди, які буквально «поховані» у паперовій роботі.

У європейських судових системах використання алгоритмів штучного інтелекту поки що залишається переважно ініціативою приватного сектору і нечасто інтегрується в державну політику. Зокрема, у Франції введена кримінальна відповідальність за аналіз судової практики, що дозволяє спрогнозувати, яке рішення у справі може винести суддя. Ці поправки до законодавства були прийняті під тиском суддівського корпусу, аргументуючи це тим, що судові рішення використовуються для аналізу моделі поведінки конкретного судді, тим самим порушуючи його особисті права.

В контексті перспектив впровадження штучного інтелекту варто згадати про прийняття у грудні 2018 року Європейською комісією з питань правосуддя Ради Європи «Європейської етичної Хартії по використанню штучного інтелекту в судових системах та оточуючому середовищі». Хартією визначено етичні принципи застосування алгоритмів у судах. Зокрема, важливим видається принцип «Усе під контролем користувача», який передбачає можливість судді власноруч проглядати судові справи, які проходили обробку штучним інтелектом та відходити від результату, що було надано інтелектом. Варто зазначити, що такі технології вже використовуються у Європейському суді з прав людини.

Наразі штучний інтелект не має остаточного права виносити рішення, проте перспективи його подальшого впровадження видаються досить високими, враховуючи принцип його дії. Показовою є одна із справ Європейського суду з прав людини. У 1970 році Людмила Терентьєвна-Александрова втратила руку під час виконання службових обов'язків на державному підприємстві. Вона домагалася компенсації протягом багатьох років у радянських, а згодом російських судах, проте безрезультатно. Згодом вона подала скаргу до ЄСПЛ і у 2007 році суд зобов'язав Російську Федерацію виплатити жінці компенсацію. У 2016 році заради експерименту справу розглянув штучний інтелект. На основі об-

робки даних 583 інших справ ЄСПЛ, алгоритм цілком підтвердив правильність рішення справи.

Враховуючи вищезазначене, може здатися, що штучний інтелект у судовій системі – невідворотна дійсність. Алгоритми, на відміну від людей, не допускають помилок пов'язаних із внутрішніми переконаннями. Алгоритм не прийме неправомірну вигоду. На алгоритм неможливо чинити психологічний тиск. Проте варто розуміти, що якщо людина здатна до осмисленого прогресу, то штучний інтелект прогресуватиме лише під дією програмного коду, який писатимуть для нього люди. І цим кодом повинні бути передбачені численні нюанси, характерні для правової сфери. В іншому випадку, є ризик знаходження алгоритмічних дір, що стане предметом зловживань учасників справи. Наразі штучний інтелект у судах застосовується переважно для аналізу та обробки даних з попередніх справ. Однак є численні питання стосовно принципу дії алгоритмів при виконанні дискреційних повноважень. Це стосується передусім розгляду клопотань сторін, оцінки доказів, заходів із забезпечення доказів, обрання запобіжного заходу у кримінальних провадженнях, обрання терміну ув'язнення у кримінальних справах тощо.

Шваб І.О.

студентка Національної академії
Служби безпеки України

ЗАРУБІЖНИЙ ДОСВІД ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ПУБЛІЧНОМУ АДМІНІСТРУВАННІ

Сучасні інформаційні технології надали людству нові комунікативні можливості чим сприяли побудові нових взаємовідносин, іманентними ознаками яких є довіра, прозорість та ефективність. Внаслідок реформування державного управління виникли такі поняття як – публічне управління та адміністрування, які доречно було б адаптувати до реалій за допомогою використання штучного інтелекту.

Слід акцентувати увагу на тому, що галузь публічного управління та адміністрування є специфічною і диференційованою, що охоплює як юридичну, соціальну, так і економічну складову, оскільки наслідком публічності є вплив на формування територіальних громад, вирішення питання функціонування економіки та соціуму, а також формування держави в цілому. І тому, на мою думку, штучний інтелект допоміг би державі ефективно функціонувати вищезазначеній сфері.

Актуальність досліджуваної тематики полягає передусім у тому, що головною характеристикою штучного інтелекту є націленість на вирішення конкретних задач публічного адміністрування ефективно та за короткий відлік часу.

Аналіз останніх досліджень і публікацій. Вивченням створення та використання штучного інтелекту в різних сферах життєдіяльності суспільства займались зарубіжні науковці : О. Бін Султан, Т. Філер, П. Хайхем.

Метою статті є дослідження зарубіжного досвіду в публічному адмініструванні за допомогою штучного інтелекту.

Виклад основного матеріалу. Використання новітніх технологій інтелектуального управління може вивести саму ідею публічного управління на новий рівень.

Мова повинна йти вже не просто про надання державою зручних механізмів надання сервісних послуг громадянам і бізнесу, а про принципове переформатування самої діяльності держави, яка отримує значне скорочення бюрократичного апарату, зменшення або навіть усунення паперового документообігу, істотне зниження транзакційних витрат, повний контроль над діяльністю чиновників, ну і найголовніше, створення сприятливого середовища для життєдіяльності бізнесу і громадян.

Серед таких технологій найбільш задіяними у міжнародній практиці публічного управління, що вже довели свою ефективність є технології штучного інтелекту, Інтернету речей, блокчейну та Big Data.

Організація економічного співробітництва та розвитку (ОЕСР) у своїх принципах, схвалених у травні 2019 року, вказує, що штуч-

ний інтелект – “ це машинна система, яка може робити прогнози, рекомендації або рішення, впливаючи на реальне або віртуальне середовище на основі заданого людиною набору цілей ”[1].

Багато зарубіжних країн вже усвідомлюють всі переваги штучного інтелекту та починають активно переходити до практики інтелектуального управління у наданні державних послуг. Розглянемо конкретні приклади : у Новій Зеландії державні органи влади використовують штучний інтелект для публічного адміністрування. Як результат – державні сервіси зручні і доступні для громадян, а також провадження цифрова ідентифікація користувачів та підтримується зворотній зв’язок з громадянами.

Доречно зазначити ,що світовим лідером у сфері впровадження цифрових технологій є КНДР, де ухвалено «План розвитку штучного інтелекту наступного покоління» (New generation AI development project, 2017).

На мою думку, вище зазначений документ є максимально повним національним планом розвитку штучного інтелекту, адже містить не лише програму досліджень та впровадження технологій штучного інтелекту, а й стандарти та норми використання штучного інтелекту, програму розвитку та навчання талановитої молоді, а також систему гарантування цифрової безпеки [2].

В Сінгапурі штучний інтелект планують використовувати у сфері охорони здоров’я . Наприклад за його допомогою здійснюватиметься профілактика, діагностика, планування лікування, регулювання обігу ліків, функціонування точної медицини та розроблення нових медичних препаратів. Це також має допомогти зменшити кадрові ресурси охорони здоров’я, при доповненні інструментами штучного інтелекту, лікарні зможуть краще задовольняти зростаючі потреби в галузі охорони здоров’я у майбутньому.

Україна на шляху запровадження штучного інтелекту у публічне адміністрування також поступово розвивається. Про це свідчить використання комп’ютерних програм, заснованих на досягненнях машинного навчання і обробки мови, які допомагають лю-

дям у виконанні певних завдань і імітують взаємодію з реальним співрозмовником.

Типовими завданнями, з яким можуть допомогти боти, є перехід до потрібної інформації, або замовлення послуги. Боти надають допомогу в формі «питання-відповідь», створюючи відчуття спілкування з людиною. Прикладом є електронний сервіс – чат-бот «Держслужбовець Тарас», який допомагає суб'єктам декларування у заповненні декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування.

Зокрема, чат-бот надає користувачам покрокову інструкцію із заповнення електронної декларації, допомагає визначити, які відомості підлягають декларуванню щодо різних активів та доходів: містить актуальні відомості щодо порогів, встановлених для декларування окремих активів; містить додаткові посилання на відкриті державні реєстри, бази даних, сервіси, що можуть бути корисними суб'єктам декларування під час заповнення декларації. Чат-бот «Держслужбовець Тарас» є некомерційним та безкоштовним електронним довідковим сервісом, який створений за підтримки Антикорупційної ініціативи ЄС та ГО «Центр демократії та верховенства права». Наповнення інформацією чат-боту «Держслужбовець Тарас» здійснювалось виключно на основі положень Закону України «Про запобігання корупції», Роз'яснення щодо застосування окремих положень Закону України «Про запобігання корупції» стосовно заходів фінансового контролю, що затверджене рішенням Національного агентства з питань запобігання корупції від 11 серпня 2016 р. № 3 (зі змінами) та інших роз'яснень та рекомендацій, прийнятих Національним агентством з питань запобігання корупції [3].

Також Національна служба здоров'я України запустила чат-бот з інструкціями щодо COVID-19 для лікарів, швидкої допомоги, місцевої влади та пацієнтів.

За допомогою цього каналу лікарі, водії швидкої допомоги, пацієнти та представники органів місцевого самоврядування 24 години на добу зможуть отримувати відповіді на найбільш важливі питання щодо коронавірусу. Чат-бот в режимі реального часу

надає інструкції щодо попередження, діагностування та лікування COVID-19 [4].

Висновки та пропозиції. В результаті проведеного дослідження, можна зробити висновок, що технології інтелектуального управління, а саме штучний інтелект стає ефективним та обов'язковим інструментом сучасного публічного управління.

В Україні після закінчення плану заходів реалізації “Стратегії реформування державного управління України на 2016–2020 роки” необхідно базуючись на існуючому зарубіжному досвіді, розробити поетапну Національну стратегію розвитку з елементами впровадження штучного інтелекту, з метою використання технологій в усіх сферах життєдіяльності, зокрема у галузі знань публічного управління. Це дозволить громадянам отримувати віддалено сервісні послуги, державі – мінімізувати витрати на управлінські кадри .

У підсумку отримаємо підвищення довіри населення до державної служби, саме тому зарубіжний досвід використання новітніх технологій у системі публічного управління є актуальним для України, та потребує належної фінансової підтримки.

Список використаної літератури

1. Recommendation of the Council on Artificial Intelligence URL: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>.
2. A Next Generation Artificial Intelligence Development Plan URL: <https://chinacopyrightandmedia.wordpress.com/2017/07/20/a-next-generation-artificialintelligence-development-plan/>
3. В Україні працює електронний сервіс-чат-бот «Держслужбовець Тарас» URL: <https://khoda.gov.ua/v-ukra%D1%97n%D1%96-pracju%D1%94->
4. Чат-бот з інструкціями щодо COVID-19 URL: <https://nszu.gov.ua/novini/chat-bot-z-instrukciyami-shchodo-covid-19-226>

Ситник О. В.

аспірант кафедри міжнародного
права Інституту міжнародних
відносин Київського національного
університету імені Тараса Шевченка

ОСОБЛИВОСТІ ПЕРЕДАННЯ ПРАВА НА ДОМЕННЕ ІМ'Я ПОТОЧНИМ РЕЄСТРАНТОМ ДОМЕННОГО ІМЕНІ МАЙБУТНЬОМУ РЕЄСТРАНТУ

Сьогодні однією з найбільш важливих складових ведення будь-якого бізнесу є присутність у мережі Інтернет, а в багатьох випадках вона є вирішальною чи взагалі безпосередньою бізнес-діяльністю. У свою чергу, така присутність переважним чином пов'язана з правом на доменне ім'я.

Під доменним іменем розуміється частина адресного простору, що ідентифікує комп'ютер або комп'ютери та ресурси у мережі Інтернет та являє собою унікальне словесне або словесно-цифрове позначення. [1, с. 325] Відтак, цілком очевидним є той факт, що в разі, якщо використання доменного імені лежить в основі тієї чи іншої успішної бізнес-діяльності, то право на доменне ім'я є ключовим для функціонування такого бізнесу, і у випадку його продажу саме належним чином оформлене набуття права на доменне ім'я буде головною метою потенційного покупця.

Втім, до здійснення характеристики належного передавання права на доменне ім'я потрібно спершу окреслити основи його функціонування.

Насамперед варто зазначити, що особа, яка володіє правом на доменне ім'я, – це реєстрант. Реєстрантом доменного імені є фізична або юридична особа, що зареєструвала доменне ім'я. [2]

Загалом реєстрація доменних імен здійснюється в рамках централізованої бази даних WHOIS, що є безкоштовним загальнодоступним каталогом, котрий містить контактну й технічну інформацію про зареєстрованих реєстрантів доменних імен. [3] Глобальне управління системою доменних імен здійснює Інтернет-корпорація з присвоєння імен та номерів (ICANN) – міжнародна непри-

бутова організація, що контролює присвоєння як IP-адрес, так і доменних імен. [2]

Безпосередньо ж реєстрацію доменного імені проводить реєстратор – організація, що акредитована ICANN та має дозвіл від оператора відповідного домену верхнього рівня (організації, що відповідальна за утримання реєстру домену верхнього рівня, у межах якого здійснюється реєстрація доменного імені) на продаж доменних імен. [2]

Отже, для фактичного здійснення поточним реєстрантом доменного імені передання права на доменне ім'я майбутньому реєстранту є необхідним внесення реєстратором змін до бази даних WHOIS про реєстранта доменного імені (переделегування доменного імені).

Такому переделегуванню має передувати ряд кроків з боку поточного реєстранта та майбутнього реєстранта – пропонуємо на прикладі України розглянути їхній перелік, наведений нижче.

1. Укладення договору про передання права на доменне ім'я між поточним реєстрантом та майбутнім реєстрантом із підписанням відповідного акта приймання-передання.

2. Подання поточним реєстрантом реєстратору доменного імені заяви про бажання передати право на доменне ім'я майбутньому реєстранту.

3. Подання майбутнім реєстрантом реєстратору доменного імені заяви про бажання прийняти право на доменне ім'я від поточного реєстранта.

4. У разі, якщо об'єктом переделегування є доменне ім'я другого рівня в домені .UA, то обов'язковою передумовою також буде:

- передання права власності на знак для товарів і послуг, що був підставою для початкової реєстрації доменного імені відповідно до Регламенту особливостей реєстрації приватних доменних імен другого рівня в домені .UA, за договором про передання права власності на такий знак із подальшим поданням реєстратору документів, що підтверджують таке передання права власності; або

- надання права на використання знаку для товарів і послуг, що був підставою для початкової реєстрації доменного імені відповідно до Регламенту особливостей реєстрації приватних доменних імен другого рівня в домені .UA, за ліцензійним договором, у якому зазначено про передання права користування відповідним доменним іменем, із подальшим поданням реєстратору документів, що підтверджують таке надання права на використання знаку для товарів і послуг та передання права користування доменним іменем. [4]

Якщо ж об'єктом переделегування є доменне ім'я третього і нижчих рівнів у домені .UA, то в такому разі переделегування здійснюється без передання права власності або надання права на використання знаку для товарів і послуг та передання права користування доменним іменем, оскільки й сама процедура початкової реєстрації такого доменного імені здійснюється без підтвердження права власності на знак для товарів і послуг або права на використання знаку для товарів і послуг та права користування доменним іменем.

Таким чином, передання права на доменне ім'я поточним реєстрантом доменного імені майбутньому реєстранту є процедурою, котра для успішного здійснення вимагає від кола її учасників чіткого та послідовного виконання всіх необхідних кроків.

Список використаних джерел:

1. Посібник для суддів з інтелектуальної власності / Бенедисюк І. М. та ін. – Київ: К.І.С., 2018. – 424 с.
2. Domain Name Registration Process. URL: <https://whois.icann.org/en/domain-name-registration-process> (дата звернення: 04.12.2020)
3. WHOIS Primer. URL: <https://whois.icann.org/en/primer> (дата звернення: 04.12.2020)
4. Інструкція щодо процедури переделегування приватного доменного імені другого рівня в домені .UA іншому реєстранту. URL: <https://hostmaster.ua/policy/?instr1> (дата звернення: 04.12.2020)

Шуміло О.М.

кандидат юридичних наук, доцент,
доцент Харківського національного
університету внутрішніх справ

ЕКОЛОГІЧНИЙ КРАУДФАНДИНГ ЯК ЗАСІБ СОЦІАЛЬНОЇ ТРАНСФОРМАЦІЇ: ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ

Головною умовою і поштовхом переходу до збору коштів для екологічних проєктів шляхом краудфандингу стане подальший розвиток громадянського суспільства у нашій країні. Залежно від різних типів проєктів та технологій збору фінансових коштів краудфандинг щодо екологічних проєктів, враховуючи його мету, прийнято відносити до соціальних, що викликані браком коштів.

Важливе місце займають проєкти щодо сталого розвитку та зеленої енергії. Значна кількість неприбуткових організацій звернулися до краудфандингових платформ, оскільки у сучасних умовах індивідуальні внески чи банківські позики важче отримати [1, с. 51].

З'явився окремий напрямок краудфандингу – еко-краудфандинг. Наприклад, у 2009 році вийшла у світ кінострічка документалістів «Століття дурнів», що розкриває проблеми кліматичних змін на планеті. На виробництво цієї стрічки збирали кошти майже п'ять років і у результаті було отримано бюджет понад 900 тисяч фунтів стерлінгів, які надали близько 600 прихильників.

У Великій Британії громадська організація «10:10» розпочала кліматичний проєкт «Solar School», який забезпечує деякі англійські школи сонячними панелями [2].

Проаналізувавши економічну та юридичну літературу, а також краудфандингові платформи, можна дійти висновку щодо основних складових етапів їх функціонування.

Краудфандингова платформа створюється з метою допомоги збору коштів (фінансування) екологічного проєкту для досягнення позитивного соціального (некомерційного) ефекту. Джерелом коштів виступають внески третіх осіб (благодійників).

Відповідальність щодо залучення коштів покладається на ініціатора збору благодійних пожертв для екологічних проєктів із використанням благодійного телекомунікаційного повідомлення. Тобто, оголошується публічна оферта та оприлюднюється публічний договір. Згідно із положеннями ст. ст. 633, 641 ЦК України [3] умови публічної оферти та публічного договору встановлюються однаковими для всіх споживачів. Отримувачем фінансової допомоги може бути: приватна особа, ініціативна група, громадська організація зі статусом юридичної особи або без такого статусу, чи благодійний фонд. Це дозволяє небайдужим громадянам оперативно отримати кошти для охорони довкілля, на відміну від міжнародних фондів-грантодавців, що вимагають обов'язкової реєстрації і т. ін..

Закономірно постає питання, якими слід вважати відносини щодо екокраудфандингу: публічними чи приватно-правовими? Оцінюючи це, потрібно взяти до уваги, що згідно зі ст. 66 Конституції України [4] кожен зобов'язаний не заподіювати шкоду природі, культурній спадщині, відшкодовувати завдані ним збитки. Тобто охорона навколишнього природного середовища визнається обов'язком кожного, і право на сприятливе довкілля має кожний. Таким чином постає потреба в публічно-правових засобах забезпечення екологічних конституційних приписів. З іншого боку, перебування деяких природних об'єктів у приватній, державній, муніципальній та інших формах власності, вільне право користування природними об'єктами права власності народу відповідно до закону (якщо це не використовується на шкоду людині і суспільству та не завдає шкоди довкіллю і не погіршує екологічну ситуацію і природні якості землі), на що вказують ст. ст. 13, 41 Конституції України [4], включає у регулювання суспільних екологічних відносин приватно-правові методи.

Охорона довкілля як загального блага, що має соціальну спрямованість, тяжіє до публічних форм впливу, а використання природних об'єктів, включених до цивільного обороту (із урахуванням права власності народу України на всі природні об'єкти), передбачає приватно-правові засади.

Однак слід розрізняти краудфандинг звичайний та екологічний, тобто той, який має на меті збір коштів, що будуть спрямовані для поліпшення стану довкілля. Вчені, як правило, застосовують комплексний підхід для розмежування публічно-правових відносин від приватно-правових і вважають, що у краудфандингових правовідносинах відбувається переважно диспозитивне (субсидіарне) правове регулювання. Сторони вільні у встановленні відносин, неврегульованих нормами цивільного права, але в той же час не суперечать його основним засадам, правилам взаємодії. Однак слід зазначити, що краудфандингові правовідносини не можуть повністю обійтися без використання імперативних правил, в тому числі заборон (ліцензування, встановлення максимальних обмежень щодо збору та пожертви, заборони використання біткоїнів, цільового використання природних об'єктів). Тобто здійснюється регуляторний вплив державних установ на процес екологічного краудфандингу.

Щодо суб'єктів краудфандингових правовідносин, то вони знаходяться між собою у відносинах координації, а не субординації, тобто учасники юридично рівні між собою. Тому цивілісти в більшості краудфандинг відносять до галузі приватного права [5].

Варто звертати увагу на суб'єктний склад учасників краудфандингової кампанії, коли краудфандинговою платформою, наприклад на «Спільнокошті» передбачається умова, що в разі досягнення певного результату у залученні коштів, виникає можливість дофінансування певною установою із подвоєнням суми. Це безповоротне дофінансування від Міжнародного фонду «Відродження» можливе на користь проєктів у сфері культури, в тому числі і тих, що мають на меті значимий соціальний вплив з фокусом на темі екологічної сталості, в межах ініціативи «Культура. Спільнота». У цій ситуації ми можемо спостерігати підвищення ролі краудфандингових платформ у суспільному житті. Коли Міжнародний фонд «Відродження», працюючи із «Спільнокоштом» як партнерською платформою програми, здійснює безповоротне дофінансування після залучення коштів від громадян на проєкт екологічної сталості.

У юридичних колах ще не сформувалась юридична позиція стосовно того до якого виду договорів слід відносити краудфандинг. Вважають, що краудфандинг може мати риси договорів: дарування, простого товариства, а також купівлі-продажу (із попередньою оплатою) [7], [8]. Але розв'язати цю дискусію зможе спеціальний закон або зміни до відповідних нормативних актів. Наприклад як у США там їх діяльність таких платформ регламентується спеціальним законодавчим актом [9].

Тому згідно національного законодавства у США краудфандингова платформа має бути зареєстрована у Комісії із цінних паперів і біржах США (U. S. Securities and Exchange Commission, SEC) – незалежне державне агентство уряду США є головним органом, що здійснює функції нагляду і регулювання американського ринку цінних паперів. Також вона має бути учасником Служби регулювання у сфері фінансових послуг (Financial Industry Regulatory Authority, FINRA) – приватна американська корпорація зі статусом саморегулюючої організації (self-regulatory organization, SRO) з контролю за дотриманням правил торгівлі на позабіржовому ринку (OTC Markets Group), ринку цінних паперів фірм, що не котируються на звичайних біржах, створена за рішенням Конгресу США.

У той же час для українських платформ відсутність подібного національного нормативного акту дозволяє громадськості діяти за принципом «дозволено все, що прямо не заборонено законом», збирати максимальні суми для своїх проєктів від благодійників, не підпадати під особливий податковий режим стягнень. Але наявність спеціального нормативного акту врегулює діяльність краудфандингу, визначить термінологію і дасть поштовх громадськості для збору та спрямування коштів на охорону довкілля. Адже поки що порівняння краудфандингу з одним із існуючих на сьогоднішній день договірних інститутів в Україні видається некоректним і тому вважаємо, що із цим слід погодитись як із правовою новелою. Тільки спеціальний закон і зміни до відповідних нормативних актів зможе повністю врегулювати інститут краудфандингу в Україні.

Література

1. Шуміло О. М. Фінансування екологічних проєктів шляхом краудфандингу: правові аспекти та практика застосування: практ. посіб. [за заг. ред. О. Кравченко]. Львів: Видавництво «Компанія «Манускрипт»», 2020. 108 с. https://manusbook.com/9042_EPL_Finansuvannya/2/index.html.
2. Шевченко Анастасія. Краудфандінг – нове джерело екофінансування [Електронний ресурс]. Сайт КліматІнфо. Режим доступу: <http://www.climateinfo.org.ua/content/kraudfanding-nove-dzherelo-eko-finansuvannya> (дата звернення: 21.01.2020). Назва з екрана.
3. Цивільний кодекс України від 16.01.2003 р. за № 435-IV. Офіційний вісник України. 2003. № 11 (28.03.2003). Ст. 461.
4. Конституція України: Закон України від 28.06.1996 р. за № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30 (23.07.96). Ст. 141.
5. Саяпин С. П. К вопросу о правовой природе краудфандинга. Вопросы российского и международного права. 2019. Том 9. № 5А. С. 170–176.
6. Конкурс ідей для партнерства в краудфандінговій ініціативі «Культура. Спільнота». Сайт Міжнародного фонду «Відродження» [Електронний ресурс]. Режим доступу: https://www.irf.ua/contest/konkurs-idej-dlya-partnerstva-v-kraudfandingovij-inicziatyvi-kultura-spilnota/?fbclid=IwAR0xFuFcOYQAJU5TzGPoEmBxlnhBkRVQ_4ARNjLWZojt5FRrPiKbTI OmsdE (дата звернення: 26.03.2020). Назва з екрана.
7. Алексеев Н.В. Краудфандинг: от реализации частной инициативы к решению общественных проблем. Бюллетень науки и практики. 2016. № 10 (11). С. 271–277.
8. Архипов Е. Понятие и правовая природа краудфандинга. Актуальные проблемы предпринимательского права. М.: Стартап, 2015. Вып. 4. С. 18–27.
9. Jumpstart Our Business Startups Act, or JOBS Act, 05.04.2012 [Electronic resource]. Access mode <https://www.govtrack.us/congress/bills/112/hr3606/text> (last accessed: 21.01.2020). Heading from the screen.

Шахбазян К.С

кандидат юридичних наук, учений
секретар, Центру досліджень
інтелектуальної власності та
трансферу технологій НАН України

**ПРАКТИКА ОХОРОНИ АВТОРСЬКОГО ПРАВА
НА НАУКОВІ ЖУРНАЛИ ТА МОНОГРАФІЇ
ВИДАВНИЦТВАМИ В ЄС ПРИ КОМЕРЦІЙНОМУ
ВИКОРИСТАННІ ТА НАДАННІ ВІЛЬНОГО ДОСТУПУ ДО
ВИДАНЬ ЧЕРЕЗ ІНТЕРНЕТ**

Узагальнення досвіду охорони авторського права у випадку публікації творів у відкритому доступі або за комерційного використання свідчить про застосування трьох основних підходів до використання творів: комерційне використання, вільний доступ та гібридна модель. Комерційне використання творів та гібридна модель застосовуються видавництвами, які всі витрати на публікацію та розповсюдження видань беруть на себе. За вільного доступу витрати, пов'язані з його забезпеченням, здійснюються авторами зацікавленими установами через сплати внесків, а також можуть компенсуватись в рамках міжнародних та національних програм досліджень (зокрема, проектах Рамкової програми Горизонт 2020) тощо.

У 2000 роках характерним для багатьох журналів є перехід від моделі комерційного розповсюдження за передплатою до моделі вільного доступу зі сплатою витрат авторами та іншими організаціями. Тоді ж виникла ідея створення гібридних журналів відкритого доступу (Hybrid open access OA journal), в яких тільки частина статей знаходиться у відкритому доступі, а решта – платні для читачів (точніше, платні для їх університетів і наукових організацій), оскільки розповсюджуються за звичайною передплатою (ця гібридна модель стала називатися Walker-Prosper model for open access journal). Публікація OA-статей здійснюється через спеціальні онлайніві видавничі платформи: ScienceDirect – для видавництва Elsevier, SpringerLink – для Springer Science,

WileyInterScience – для John Wiley & Sons, BlackwellSynergy – для Blackwell Publishing і т. д.

Моделі фінансування журналів відкритого доступу. Основні моделі фінансування наукових журналів в Європі – поширення за передплатою (paywall) або модель Відкритого доступу (OpenAccess – OA), гібридна модель – «*принцип подвійного збору*».

За чверть століття розвитку відкритих журналів було придумано кілька схем, які дозволяють забезпечувати видання Open Access або навіть отримувати з нього надприбуток. Найбільш поширеним способом монетизації журналу відкритого доступу вважається стягнення «плати за публікацію» (*Article-processing charges* або *APC*), при цьому результати різних досліджень показують, що таку модель використовують від 30 до 50% видань [1]. Модель передбачає утримання журналу за рахунок авторів, які хочуть зробити свої публікації загальнодоступними (що підвищує видимість, цитованість і в цьому сенсі значимість матеріалів).

Стійкість цієї моделі підтримують численні державні та некомерційні організації, які вимагають, щоб фінансовані ними дослідження були у відкритому доступі, і платять за відкриту публікацію. Автори, як правило, вибирають *APC*, коли такі витрати бере на себе третя сторона (фонд, або університет, або це – умова робіт за грантом), оскільки така плата становить близько 2-3 тисяч доларів. Серед найбільш відомих журналів, які стягують *APC*, – BioMed Central, Hindawi, Public Library of Science (PLOS).

Існують гібридні журнали відкритого доступу, які публікують як відкриті, так і закриті матеріали, доступні лише за передплатою. Така модель особливо вигідна видавцеві, оскільки, крім платежів за підписку, він отримує ще й плату за публікацію у відкритому доступі від автора.

Проблеми доступу до наукових знань. Причина проста: модель Open Access при традиційній схемі монетизації наукових журналів нівелює доходи видавця від продажу доступу до контенту, а для компенсації цих втрат потрібні істотні кошти. «Аналіз ринку наукової літератури та періодичних видань показав, що п'ять най-

більших видавничих будинків – Elsevier, Wiley, Taylor & Francis, Sage і Springer – сьогодні контролюють понад 50% наукових публікацій». За твердженням В. Ларив'єра (V.Lariviere) (Канада) [2], у всіх цих комерційних компаній величезні продажі і їх норма прибутку становить близько 40%.

Plan S. Для зміни ситуації, що склалась у науковій видавничій діяльності, Єврокомісія розробила так зв. Plan S[3]. Згідно «плану S», з 1 січня 2021 року всі результати досліджень, здійснених за рахунок бюджетних коштів або громадського фінансування, повинні бути опубліковані в журналах Open Access або на інформаційних платформах, що знаходяться у відкритому доступі.

Нарівні з ініціативою Єврокомісії, в мережі з'явився відкритий лист від вчених, які вважають подібний метод регулювання небезпечним для європейської науки [4]: вчені турбуються, що нові обмеження в рамках Plan S (якщо в складі бюджету дослідження були урядові гранти або гроші ЄС, то результати повинні публікуватися в безкоштовних для читачів журналах) скоротять для багатьох галузей науки вибір майданчиків для публікації на 80-90%. Тобто, поточна система публікації наукових робіт настільки щільно загрузла в моделі «за передплатою» (Paywall), що альтернативних безкоштовних журналів просто немає. Противники Plan S також наводять дані, що в коаліцію з безоплатного розповсюдження робіт входить всього 11 фондів, що підтримують безкоштовні журнали, а це всього від 3 до 4,1% світового ринку публікацій наукових робіт. У Plan S є тільки одна перевага – підтримка державних регуляторів, оскаржити рішення яких буде практично неможливо.

Політика сучасних наукових видань щодо закриття доступу до наукових публікацій пейволлом давно є причиною суперечок у науковому співтоваристві. З одного боку стверджується, що обмеження доступу до наукового знання – недозволено в умовах загальної вільної циркуляції інформації. З іншого боку зазначають, що інститут публікації, вичитки і рецензування наукових робіт професійними видавцями необхідний для того, щоб відсіювати нерелевантні, підтасовані і просто несправжні дослідження від

реальних наукових робіт. Журнали, що входять до бази даних Web of Science, Scopus і деякі інші, визнаються особливо якісними з наукової точки зору.

Надання вільного доступу до видання. Приклади ОА наукових журналів та видавництва [5].

Bio Med Central – видавництво у сфері науки, технологій та медицини, яке першим запровадило модель публікацій у відкритому доступі. Всі оригінальні дослідницькі (наукові) статті, опубліковані *Bio Med Central*, знаходяться у вільному доступі і викладаються в мережі Інтернет відразу ж після публікації.

Видавництво *Nature Publishing Group (NPG)*. У 2007 р. NPG упровадила ліцензії *Creative Commons Attribution Non Commercial – Share-Alike* для публікації тих статей в журналі *Nature*, які уперше описують основну послідовність геному організму.

Журнали відкритого доступу сімейства PLoS (Публічна бібліотека наукових видань – www.plos.org) випускаються вже більше 10 років і популярні в галузі медицини та біології. У рамках моделі відкритого доступу журнали Бібліотеки стали доступні в інтернеті без оплати за доступ і без обмежень на подальше поширення або використання, за умови зазначення автора і джерела, звідки взята цитата, що відповідає положенням відкритої, найбільш дозвоільної ліцензії *CCBY*, і які індексуються зовнішніми пошуковими системами. *PLoS* застосовує ліцензії *Creative Commons Attribution (CCBY)*.

Журнал відкритого доступу PeerJ (www.peerj.com), що має, на відміну від *PLoS*, іншу політику оплати – учений вносить абонентську плату (близько 500 доларів рік) за публікацію своїх статей.

На сайті визначено, які ліцензії відкритого доступу використовуються. Зазначено, що публікуються всі матеріали згідно з ліцензією *CCBY*. Той, хто використовує опублікований матеріал вдруге, повинен зазначити автора (авторів) і походження оригіналу, але може вільно повторно використовувати твір, як вважає за потрібне. Ця ліцензія має ознаки дійсно відкритого доступу.

Журнали видавництва Springer. Платформа *Springer Open* містить 195 рецензованих журналів повністю відкритого доступу,

що охоплюють усі галузі науки, техніки, медицини, гуманітарних і соціальних наук. Більшість журналів відкритого доступу мережі Springer публікують статті згідно з ліберальною ліцензією *Creative Commons Attribution 4.0* (CCBY). Ця ліцензія дозволяє необмежене використання, поширення і відтворення в будь-якому середовищі, за умови посилання на авторів і джерело походження, надання посилання на відповідні умови ліцензії Creative Commons, та визначення змін, які були вчинені.

Література

1. Neil J. Open Access: Key Strategic, Technical and Economic Aspects. Elsevier. 2006. P. 24–25; Suber P. OA journal business models [Електрон.ресурс]. URL: http://oad.simmons.edu/oadwiki/OA_journal_business_models
2. McGuigan G., Russell R. The Business of Academic Publishing: A Strategic Analysis of the Academic Journal Publishing Industry and its Impact on the Future of Scholarly Publishing // Electronic Journal of Academic and Special Librarianship. 2008.
3. Plan S. Making full and immediate Open Access a reality: <https://www.coalition-s.org/>
4. Plan S Open Letter. Reaction of Researchers to Plan S: Too Far, Too Risky: <https://sites.google.com/view/plansopenletter>
5. Капіца Ю.М, Шахбазян К.С. Застосування ліцензій відкритого доступу при розміщенні матеріалів наукових журналів в електронному середовищі // Наука України в світовому інформаційному просторі, № 13, 2016. – 62-70 р.

Бойко О.І.

студентка КПІ ім. Ігоря Сікорського

Костенко І.В.

кандидат юридичних наук, доцент

КПІ ім. Ігоря Сікорського

РЕКЛАМА ЯК ОБ'ЄКТ АВТОРСЬКОГО ПРАВА: ЮРИДИЧНИЙ АНАЛІЗ ЧЕРЕЗ ПРИЗМУ ВІТЧИЗНЯНОГО ЗАКОНОДАВСТВА

Можливість застосування інноваційних методик для популяризації продукції та послуг шляхом їх рекламування посилила у суб'єктів господарювання потребу в аналізі та переоцінці реклами як об'єкту авторського права. З одного боку, питання виникає відносно правового механізму наповнення контенту, що, як правило, включає в себе декілька видів об'єктів, котрі захищаються авторським правом, з іншого – яким чином в епоху розвитку Інтернету та ІТ – технологій легально захистити рекламу від посягань з боку інших суб'єктів.

Вільний та безкоштовний доступ до рекламного контенту, що розповсюджується в мережі Інтернет, формує уявлення про вільне використання певних його елементів. В певній мірі це може бути вірно, адже для віднесення реклами до об'єкту, що підлягає охороні з точки зору авторського права необхідно, щоб він відповідав двом ключовим вимогам: творчий характер та вираженість в об'єктивній формі.

Апелюючи до Закону України «Про авторське право і суміжні права» [3] та враховуючи положення Цивільного кодексу України [2] приходимо до висновку про те, що законодавець не визначає рекламу в якості самостійного об'єкту авторського права. Разом з цим, ст. 4 Закону України «Про рекламу» обмежується лише фразою про те, що використання у рекламі об'єктів авторського права і суміжних прав має здійснюватися відповідно до законодавства про авторське право та суміжні права [6]. Окрім зазначеного, ст. 9 Угоди про співробітництво держав – учасниць СНД у сфері регулювання рекламної діяльності [7] передбачено, що реклама пози-

ціонується як об'єкт авторського права як в її цілісному вигляді, так і в окремих частинах. Це логічно, адже рекламні матеріали наповнюються, як правило, різними об'єктами, що підлягають правовому захисту: зображення, створений дизайн, слоган, ілюстрація, торгова марка. Що стосується останнього аспекту, то його використання у рекламі може здійснюватися на підставі відповідного договору про співпрацю або спільне просування (стосується торгової марки третіх осіб). Зазвичай, така колаборація носить комерційний характер та спрямована на спільну популяризацію товару чи послуг різними суб'єктами господарювання. У випадку із рекламними відеороликами, що позиціонуються як складний, комплексний матеріал, в якому можуть бути присутні музичні композиції, елементи комп'ютерної графіки, відеоматеріали, спеціальний (розроблений) шрифт тексту тощо. Орім зазначеного, забороняється використовувати зображення фізичної особи, в тому числі її персональні дані без належної згоди такого суб'єкта.

Таким чином, перед публікацією рекламного матеріалу його варто піддати детальному юридичному аналізу на предмет відповідності законодавства про рекламу та охорони авторського права та суміжних прав. Деталізуємо ключові моменти, на які першочергово звертається увага:

- наявність у рекламодавця (чи відсутність) згоди від фізичної особи щодо права на використання її зображення (персональних даних) за умови, якщо такі об'єкти фігурують в рекламі;
- у випадку використання в рекламному матеріалі фотозображення, яке придбане з фотобанку, необхідно детально проаналізувати, на яких умовах (місце, територіальність, період використання; обмеження кількості друкованої продукції; розмір рекламного матеріалу; де можна використовувати фотозображення тощо) придбані права на використання цього фотозображення в рекламному матеріалі та чи можна його використовувати в комерційних, зокрема в рекламних, цілях;
- якщо у рекламі об'єктом виступає товар / послуги, який за законодавством підлягає ліцензуванню відповідно до ст. 7

Закону України «Про ліцензування видів господарської діяльності» (до прикладу, туроператорські послуги, ветеринарні препарати, лотерея, освітні заклади тощо) [5], доцільно переконатися у наявності такого документу дозвільного характеру у особи, яка замовляє / рекламує свою діяльність / продукцію та його дійсності. В протилежному випадку, – рекламувати даний об’єкт заборонено ст. 8 Закону України «Про рекламу» [6];

- встановити, чи не є зображення / відео – чи аудіофайл, текстова частина матеріалу зімітованою або скопійованою;
- переконатися у відсутності прив’язки ціни товару / послуги до іноземної валюти тощо.

Таким чином, законодавством визначено ряд вимог до реклами та встановлена заборона на запозичення вказаних матеріалів.

На захисті прав авторів реклами також перебуває Закон України «Про захист від недобросовісної конкуренції» [4], адже як правило, рекламують свою діяльність ті суб’єкти господарювання, котрі перебувають у конкурентних відносинах з іншими контрагентами. Зокрема, норми цього Закону застосовуються у випадку, коли один суб’єкт господарювання зімітував чи скопіював рекламу, творцем якої є інша сторона. Для того, щоб звернутись за захистом своїх авторських прав, за умови неправомірного використання належних йому рекламних матеріалів, до суб’єкта висувається ряд вимог: в першу чергу, він має виступати суб’єктом господарювання; між суб’єктами господарювання має бути конкуренція; реклама має використовуватись. Відповідно, за зверненням щодо захисту своїх авторських прав можуть апелювати одразу замовники реклами (фізична або юридична особа, яка рекламує свою діяльність чи послуги); а право інтелектуальної власності на об’єкт виникає у творця з моменту створення та вираження в об’єктивній формі.

З інтеграцією в більшість сфер суспільного життя інформаційно – комунікаційних платформ досить поширеним видом порушення авторських та суміжних прав (в тому числі, по відношенню до реклами) став плагіат – привласнення авторства на чужий твір або його запозичення без належного посилання. Дана проблема-

тика є досить поширеною на вітчизняних теренах, проте судова практика показує, що більшість судових справ стосуються оскарження рішень державних органів, задіяних у даній сфері (Держпродспоживслужба, Антимонопольний комітет).

Частково, вирішити проблематику та мінімізувати порушення авторських прав на рекламу могла б імплементація Директиви про авторське право та суміжні права на Єдиному цифровому ринку № 2019/790 [8], яка за своєю природою хоч і залишається суперечливою, але більшою мірою акумулює в собі значну кількість передових ідей та норм, що йдуть в ногу із технологічним прогресом. Разом з цим, Закон України «Про авторське право і суміжні права» варто доповнити переліком умов вільного використання творів у мережі Інтернет. Коректив потребує Закон України «Про рекламу», що регулюватиме відносини, які виникають у процесі виробництва, розповсюдження та споживання реклами, в тому числі, поширеної в мережі Інтернет. Удосконалення нормативно – правової бази має кореспондуватись із активною роботою у соціальній сфері, зокрема, доцільно проводити лекції та семінари, роз'яснюючи негативний вплив від посягань на об'єкти авторського права і суміжних прав в учбових закладах; підвищувати правову обізнаність громадян щодо захисту, охорони авторських і суміжних прав в мережі Інтернет та відповідальності за правопорушення в даній сфері.

Список використаних джерел:

1. Конституція України від 28 червня 1996. Відомості Верховної Ради України. 1996. № 30. Ст. 141.
2. Цивільний кодекс України від 16.01.2003 № 435-IV Відомості Верховної Ради України. 2003. № 40-44 URL: <http://zakon2.rada.gov.ua/laws/show/435-15>.
3. Про авторське право і суміжні права: Закон України від 23.12.1993 року № 3792-XXII. URL: <https://zakon.rada.gov.ua/laws/show/3792-12>.
4. Про захист недобросовісної конкуренції: Закон України від 07.06.1996 № 236/96-ВР URL: <http://zakon3.rada.gov.ua/laws/show/236/96-вр>.

5. Про ліцензування видів господарської діяльності : Закон України від 02.03.2015 №222-VIII. База даних «Законодавство України». URL: <http://zakon0.rada.gov.ua/laws/show/222-19>.

6. Закон України «Про рекламу» № 1121-IV від 11.07.2003 (Нова ред. із змінами, внесеними згідно із Законом № 270/96-ВР від 26.07.2018 р.): URL: <https://zakon.help/law/>.

7. Угода про співробітництво держав – учасниць СНД у сфері регулювання рекламної діяльності № 997_748 (затверджено Постановою КМ №1654 (1654-2004-п) від 13.12.2004) URL: https://zakon.rada.gov.ua/laws/show/997_748#Text.

8. The Digital Millennium Copyright Act of 1998. U.S. Copyright Office Summary. URL: www.copyright.gov/legislation/dmca.pdf.

Холдосенко А.В.

аспірант Харківського національного
університету внутрішніх справ

РЕКЛАМА ЯК ВАЖІЛЬ ВПЛИВУ НА СУСПІЛЬСТВО

Існування в інформаційному столітті вимагає просування та налагодження контактів зі споживачами як необхідного засобу у діяльності сучасних підприємств. Тому механізмом, який надає інформацію про особу чи товар, розповсюджену в будь-якій формі та в будь-який спосіб, і призначену сформувати чи підтримати обізнаність споживачів реклами та їх інтерес щодо таких особи чи товару, є реклама. [1, ст. 1]

Звичайно, реклама, яку ми бачимо сьогодні є модернізованою, котра пройшла доволі тривалий період розвитку та формування. Витоки свого становлення реклама черпає ще з часів Давнього Риму, Єгипту та Греції. Вихідні рекламні форми були усними і виглядали таким чином: глашатаї ходили по вулицях і викрикували різні розпорядження влади, а також, «комерційну інформацію», яка містила в собі повідомлення про продаж рабів, гладіаторські бої, роздачі хліба [2 с. 16].

Згодом, важливим етапом стало винахід друкарської машини (в середині XV ст.), що в свою чергу мало такі наслідки, як замі-

на усної реклами, на друковану. Спочатку це були просто певні тексти-оголошення, далі доповнені ілюстраціями (1839 р.), згодом було винайдено телеграф, який зруйнував територіальні межі рекламного простору (1844 р.) [2 с. 111]. Вагомим внеском в рекламну діяльність було виникнення газети (приблизно 1609 р.), яка користувалися попитом доволі тривалий час. І саме ці періоди становлення та розвитку, посприяли тому, що ми бачимо таку модернізовану рекламу в наш час.

Проте, крім позитивної складової реклама має іншу, негативну складову. Звісно при появі нового вагомого соціального явища, відбуваються й певні зловживання, які не залишаються осторонь. Одним з таких «зловживань» було розповсюдження реклами, яка вводила людей в оману. Так, на початку ХХ ст. прокотилася хвиля протестів проти реклами. І з того часу для реклами настав новий період, так званий «дослідницький», що надав рекламі наукового змісту, та призвів до закріплення та регулювання рекламних відносин в законодавстві країн [2, с. 3-18].

Метою будь-якої реклами є спонукання людини через її свідомість до здійснення певного вчинку, що полягає переважно в купівлі товару або послуги. Тобто реклама взаємопов'язана з пізнавальною діяльністю тих осіб, на кого безпосередньо спрямовується ця реклама. І ось під цим «спонуканням» криється величезна кількість психологічних прийомів, які інколи грають з особою в злий жарт. Більш детально зупинимось на деяких з них:

Гіпноз – це особлива форма сну, штучно викликана і яка впливаючи на свідомість особи, стимулює її на здійснення певних вчинків. Важливим моментом є те, що більшість науковців вважають, що гіпнозу можуть піддаватися не всі особи, а тільки певні, котрі мають властивості, необхідні для цього. І пов'язують це все з минулим досвідом конкретної людини.

Навіювання – є основним психологічним методом впливу, котрий застосовується в рекламі. Суть навіювання полягає у впливі на почуття людини, а через них – на її волю й розум. Сила впливу багато в чому залежить від наочності, доступності і логічності інформації, а також від авторитету особи, яка здійснює вплив. Ефект

особливо сильний тоді, коли те, що навіюється, в цілому відповідає потребам та інтересам того, на кого чиниться цей вплив.

Наслідкування – головним важелем тут є те, що рекламується те, що для людини престижним, що купується нею з метою бути схожим на відому, популярну, авторитетну особистість, відтворення особу чи товар особою рис та зразків поведінки, яка кимось спеціально демонструється.

Переконання як метод рекламного впливу полягає у тому, щоб за допомогою аргументації довести споживачу переваги даного товару і необхідність його придбання. Процес переконання споживача передбачає критичне осмислення отриманої рекламної інформації, її співвіднесення з попереднім власним життєвим досвідом. Особливість процесу переконання полягає у тому, що він спрямований на раціональну сферу свідомості потенційного покупця, тобто реклама звертається до його розуму.

Стереотип – спрощене, заздалегідь прийняте уявлення, що не впливає з власного досвіду. Ці спрощення суттєво впливають на сприйняття і розуміння явищ навколишньої дійсності, тобто мається на увазі, що людина обирає шаблонно думати, не приймати нічого нового.

Імідж – змістом цього явища є майстерність реклами під час створення ілюзії перетворення одних речей в інші. Таким чином, на будь-що можна надягнути будь-яку маску, зроблену на замовлення заінтересованих осіб.

Ідентифікація – це дієвий механізм, який надає можливість споживачу реклами пережити стан, в якому перебувають рекламні актори, тобто подумки ставити себе на місце персонажа в рекламі, і при цьому споживач реклами хоче бути на нього схожий.

Технологія «25-го кадру» – доволі цікавий феномен, свого плану ефект «дежавю», коли особі один раз показати якусь інформацію на короткий проміжок часу- ймовірність того, що інформація запам'ятається доволі невелика. А якщо інформація, подана повторно, багаторазово продемонстрована і буде цим ефектом, необхідним для реклами.

Рекламні шоу відрізняються від звичайної реклами тривалістю в часі – від 5 до 30 хвилин, місцем проведення – це спеціально оформлені телевізійні аудиторії, зі штучно створеною аудиторією, підібраними акторами-експертами, спостерігачами, глядачами. Найчастіше наприкінці рекламного шоу пропонується негайно подзвонити по телефону що добре запам'ятовується, одержати знижку і безкоштовну доставку[3, с. 34].

Аналізуючи всі ці механізми впливу на свідомість особи, можна замислитися про те, наскільки різноаспектними методами нами маніпулюють. І тут постає питання, чи можемо ми захиститися від всіх цих зовнішніх впливів.

Нормативне регулювання рекламних відносин в нашій державі здійснюється на трьох рівнях, що діють водночас та складають механізм правового регулювання цих відносин.

Первинним рівнем є саморегулювання, яке має на меті самостійне узгодження своїх дій учасниками рекламних відносин, намагаючись, не порушуючи інтересів інших учасників, забезпечити власні інтереси. Так, це дієвий механізм регулювання, адже в цих випадках учасники не залежать від уряду, більш швидко реагують на зміни, що відбуваються в рекламній діяльності, проте саморегулювання не в змозі виконати всі необхідні функції для забезпечення стабільності та контролю за запобіганням порушень інтересів інших учасників[4, с. 55].

Другим рівнем регулювання є рекламні асоціації, які розробляють стандарти рекламної діяльності, здійснюють контроль за діяльністю членів асоціацій, а також затверджують звичай ділового обороту у вигляді Кодексів рекламної практики, які мають за мету встановлення морально-етичних норм, правил ведення реклами та загально вимог до самого змісту реклами. Також асоціації можуть виконувати інформаційну функцію, надавати допомогу, проводити семінари, круглі столи та наукові дослідження.

Державне регулювання займає третій рівень в механізмі правового регулювання рекламних відносин. Воно здійснюється за допомогою норм різних галузей права, якими передбачені контроль та захист відносин у сфері рекламної діяльності. Контроль може

здійснюватися спеціально уповноваженими державними органами, які наділені правом самостійно застосовувати до порушників заходи державного примусу, якщо ж вони таким правом не наділені-звертатися до суду з відповідною вимогою. Закон надає пріоритет державному регулюванню реклами в Україні [1, ст. 3]; а за організаціями самоконтролю закріплено право на консультативну співпрацю з державними органами [1, ст. 29].

Пройшовши тривалий період розвитку, сучасна реклама є дієвим важелем не тільки розповсюдження інформації, але й механізмом спонукання осіб вчиняти певні дії різними психологічними засобами впливу. Для того, щоб захистити себе від цих впливів, крім того, що передбачене нормативне регулювання зі сторони держави, кожна особа повинна об'єктивно сприймати та аналізувати інформацію, яка до неї надходить.

Список використаної літератури

1. Закон України Про рекламу (Відомості Верховної Ради України (ВВР), 1996, № 39, ст. 181.
2. Ученова В.В. История рекламы. Детство и отрочество. / В.В. Ученова, Н.В. Старых. – М.: Смысл, 1994. – 96с.
3. Бутенко Н. Ю. Соціальна психологія в рекламі: Навч. посіб. – К.: КНЕУ, 2006. – 384 с. Електронний ресурс <http://ubooks.com.ua/books/00011/inx34.php>
4. Семенов Б.Д. Рекламный менеджмент/ Б.Д. Семенова. – Учебное пособие для студентов эконом. специальностей ВУЗов. – Мн., Эко-перспектива, 1999. – 268 с.

Бережницький Р.В.

студент КПП ім. Ігоря Сікорського

Науковий керівник: **Сторова В.С.**

к.ю.н., доцент КПП ім. Ігоря

Сікорського

ПРОБЛЕМАТИКА ПРАВОВОЇ ОХОРОНИ КОМП'ЮТЕРНОЇ ПРОГРАМИ В УКРАЇНІ

В сучасному світі ринкових відносин зараз відбувається швидке збільшення вагомості об'єктів інтелектуальної власності, яке в свою чергу робить з них цінні інвестиції і вигідний спосіб для отримання доходу. Внаслідок цього, на міжнародному рівні почався стрімкий розвиток права інтелектуальної власності. Охорона та захист прав на «інтелектуальні об'єкти» є однією з головних і найважливіших частин цього розвитку. Слід зазначити, що серед об'єктів інтелектуальної власності яскраво виділяється комп'ютерна програма, яка зараз стала одним із найцінніших ресурсів як держави в цілому, так і окремих суб'єктів. Постійне технологічне оновлення процесу створення так само, як і загальне розповсюдження і швидке поширення комп'ютерних програм, призвело до розширення сфери застосування цих об'єктів інтелектуальної власності, одночасно із цим зробиши їх частим об'єктом неправомірних посягань.

Мета дослідження цієї теми полягає у виконанні таких завдань: аналіз законодавчої бази та правозастосовного досвіду українського законодавства із точки зору можливості охорони комп'ютерної програми та її складових елементів нормами різних інститутів права інтелектуальної власності; розкриття правової природи охорони комп'ютерної програми як комплексного об'єкта інтелектуальної власності; порівняння існуючих методів захисту прав на комп'ютерну програму в Україні; визначення найоптимальнішого та найдієвішого способу захисту прав на комп'ютерну програму

Відповідно до статті 1 Закону України «Про авторське право і суміжні права»: «комп'ютерна програма – це набір інструкцій у

вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його у дію для досягнення певної мети або результату». Але такий підхід і таке визначення не є оптимальними для всіх громадян, тому що дискусії на тему коригування в законодавстві визначення «комп'ютерна програма» на більш нове і актуальне, як і перенесення програми до об'єктів промислової власності продовжуються.

Згідно з п. 4 ст. 433 Цивільного кодексу України та п. 5 ст. 15 Закону України «Про авторське право і суміжні права» та у відповідності до положень Бернської конвенції з охорони літературних і художніх творів, учасником якої є Україна – комп'ютерна програма визначається як об'єкт авторського права, тобто охороняється як твір літератури.

В момент створення комп'ютерної програми на неї виникає авторське право, яке не потребує додатково обов'язкової реєстрації. Однак, як показують численні рішення суддів, відсутність реєстрації, або наявність лише так званої «презумпції авторства» на комп'ютерну програму, не є достатньою правовою базою для захисту своїх прав. Через це, передбачаючи в майбутньому можливість порушення своїх авторських прав, автори комп'ютерних програм обирають варіант реєстрації своїх авторських прав в Державному реєстрі, що полягає в отриманні свідоцтва про реєстрацію об'єкта авторського права, який в свою чергу надає їм ряд переваг. Серед них варто виокремити наступні: документально засвідчене право власності на об'єкт авторського права, можливість підтвердження цього права у разі неправомірного посягання на нього; змога внести об'єкт авторських прав до статутного капіталу підприємства; спрощена процедура, пов'язана з розпорядженням майновими правами, такими як передача права власності або надання третім особам права на використання об'єкта авторського права; можливість отримання авторських прав у спадок.

Однак в той же час, більшість авторів комп'ютерних програм не користуються можливістю отримання цих переваг, звертаючись до Державного підприємства «Український інститут ін-

телектуальної власності» із заявою про отримання свідоцтва на об'єкт авторського права. Це можна пояснити розповсюдженою у суспільстві легковажною впевненістю в «презумпції авторства», але зважаючи на судову практику, розраховувати на неї стовідсотково не можна [1. Справа № 6-40849св14]. Тому для тих авторів комп'ютерних програм, які не вважають за необхідне реєструвати свої авторські права, буде доцільним прислухатись до думки Селіванова М.В., який рекомендує записати ім'я та ініціали автора програми в її коді, зображеннях в середині програми та її упаковці [2, с. 197-200], задля збільшення шансів захистити свої авторські права в майбутньому.

Проте, незважаючи на велику кількість плюсів реєстрації комп'ютерної програми як об'єкта авторського права, цей метод охорони права має свій недолік, а саме охорона авторським правом лише форми об'єкта і способу втілення ідеї програми, захист лише від повного копіювання програми і її коду, залишаючи без захисту саму ідею програми (її зміст, те, для чого вона призначена), її алгоритм та функції [3, п. 3. ст. 8]. У відповідності до п.3 ст. 8 Закону України «Про авторське право і суміжні права»: «правова охорона поширюється тільки на форму вираження твору і не поширюється на будь-які ідеї, теорії, принципи, методи, процедури, процеси, системи, способи, концепції, відкриття, навіть якщо вони виражені, описані, пояснені, проілюстровані у творі». Тобто, змінивши тільки зовнішній вигляд програми, її візуальну частину, залишивши без змін її ідею та суть можна отримати цілком інший об'єкт авторського права. Все це робить ринок комп'ютерних програм перенасиченим плагіатом та продукцією з низькою якістю.

Зважаючи на недоліки охорони комп'ютерної програми як об'єкта авторського права, кращим варіантом може виступити патентування комп'ютерної програми. І хоча на даний час програмні продукти не можна віднести до винаходів, тим самим роблячи неможливим їх патентування в даний спосіб, все ж залишається можливість отримати патент на алгоритм програми, а саме як на певний спосіб вирішення конкретних завдань.

Процес патентування алгоритму комп'ютерної програми полягає в записі алгоритму, його суті і етапів, у зрозумілу словесну форму, яка доповнюється блок-схемами і діаграмами. Перевагою такого способу патентування є те, що охорона та захист будуть розповсюджуватись саме на функцію і алгоритм програми, тобто на її принципи і методи вирішення поставлених задач. Це означає, що незалежно від мови програмування чи зовнішнього вигляду та оформлення програми, якщо її функції та алгоритм вирішення задач будуть такими самими, як і в запатентованій, то вона буде порушувати патент. В патентній охороні є також і ряд недоліків. По перше – процедура отримання патенту є складною і тривалою по часу [4, розділ IV], по друге – отримання патенту дороге коштує, особливо, якщо патент необхідно отримати не тільки для України. По третє – відсутність стовідсоткової гарантії отримання патенту, оскільки не кожна комп'ютерна програма, у вигляді алгоритму, відповідає критеріям патентоспроможності [5, Ст. 7].

Способом вирішення досліджуваної проблеми, на нашу думку, є одночасне поєднання всіх наведених підходів правової охорони комп'ютерної програми, задля взаємного перекриття мінусів і недоліків кожного з підходів. Прикладом такого способу може слугувати американська модель «пакетної реєстрації», яка працює за принципом «Парасольки» і дозволяє відразу зі створенням нового об'єкту – комп'ютерної програми – максимально забезпечити охорону прав інтелектуальної власності на останню, отримавши на неї свідоцтво про авторське право, патент та свідоцтво на знак для товарів і послуг для назви [6, с. 27-28]. Даний спосіб дозволить комплексно захистити комп'ютерну програму та запобігти неправомірному посяганню на права власника.

Підбиваючи підсумок, варто сказати, що попри достатнє законодавче закріплення правового статусу комп'ютерної програми як об'єкта інтелектуальної власності, способи його правової охорони в Україні викликають сумніви. Комп'ютерна програма віднесена до об'єктів авторського права, а саме нормативно закріплена як літературний твір, для прав на який не передбачено обов'язкової державної реєстрації. Однак, як показує судова практика, такий

статус комп'ютерної програми не забезпечує її належного захисту. Адже, частими є випадки порушення зловмисниками авторського права автора комп'ютерної програми, що знехтував отриманням свідоцтва, в силу того, що «презумпція авторства» дозволяє йому не витратити час на те, щоб зареєструвати своє авторське право. В той же час, єдиною альтернативою до одностороннього «авторського підходу» по охороні прав на комп'ютерну програму, який захищає зовнішню форму вираження програми, забуваючи про її ідею та функцію, може виступати лише дороге, довготривале і не загальнодоступне патентування, яке до всього іншого ще й не розглядає комп'ютерну програму як цілісний об'єкт, не надаючи їй статусу винаходу, а працює лише з її частиною, у вигляді алгоритму. Я вважаю, що гармонічне поєднання обох підходів забезпечить надійний захист прав на комп'ютерну програму.

Список використаних джерел:

1. Парінова І.К., Ступак О.В., Штелих С.П., Колегія суддів судової палати у цивільних справах Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ, Справа № 6-40849св14, 22.01.2015 року м. Київ
2. Селіванов М.В. Правові підстави та докази визнання права на комп'ютерну програму //Вісник Університету внутрішніх справ. –2000. –Спецвипуск. –С.197-200.
3. Закон України «Про авторське право і суміжні права», Документ 3792-ХІІ, чинний, поточна редакція – Редакція від 04.11.2018, підстава – 2581-VIII – Пункт 3 стаття 8.
4. Закон України Про охорону прав на винаходи і корисні моделі Документ 3687-ХІІ, чинний, поточна редакція – Редакція від 05.12.2012, підстава – 5460-VI – розділ IV.
5. Закон України Про охорону прав на винаходи і корисні моделі Документ 3687-ХІІ, чинний, поточна редакція – Редакція від 05.12.2012, підстава – 5460-VI – стаття 7.
6. Петренко І.І. ОСОБЛИВОСТІ РЕЄСТРАЦІЇ АВТОРСЬКОГО ПРАВА В УКРАЇНІ ТА ІНШИХ КРАЇНАХ СВІТУ// Теорія і практика інтелектуальної власності. –2019. –С.27-28.

Васько В.А.

аспірант НДІ інформатики і права
НАПрН України

**ПРОБЛЕМА ВИЗНАЧЕННЯ ЗМІСТУ ЮРИДИЧНОЇ
ВІДПОВІДАЛЬНОСТІ РОЗРОБНИКІВ ВІДКРИТОГО
ВИХІДНОГО ПРОГРАМНОГО КОДУ
БЛОКЧЕЙН-ПРОЄКТІВ**

Останнім часом технологія розподіленого розташування інформації (далі – DLT) привертає до себе все більшої уваги. На початковому етапі застосування цієї технології остання прирівнювалась виключно до криптовалют, проте на сьогодні технологія блокчейн вийшла за їх рамки, і тепер її застосування можливе у сфері публічного управління та майже у всіх складових елементах фінансової системи (торгівля, глобальні платежі, кліринг, залучення капіталу, депозити і кредитування, страхування та ін. вже отримали ряд переваг за рахунок DLT).

Проте, коли між сторонами договору утворюються транзакційні зв'язки за допомогою технології блокчейн, то часто вони можуть перебувати у таких відносинах, які не визначені та не регулюються на законодавчому рівні. А відтак виникає одна із основних правових проблем застосування DLT – проблема визначення змісту юридичної відповідальності суб'єктів, які використовують блокчейн.

Будь-яка правова норма, переважно завжди складається із прав, обов'язків та встановлення заборон на вчинення чітко визначених дій (в окремих випадках бездіяльності) і встановлює відповідальність для осіб, які їх недотримуються. Основною метою встановлення відповідальності – є прагнення законодавця стабілізувати суспільні відносини. Для того щоб встановити зміст юридичної відповідальності у відносинах, що виникають під час застосування технології блокчейн, необхідно у першу чергу розуміти, які суб'єкти беруть у них участь, які для них відведені ролі в цьому доволі складному технологічному процесі, і як вони можуть впливати на інших учасників цих відносин.

У цьому дослідженні всі ці проблеми ми розглянемо на прикладі криптовалют – найбільш поширеному на сьогодні зразку застосування технології блокчейн. Таким чином, ми будемо досліджувати саме публічний (відкритий) блокчейн, а не приватний (закритий), там де визначення змісту правової відповідальності зазвичай є менш складним, враховуючи особливості цієї технології.

Для реалізації поставленої мети, нам у першу чергу необхідно встановити межі відповідальності розробників відкритого програмного забезпечення блокчейну, оскільки на перший погляд їх роль у розробці програмного коду та обслуговуванні блокчейн-платформ встановлює для них певні обов'язки, за невиконання або неналежне виконання, яких може наставати юридична відповідальність.

Головна задача розробників блокчейн-проектів – це написання вихідного відкритого програмного коду на основі якого створюється програмне забезпечення для функціонування самого блокчейну. Іншими словами, розробники пишуть код програмного забезпечення, який забезпечує злагоджену роботу комп'ютерів учасників блокчейну [1]. Оскільки, по-суті це єдина функція розробників, то в наукових колах виникла дискусія стосовно того, чи взагалі є обов'язки у останніх, особливо у розробників децентралізованих сервер-клієнтських додатків (англ. decentralized applications) та загальнодоступних протоколів публічних блокчейн-проектів[2].

Враховуючи керівні принципи роботи блокчейн технології та її особливу програмну архітектуру виникають абсолютно логічні запитання:

1. Чи повинні розробники нести відповідальність, у тому випадку, якщо створений ними відкритий програмний код використовується для відверто незаконних цілей?
2. Чи повинні розробники нести відповідальність за те, що у створеному ними відкритому коді відсутня можливість для запобігання такій незаконній діяльності?

Перед тим як надати відповіді на ці питання, необхідно відзначити, що переважно завжди розробники ліцензують вихідний програмний код свого продукту на певних умовах. Коли користувачі починають його використовувати, то зазвичай приймають умови

ліцензії не читаючи її. Наприклад, розробники найпопулярнішої на сьогодні криптовалюти Bitcoin ліцензували своє програмне забезпечення однією із найуживаніших ліцензій для ПЗ з відкритим кодом – MIT (яка містить застереження про відсутність відповідальності розробників такого ПЗ) [3]. Таким чином, у даному випадку враховуючи відкритість вихідного коду Bitcoin, саме у користувачів з'являється обов'язок вивчити останній перед його запуском, але на практиці це майже ніхто не робить.

Отже, відповідаючи на питання зазначені вище, ми стоїмо на позиції, що притягувати розробників блокчейн-проектів до відповідальності за будь-яке незаконне використання ПЗ із відкритим вихідним програмним кодом не можна, оскільки розумно передбачити з якою ціллю (законною чи навпаки) буде використовуватись блокчейн – не можливо. Такої ж думки притримується і комісар Комісії з торгівлі товарними ф'ючерсами США (англ. Commodity Futures Trading Commission; CFTC) Брайан Д. Квінтенц, у своїй доповіді на 38-й щорічній конференції GITECH Technology Week він говорить: «Здається нерозумним притягати до відповідальності розробників за кожний додаток, що використовує базову технологію блокчейна для незаконних цілей... Точно так самозвичайні користувачі блокчейна не можуть знати і оцінювати законність кожного конкретного додатку в блокчейні»[4].

Однак це лише перший і найпростіший варіант встановлення змісту юридичної відповідальності розробників відкритого вихідного програмного коду блокчейну. Тепер давайте розглянемо інший, більш складний варіант, і поставимо такі питання:

1. Чи повинні розробники нести відповідальність за навмисно хибний вихідний відкритий програмний код, який запрограмований на те, щоб криптовалютні вузли несправедливо перерозподіляли активи між користувачами блокчейну?

2. Чи повинні розробники нести відповідальність за помилки у вихідному відкритому програмному коді, якщо вони призводять до втрати криптовалюти?

Для того, щоб дати відповідь на перше питання, нам необхідно розуміти, що дані та записи, які зберігаються в блокчейні, ві-

докремлені від вихідного програмного коду ПЗ, яке безпосередньо керує блокчейном. Наприклад, у Bitcoin можна завантажити окремо копію блокчейна і окремо копію вихідного відкритого програмного коду. Таким чином, можна змінити початковий вихідний програмний код та створити нову версію блокчейна за рахунок попередньо завантаженої копії. Для того щоб, такий варіант блокчейну запрацював, необхідно переконати достатню кількість людей переключитись на оновлену версію вихідного програмного коду та таку ж копію блокчейну. З моменту першої транзакції, керованої альтернативним вихідним кодом усі наступні транзакції потрапляють в різні гілки блокчейна, оскільки з одного боку ПЗ кожної з гілок працює з попередніми форматами блоків, але з іншого – відхиляють нові формати один одного (існують паралельно) [5]. Одним із прикладів цього процесу можна назвати «хардфорк» Bitcoin, який відбувся 1 серпня 2017 року, внаслідок якого із цієї криптовалюти виділилась нова криптовалюта під назвою Bitcoin Cash [6].

Проте цей приклад не дає відповіді на наше питання, оскільки мотиви цього «хардфорку» були зовсім іншими, розробляючи новий програмний код Bitcoin його учасники та розробники хотіли покращити роботу цього блокчейн-проекту. Нас же цікавить ситуація, коли розробники мають протилежні цілі. Очевидно, що за такого розвитку подій, очікуваний користувачами блокчейну результат не настане, а відтак можна вважати, що відповідальними за це будуть розробники відкритого вихідного коду блокчейн-проектів. Але, на нашу думку це не зовсім так, оскільки хибний для користувачів блокчейну програмний код завідомо не означає власне програмну помилку, оскільки код буде виконаний так, як він написаний, «код – це закон» [7]. Це твердження відсилає нас до наших попередніх висновків, що саме у користувачів з'являється обов'язок вивчити вихідний програмний код перед його запуском, або прийняттям пропозиції оновлення чи «хардфорку» для уникнення небажаних наслідків.

Ще більш складним видається надати відповідь на друге питання. 20 вересня 2018 року в мережі Bitcoin була знайдена критична

помилка CVE–2018–17144 [8], яка могла закрити найпопулярнішу криптовалюту в світі. Якби її вчасно не виявили і не виправили, то користувачі цієї мережі втратили б свої активи. Гіпотетично уявимо, що це сталось, хто буде відповідальним за збитки, які понесуть користувачі цього блокчейн-проєкту та інвестори? Очевидно, що розробники вихідного відкритого програмного коду, якщо останні не обмежили свою відповідальність, але як встановити саме того розробника, який під час оновлення допустив можливість виникнення такої помилки. У наведеному нами прикладі вину на себе взяв розробник Bitcoin Core Джон Ньюбері, проте учасники Bitcoin мережі не погодились із його рішенням і заявили, що винними є й інші розробники у т.ч. розробники алгоритму The Fast Internet Bitcoin Relay Engine (FIBRE) [9]. Таким чином, враховуючи особливості технології блокчейн, встановити реальних винуватців таких помилок, а відтак притягти останніх до правової відповідальності є надзвичайно складно.

Поступово ми дійшли до останнього, третього можливого варіанту визначення змісту юридичної відповідальності розробників відкритого вихідного коду блокчейн додатків. За яким варто розглянути можливість притягнення до відповідальності розробників ПЗ, які одночасно ще й є засновниками бізнес-проєктів на основі блокчейну. Зазвичай такі розробники випускають криптоактиви у вигляді токенів і залишають за собою право власності на їх певну кількість. Вигоду вони отримують тоді, коли їхнім ПЗ починає користуватись значна кількість людей у результаті чого збільшується вартість таких токенів [10]. У такому випадку сфера відповідальності підприємців-розробників значно розширюється, оскільки останні розумно передбачають із якою ціллю створюють своє ПЗ та яким чином його підтримують. Історія знає вже не один приклад притягнення таких розробників до цивільної, а в окремих випадках і до кримінальної відповідальності [11, 12]. Проте з іншого боку розробник і засновник підприємницького блокчейн-проєкту на відкритому коді, може повністю або частково втрати контроль над діяльністю свого проєкту (згадаємо приклад із BitcoinCash), і тоді ми повертаємось до першого питання другого варіанту визначення змісту юридичної відповідальності наведеного вище. На

сьогоднішній день, на практиці дуже складно встановити, коли засновник або співзасновники блокчейн-проектів, котрі здійснювали управління ними на початковому етапі втрачають його та перестають нести відповідальність.

Отже, враховуючи вище названі моделі визначення змісту юридичної відповідальності розробників відкритого вихідного коду можна дійти висновку, що притягнути останніх до відповідальності на відміну від інших учасників блокчейну можна лише в одичних випадках.

Система правового регулювання застосування технології блокчейн тільки зараз поступово починає вибудовуватись. Для того щоб встановити межі правової відповідальності користувачів технології блокчейн, на правовому рівні необхідно дійти до консенсусу відносно їх прав та обов'язків у відносинах один з одним.

Для уникнення проблем зазначених у другому та третьому варіантах розробникам необхідно спробувати розробити алгоритм який зможе фіксувати хто, коли і як вносив зміни у програмний код блокчейну, хоча враховуючи особливості цієї технології – це не видається можливим, але з іншого боку, колись і створення самого блокчейну видавалось неможливим.

Список використаної літератури

1. Kit J. Blockchain Developer. URL: <https://cdn2.hubspot.net/hubfs/4795067/Blockchain%20Job%20Kit/Blockchain-Developer-Job-Kit.pdf>
2. De Filippi P., Wright A. Blockchain and the Law: The Rule of Code. Cambridge: Harvard University Press, 2018. 250 p.
3. Bitcoin is license dunder the MIT License. URL: <https://github.com/bitcoin/bitcoin/blob/master/COPYING>
4. Remarks of Commissioner Brian D. Quintenz at the 38th Annual GITEX Technology Week Conference. URL: <https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz16>
5. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. URL: <https://bitcoin.org/bitcoin.pdf>
6. Yongdae K. Bitcoin vs. Bitcoin Cash: Coexistence or Down fall of Bitcoin Cash? URL: https://www.researchgate.net/publication/331429454_Bitcoin_vs_Bitcoin_Cash_Coexistence_or_Downfall_of_Bitcoin_Cash

7. Блокчейн на пике хайпа: правовые риски и возможности: текст / А. Ю. Иванов (рук. авт. колл.), М. Л. Башкатов, Е. В. Галкова и др.; Нац. исслед. ун-т «Высшая школа экономики», Ин-т права и развития ВШЭ – Сколково. – М.: Изд. Дом Высшей школы экономики, 2017. 237 с.

8. Bitcoin Core CVE-2018-17144 vulnerability research and analysis. URL: <https://www.programmersought.com/article/3673158851/>

9. Bitcoin Cash Developer Shares Method of Finding the Scary BTC Blockchain Bug. URL: <https://bitcoinexchangeguide.com/bitcoin-cash-developer-shares-method-of-finding-the-scary-btc-blockchain-bug/>

10. HackerP., Thomale C. Crypto-Securities Regulation: ICOs, Token Sales and Crypto currencies under EU Financial Law. 15 European Company and Financial Law Review, 2018. P. 645-696. URL: <https://ssrn.com/abstract=3075820>

11. U.S. District Court Eastern District of New York USA v. Zaslavskiy, No. 17-CR-647 (EDNY). URL: <https://ru.scribd.com/document/388358607/USA-vs-Zaslavskiy>

12. U.S. District Court for the Southern District of Florida C.A. No. 1:17-cv-24500-JLK/Simonton. URL: http://securities.stanford.edu/filings-documents/1064/CTI00_03/2018109_r01c_17CV24500.pdf

Касперович О.Ю.

головний економіст Інституту
економіки промисловості НАН
України

ПІДВИЩЕННЯ СТІЙКОСТІ СФЕРИ ПРАЦІ ТА ЗАЙНЯТОСТІ В УМОВАХ ПАНДЕМІЇ COVID-19 ЧЕРЕЗ ЗАЛУЧЕННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ: НАПРЯМИ УДОСКОНАЛЕННЯ РЕГУЛЯТОРНОЇ ПОЛІТИКИ

Ситуація в економіці, в сфері праці та зайнятості України в умовах впливу пандемії COVID-19 є складною та неоднозначною. Українська економіка, потерпаючи від негативних наслідків впливу пандемії COVID-19, має серйозні проблеми щодо забезпечення умов для гідної праці, які виникли задовго до пандемії COVID-19. Країна тривалий час перебуває в стані значних дисбалансів у сфері праці та зайнятості, за умов відсутності стратегічної виваженої

політики щодо забезпечення продуктивної зайнятості, збалансування попиту та пропозиції на національному та регіональних ринках праці, погіршення якості та скорочення робочих місць. Серйозні ризики втрати існуючих робочих місць, скорочення рівня зайнятості, зростання рівня бідності, дискримінації та нерівності українських громадян в доступі до освіти та гідної зайнятості, незалежно від віку або статі, стану здоров'я [1], стали системними задовго до пандемії COVID-19. Але вплив пандемії загострив існуючі проблеми, що знайшло свій прояв у загрозливому характері безробіття, поширенні нестійкої зайнятості, збереженні виплат заробітної плати на рівні мінімальної, ослабленні колективно-договірного регулювання соціально-трудова відносин, незахищеності працівників на робочому місці. В умовах впливу пандемії COVID-19 дефіцит гідної праці буде тільки посилюватися [2].

В цих умовах особливої актуальності набуває потреба у визначенні, розробці та реалізації відповідної національної та регіональної політики, спрямованої на забезпечення якісного та ефективного управління соціально-трудова сферою в умовах пандемії COVID-19, що має стабілізувати ситуацію в сфері праці та зайнятості та суттєво підвищити її стійкість до форс-мажорних ситуацій, подібних до пандемії COVID-19. Відповідно, пошук механізмів забезпечення такої стійкості стає пріоритетним завданням та необхідною умовою відновлення сфери праці та зайнятості. Яскравим феноменом, безпосередньо пов'язаним із впливом пандемії COVID-19 та пов'язаних з нею жорстких карантинних обмежень, став бурхливий розвиток дистанційної зайнятості, який певним чином дозволив компенсувати вплив цих обмежень та виявив значний потенціал використання цифрових технологій щодо забезпечення тривалого та стійкого функціонування сфери зайнятості та економіки цілому в умовах карантину. Тож не буде перебільшенням зазначити, що ефективність державної політики України щодо протидії негативним наслідкам пандемії в сфері праці та зайнятості в значній мірі залежатиме від ступеню цифровізації соціально-економічного життя та залучення потенціалу сучасних цифрових технологій.

Зважаючи на надзвичайну швидкість та – одночасно – складність процесів, що відбуваються в сфері праці та зайнятості України, необхідним є забезпечення координації, комплексності та інституціоналізації державного управління щодо залучення ресурсів цифровізації до відновлення та подальшого забезпечення стійкості сфери праці та зайнятості до форс-мажорних обставин, подібних до пандемії COVID-19,

Таким чином, розумна та збалансована цифрова трансформація економіки та суспільства не просто сприятиме стабілізації та відновленню сфери праці та зайнятості в світі та в Україні, а є необхідною умовою її подальшого розвитку. Залучення потенціалу цифрових технологій дозволить суттєво знизити негативні соціально-економічні наслідки впливу пандемії на глобальний та національні ринки праці, долати обмеження в процесі взаємодії ключових суб'єктів суспільних та соціально-трудових відносин для ефективного узгодженого реагування, створювати сприятливі умови для поширення дистанційної роботи та інших гнучких форм зайнятості, а також більш ефективно дотримуватись міжнародних трудових норм і рекомендацій при підтримці життєдіяльності підприємств і бізнесу, забезпеченні захисту і безпеки працівників у форс-мажорних обставинах.

В той же час очевидно, що залучення потенціалу цифровізації задля стабілізації сфери праці та зайнятості та підвищення її стійкості потребує відповідного та негайного удосконалення державної регуляторної політики в цій сфері.

При удосконаленні державної регуляторної політики необхідно мати на увазі, що протидія ризикам та загрозам пандемії COVID-19 в сфері праці та зайнятості має два аспекти: оперативний (необхідність терміново вирішувати найгостріші проблеми, так би мовити, в режимі «гасіння пожежі») та стратегічний (пов'язаний із передбаченням довгострокових наслідків пандемії та відповідним реагуванням на них). Потрясіння сфери праці та зайнятості, які спричинила пандемія COVID-19, засвідчили її вразливість до форс-мажору. Тож базовим принципом щодо всієї системи діяльності (та, зокрема, відповідної регуляторної політики), спрямо-

ваної на відновлення сфери праці та зайнятості, повинно стати забезпечення тривалого та стійкого функціонування економіки в умовах обмежувальних заходів, здатного підтримувати критичну локальну інфраструктуру, забезпечувати безпечне консервування тимчасово зупинених секторів, сприяти розвитку секторів, які можуть розвиватись в умовах обмежувальних заходів тощо, та, в якості обов'язкової умови реалізації зазначеного імперативу – формування та розвиток оновленого, більш стійкого середовища взаємодії суб'єктів сфери праці та зайнятості в новітніх умовах.

У зазначеному контексті одним з першочергових завдань щодо удосконалення державної регуляторної політики є забезпечення координації, комплексності та інституціоналізації державного управління щодо залучення ресурсів цифровізації до сталого відновлення сфери праці та зайнятості, та підвищення її стійкості до форс-мажорних обставин, подібних до пандемії COVID-19, в першу чергу – шляхом всебічного стимулювання розвитку «Індустрії 4.0», створення відповідних механізмів нормативно-правового та організаційно-управлінського забезпечення, впровадження технологій дистанційної роботи, розвитку систем електронного урядування та надання адміністративних он-лайн послуг населенню тощо.

Важливим напрямом удосконалення регуляторної політики з метою забезпечення стійкості сфери праці та зайнятості у форс-мажорних обставинах, спричинених пандемією COVID-19, є підтримка та всебічне сприяння розвитку платформної економіки. Сучасні цифрові та інформаційно-комунікаційні технології вже створили необхідний фундамент для цифрових платформ, нові бізнес-моделі та соціально-поведінкові трансформації стимулювали попит, а пандемія COVID-19 ще більше його актуалізувала. В першу чергу необхідно здійснити термінологічне та нормативно-правове визначення понять “платформної економіки”, “трудової платформи”, “платформної зайнятості”. Доцільним також є проведення спеціальних досліджень, які мають бути спрямовані на аналіз типів платформ, а також передбачати цикл обстежень за репрезентативною вибіркою для визначення загальних масштабів

явища – з метою подальшого удосконалення нормативно-правового, управлінського, організаційного та іншого забезпечення розвитку платформної економіки.

Окремим та вкрай важливим напрямом удосконалення державної регуляторної політики має стати створення сприятливих умов для діяльності щодо посилення захисту працівників на робочому місці. Зокрема, мова йде про створення сприятливих умов для впровадження смарт-технологій, технологій оптимізації виробничих процесів в напрямі мінімізації безпосередніх контактів між працівниками та розширення можливостей дистанційної та ізольованої роботи в умовах карантинних обмежень, радикальне підвищення епідеміологічної захищеності робочих місць у тих випадках (професіях), коли дистанційна робота є неможливою – через відповідне удосконалення технологій та реінжиніринг бізнес-процесів, проведення наукових досліджень та реалізація інноваційних проєктів, що спрямовані на запобігання поширенню COVID-19, на використання цифрових технологій в боротьбі з пандемією.

При цьому необхідною умовою формування ефективної та адекватної регуляторної політики в сфері праці та зайнятості є впровадження моніторингової оцінки структурних зрушень у сфері праці та зайнятості, їх наслідків (ризиків, небезпек та – одночасно – можливостей) в умовах впливу пандемії COVID-19 з метою збереження трудового потенціалу та людського капіталу, захисту прав людини праці, зниження конфліктної напруженості в українському суспільстві. Такі оцінки виступають науковим обґрунтуванням ефективних управлінських рішень щодо попередження прояву ризиків і небезпек та своєчасної мінімізації їх негативних наслідків [3, с. 9], в тому числі – через залучення потенціалу сучасних цифрових технологій.

Література

1. Костриця В.І., Бурлай Т.В. Дисбаланси і дивергенція у сфері зайнятості: підходи ЄС та України до їх подолання // Український соціум. – 2020. – №1. – С. 83-109. URL: <https://doi.org/10.15407/socium2020.01.083>

2. Колот А., Герасименко О. Сфера праці в умовах глобальної соціо-економічної реальності 2020: виклики для України. / Фонд ім. Фрідріха Еберта. Київ, 2020. – 36 с. URL: <http://library.fes.de/pdf-files/bueros/ukraine/16344.pdf>

3. Novikova O., Shamileva L. Evaluation of social and economic insecurity risks for employees during structural transformations in the modern labor market. Social and labour relations: theory and practice, 2020. Vol. 10, Iss. 1, pp. 1-10. URL: [http://dx.doi.org/10.21511/slrrp.10\(1\).2020.01](http://dx.doi.org/10.21511/slrrp.10(1).2020.01)

Рашевська К.Є.

молодший науковий співробітник,
аспірантка Інституту міжнародних
відносин Київського національного
університету імені Тараса Шевченка

ІНТЕГРАЦІЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ У ТРАДИЦІЙНІ МЕХАНІЗМИ ВИРІШЕННЯ МІЖНАРОДНИХ ТОРГОВЕЛЬНИХ СПОРІВ

13 грудня 2016 року Генеральна Асамблея ООН прийняла резолюцію A/RES/71/138, поклавши початок розробці технічних рекомендацій ЮНСІТРАЛ щодо врегулювання спорів онлайн[1]. Однак, проблема використання інформаційно-комунікаційних технологій (ІКТ) у даній сфері вже давно привертає увагу як окремих держав, так і міжнародного співтовариства в цілому. Актуальна вона і для юридичної науки, про що свідчать сформовані на сьогодні окремі групи вчених «за інтересами»: одні з них досліджують існуючі національні механізми посередництва та арбітражу в Інтернеті, намагаючись запропонувати нову модель врегулювання спорів, інші – зосереджують свою увагу лише на вивченні транскордонної електронної торгівлі та оптимальних для неї способів онлайн-судочинства[2]. Попит на теоретичні розробки в даній сфері створюють і сучасні епідеміологічні реалії, які додають до проблем, пов'язаних із визначенням юрисдикції, вартістю та тривалістю, також тимчасові обмеження на рух через державні кордони та необхідність перенесення

більшості процесуальних стадій розгляду торговельних спорів у дистанційний формат.

Механізм вирішення спорів онлайн – це новий тип врегулювання спорів, який відповідно до визначення ЮНСІТРАЛ охоплює широкий спектр підходів і форм: консультації, переговори, примирення, посередництво, спрощене врегулювання, арбітраж, судовий розгляд, а також гібридні процеси, що включають як онлайн, так і офлайн елементи [3]. Наприклад, у США функціонує арбітражна платформа, яка займається питаннями інвестиційної безпеки. Для захисту своїх прав та інтересів сторони можуть скористатися платформою для подання заяви на проведення онлайн-арбітражу. І хоча судовий процес в мережі є більш складним як з точки зору технічної організації, так і правової регламентації розгляду, він не тільки дешевший і швидший, але й допомагає розвантажити традиційну судову систему. Серед інших переваг: необмеженість географічним положенням, спроможність врегулювання спорів між різними юрисдикціями та в будь-якому місці, можливість заощадити на операційних витратах (транспорт, проживання, харчування представників сторін), порівняно більша ефективність, гнучкість та простота через відсутність формальних вимог, закріплених у процесуальних кодексах, швидкість комунікації між сторонами та розгляду в цілому, більший потенціал забезпечення одноманітності судової практики [2].

Очевидно, що, окрім переваг, на сьогодні існує також низка недоліків даного механізму врегулювання торговельних спорів. Незважаючи на те, що сама ідея з'явилася вже давно, її реалізація відбувається повільно. На національному рівні необхідне нормативне забезпечення розробляється з початку ХХІ століття, однак, переважно, розвиненими державами (ЄС, США, Японія, Канада, Австралія). У свою чергу, в Китаї, для якого використання ІКТ в судочинстві є особливо актуальним з погляду на розмір та фізичні характеристики території, чисельність населення та першість у сфері електронної комерції, хоча *defacto* з 2004 року й існує врегулювання торговельних спорів між індивідами онлайн, однак станом на 2020 рік досі не розроблено спеціальних норма-

тивних актів, які б регулювали режим та процесуальні питання цього механізму [4]. Окрім того, використання ІКТ у судочинстві та в альтернативних методах врегулювання спорів зіштовхується з викликами, включаючи технічні проблеми, нерівність у доступі до Інтернет-ресурсів, проблеми конфіденційності та виконання рішень.

На міжнародному рівні розвиток механізму врегулювання спорів онлайн тривалий час не був особливо інтенсивним через ефективне функціонування інших способів вирішення торговельних спорів. Перш за все, Органу з вирішення спорів СОТ. Це й не дивно, оскільки після завершення Уругвайського раунду, він перетворився на авторитетну установу з передбачуваними та прозорими процедурами відповідно до Домовленості про правила та процедури врегулювання спорів. Відповідно до останньої уніфіковані підходи застосовуються до спорів між членами організації за всіма договорами (covered agreements), хоча окремі з них і передбачають спеціальні правила. Інституційна структура вирішення спорів складається з трьох органів: груп експертів, Апеляційного органу та Органу з вирішення спорів, який є однією з іпостасей Генеральної Ради СОТ. Групи експертів, що складаються, з трьох, а у виняткових випадках – з п'яти членів, створюються ad-hoc і розглядають кожен зі спорів окремо. У свою чергу, Апеляційний орган є постійно діючим. Він складається з семи членів та переглядає за вимогою сторони спору правові питання звіту групи експертів і тлумачення права, зроблене нею. Звіти груп експертів/Апеляційного органу затверджуються ОВС «негативним консенсусом», після чого починається відлік імплементації для забезпечення відповідності заходів угодам СОТ [5].

Режим врегулювання спорів у СОТ від початку містив окремі недоліки. Перш за все, країни, що розвиваються, та найменш розвинені держави критикують ОВС за те, що вони перебувають у невідгідному становищі, оскільки ГАТТ, а, потім, СОТ була створена задля задоволення інтересів розвинених держав, й покладає на держави Півдня зобов'язання, які часто не сприяють розвитку їхніх торговельних спроможностей. Окрім того, процедури врегу-

лювання спорів в ОВС є досить витратними, зокрема, через їхню тривалість, а перегляд Апеляційним органом – зазвичай, завершується підтвердженням рішення групи експертів. Так, згідно з даними на офіційному сайті СОТ, станом на 2018 рік зі 166 справ, які були подані на оскарження, у 156 (94%) Апеляційний орган підтвердив правову позицію групи експертів [6]. Цікаво, що за цей же період жодний з поданих 55 спорів так і не дійшов до етапу оприлюднення рішення. Окремі розвинені держави також висловлюють невдоволення щодо роботи ОВС: через розширення зобов'язань членів СОТ (наприклад, тлумачення «обнулення», «державного органу»), ігнорування 90-денного терміну, «зловживання» повноваженнями з боку членів, оцінка Апеляційним органом фактів та національного законодавства *denovo*. Зокрема, США не лише дипломатично, але й вже фактично заблокували роботу цілої системи, унеможливаючи обрання членів Апеляційного органу.

Криза механізму врегулювання спорів СОТ збільшила увагу до процедур, закріплених в регіональних угодах, однак юридична природа останніх не дозволяє їм повністю замінити ОВС, оскільки деякі угоди про вільну торгівлю не містять положень у певних сферах (ТБТ, торговельний захист), а окремі, навпаки, містять т.зв. правила СОТ+, деякі ЗВТ виключають певні сфери із дії положень про врегулювання спорів, інші не передбачають створення окремих механізмів, а містять клаузулу про вибір суду. Викликають занепокоєння і проблеми з призначенням суддів, часові обмеження та можливість оскарження. За таких обставин вбачається більш доцільним спробувати вдосконалити існуючі механізми врегулювання спорів за допомогою ІКТ.

По-перше, можна інтегрувати онлайн-модель врегулювання торговельних спорів у традиційні механізми. Наприклад, в рамках Домовленості в СОТ початковим обов'язковим етапом завжди виступають консультації між сторонами, після яких останні можуть вдаватися до посередництва чи медіації. Ці процедури не є детально врегульованими положеннями Домовленості, тому їхня модернізація завдяки ІКТ не зумовить особливих труднощів, а, навпаки, спростить нотифікацію та обмін правовими позиціями. Що сто-

сується діяльності групи експертів та Апеляційного органу, то, зазвичай, вона відбувається через розгляд необхідних письмових подань сторін та оглядові зустрічі, при цьому Апеляційний орган майже завжди обмежується письмовим переглядом. Це означає, що не існує жодної процесуальної стадії, яку не можна би було провести онлайн.

Що стосується механізму врегулювання торговельних спорів, передбаченого в угодах про вільну торгівлю, варто зазначити, що він, переважно, організований відповідно до моделі ОВС СОТ, однак з певними особливостями, що описані вище. Найбільш популярними способами врегулювання є переговори, посередництво та арбітраж, виходячи з чого в такий механізм можуть бути вдало інтегровані ІКТ.

По-друге, традиційні процесуальні стадії можна вдосконалити, здешевити та пришвидшити, якщо використовувати спеціальне програмне забезпечення та мережеві технології, наприклад, формування групи експертів відповідно до характеру справи, бажаної компетенції потенційних членів, регіонального представництва тощо або ж пряма комунікація між сторонами, що особливо актуально для країн, що розвиваються та найменш розвинених держав, які не мають власного представництва при організації або ж навіть дипломатичного представництва в Швейцарії.

Врешті, засідання квазі-судових органів можна проводити в будь-який час і в будь-якому місці, забезпечуючи більшу конфіденційність та оперативність. Остаточне рішення (звіт) може бути опубліковане в Інтернеті, що дозволить сторонам швидше отримати результат і визначитися з подальшими діями, оскільки в торговельних спорах втрати навіть за один день можуть відобразитися на цілій національній галузі. Крім того, всі види доказових матеріалів для процесу можуть зберігатися в електронному вигляді, що не тільки зменшує використання паперу, але й полегшує їхнє опрацювання та схоронність. Звичайно, онлайн-процес не виключає використання офлайн-елементів. Однак в цілому врегулювання торговельних спорів вже може бути переведене в дистанційний формат.

Відтак, хоча механізм врегулювання спорів онлайн все ще потребує значних зусиль для його реалізації: починаючи від розробки необхідного правового забезпечення як на національному, так і на міжнародному рівні, а також вирішення проблеми інформаційного розриву між державами, він може допомогти збільшити потенціал судової системи та альтернативних методів врегулювання спорів, пропонуючи вирішення проблем судової неефективності, високої вартості судових процесів та географічних бар'єрів.

Список використаної літератури

1. Technical Notes on Online Dispute Resolution of the United Nations Commission on International Trade Law. General Assembly Resolutions. 2016. URL: <https://undocs.org/en/A/RES/71/138>.
2. Li Ma. Xin Ni. Study on Online Dispute Settlement Model of International Trade Disputes Against the Background of “the Belt and Road”/Proceedings of the 5th International Conference on Economics, Management, Law and Education (EMLE 2019). 2019. URL: https://www.researchgate.net/publication/338603281_Study_on_Online_Dispute_Settlement_Model_of_International_Trade_Disputes_Against_the_Background_of_the_Belt_and_Road.
3. Technical Notes on Online Dispute Resolution. UNCITRAL. 2017. URL: https://www.uncitral.org/pdf/english/texts/odr/V1700382_English_Technical_Notes_on_ODR.pdf.
4. Zhao Qi. Discussion on China's Online Dispute Resolution Mechanism [D]. Shandong University. 2019. URL: https://www.cityu.edu.hk/slwl/lib/doc/Frank_pub/5.pdf.
5. Домовленість про правила та процедури вирішення спорів. 1994. URL: https://zakon.rada.gov.ua/laws/show/981_019.
6. Dispute settlement activity – some figures. WTO. URL: https://www.wto.org/english/tratop_e/dispu_e/disputstats_e.htm#:~:text=Between%20the%20entry%20into%20force,in%20at%20least%20one%20dispute.

Солончук І.В.

старший викладач КПП імені Ігоря
Сікорського”

АНТИКОРУПЦІЙНІ ПИТАННЯ РЕФОРМУВАННЯ СУДОЧИНСТВА В УМОВАХ СОЦІАЛЬНОЇ ТА ЦИФРОВОЇ ТРАНСФОРМАЦІЙ

Соціальна та цифрова трансформації, викликані об’єктивними закономірностями розвитку соціуму, вимагають детальної уваги як науковців, так і органів державної влади до питання правового регулювання суспільних відносин. Наразі вимоги життя такі, що соціальні зміни потребують негайної реакції законодавця щодо врегулювання певних відносин. У зворотному випадку не уникнути проблем, суперечностей та конфліктів. Інституцією, покликаною врегульовувати подібні спірні ситуації, є суд як особливий державний орган, який на конституційному рівні наділений виключним правом здійснювати правосуддя в Україні (ст. 124) [1].

Захист прав, свобод та інтересів, як завдання органів судустрою, визначається низкою нормативно-правових актів [1; 2; 3]. Організація та діяльність суду детально регламентуються Законом, адже суд зобов’язаний здійснювати захист у розумні строки та бути незалежним, безстороннім, справедливим. Дотримання вказаних елементів гарантує *право на справедливий суд*, що, безспірно, є метою здійснення правосуддя.

Питання реформування судової системи України постійно виникає з часу здобуття незалежності. Ще у 1992 р. Верховною радою України затверджено Концепцію судово-правової реформи в Україні. У 2006 р. Президент України своїм Указом запроваджує Концепцію вдосконалення судівництва для утвердження справедливого суду в Україні відповідно до європейських стандартів. Закон «Про судوустрій України», прийнятий у 2002 р, втратив чинність у 2010 р. на підставі прийняття наступного нового Закону України «Про судоустрій і статус суддів», який також на сьогодні втратив чинність (окрім кількох положень, визначених у пунктах 7, 23, 25, 36 розділу XII Закону № 1402-VIII від 2 червня 2016

р.) на підставі нового Закону України «Про судоустрій і статус суддів» № 1402-VIII від 2 червня 2016 р. [2]. Такі важливі, часом кардинальні зміни у правовому регулюванні судоустрою, на жаль, до сьогодні все ще не дали бажаного результату. Тому виникає питання: можливо, потрібно здійснювати реформування комплексно, охоплюючи різноманітні сфери, зокрема питання подолання корупції в Україні, адже однією з підстав недовіри людей до суддів є переконання людей причетності останніх до корупційних дій. Згідно з дослідженням, проведеним соціологічною службою Центру Разумкова з 30 жовтня по 5 листопада 2020 року, ситуація з довірою людей органам судоустрою є вкрай негативною: 75% респондентів висловили недовіру загалом всій судовій системі та зокрема місцевим судам (63%), Вищому антикорупційному суду (70%), Верховному Суду (63%). Для порівняння: водночас, люди висловлюють довіру церкві (62% опитаних) [4]. Така ситуація є неприпустимою, адже виникають обґрунтовані сумніви, чи виконують органи судоустрою свої завдання і чи є виправданими ті економічні та соціальні затрати, які несе держава в кожному черговому етапі судового реформування? Можливо, до вирішення цього питання слід підійти з позиції суб'єкта процесуальних правовідносин – судді та учасника цивільного процесу.

За інформацією Кабінету Міністрів України корупція була й досі залишається однією з найбільших проблем України. В Індексі сприйняття корупції (ІСК), що укладається глобальною антикорупційною організацією *Transparency International* на базі оцінок підприємців та аналітиків, за підсумками 2018 року Україна посідає 120 сходинку у переліку зі 180 країн світу [5].

Важливим кроком у подоланні ситуації, що склалася, є прийняття Україною низки нормативно-правових актів, спрямованих на боротьбу з корупцією [6; 7].

Новели процесуального законодавства також мають позитивну динаміку [3]. У цивільному процесі учасниками справи, поряд з іншими суб'єктами, можуть бути органи та особи, яким закон надає право звертатися до суду в інтересах інших осіб. На підставі Закону України № 198-IX від 17.10.2019 р. статтю 56

Цивільного процесуального кодексу України доповнено частиною сьомою, в котрій до органів та осіб, яким законом надано право звертатися до суду в інтересах інших осіб, законодавець відносить Національне агентство з питань запобігання корупції (далі – Національне агентство). Національному агентству надається право звертатися до суду з позовом (заявою) в інтересах викривача на підставі звернення викривача. Згідно ч. 1 ст. Закону України «Про запобігання корупції» викривачем є фізична особа, яка переконана в достовірності інформації та повідомила про можливі факти корупційних чи пов'язаних з корупцією правопорушень, інших порушень Закону «Про запобігання корупції», вчинених іншою особою, якщо така інформація стала їй відома у зв'язку з певною її діяльністю: трудовою, професійною, господарською, громадською, науковою або через проходження нею служби, навчання або її участь у передбачених законодавством процедурах, які є обов'язковими для початку такої діяльності, проходження навчання, служби [6]. Національне агентство може брати участь у судовому розгляді справ за такими позовами (заявами), може на будь-якій стадії розгляду вступати у справу, провадження в якій відкрито за позовами (заявами) викривачів, подавати апеляційну, касаційну скаргу, заяву про перегляд судового рішення за нововиявленими чи виключними обставинами, при чому навіть у справі, провадження в якій відкрито за позовом (заявою) викривача [3].

Відбулися зміни і в правовому регулюванні організації судоустрою. Сьогодні на посаду судді не може претендувати особа, яка не бажає чи не може підтвердити законність джерела походження свого майна (ч. 4 ст.69) [2]. Особа, призначена на посаду судді, набуває повноважень судді після складення присяги судді, зміст якої визначається ч.1 ст.57 Закону України «Про судоустрій і статус суддів». Складаючи присягу, особа зобов'язується не вчиняти дій, що порочать звання судді або підривають авторитет правосуддя. Адже корупційні діяння підривають авторитет правосуддя значно більше, ніж всі економічні труднощі та організаційні недоліки. Виконавши аналіз правових норм, які регулюють статус суд-

ді та покликані відображати державну антикорупційну політику, вбачаємо позитивним кроком запровадження:

1) *повної перевірки декларації судді*, що полягає у з'ясуванні достовірності задекларованих відомостей, точності оцінки задекларованих активів, перевірки на наявність конфлікту інтересів та ознак незаконного збагачення. На наш погляд є недоліком досить великі часові межі, визначені законодавцем для її проведення, адже така повна перевірка декларації судді, як правило, має відбуватися щонайменше один раз на п'ять років (якщо інше не передбачено законом), або за запитом відповідних органів – Вищої кваліфікаційної комісії суддів України чи Вищої ради правосуддя;

2) *подання суддею декларації його родинних зв'язків* (ст. 61) [2]. Закон встановлює обов'язок судді є щорічно (а саме до 1 лютого) подавати декларацію родинних зв'язків за формою, що визначається Вищою кваліфікаційною комісією суддів України. Декларація є відкритою для загального доступу, оскільки має бути оприлюдненою на офіційному веб-сайті ВККС України. На наш погляд недоліком є те, що декларація перевіряється ВККС України не у кожному випадку заповнення, а лише на підставі одержання інформації, що може свідчити про недостовірність (у тому числі неповноту) відомостей, поданих суддею у декларації, оскільки за відсутності доказів іншої відомості, подані суддею у декларації родинних зв'язків, вважаються достовірними (ч. 4 ст. 61) [2];

3) *подання суддею декларації доброчесності судді* (ст.62) [2]. Обов'язком судді є подання щорічно до 1 лютого декларації доброчесності за формою, що визначається ВККС України. Декларація включає перелік тверджень, правдивість яких суддя повинен задекларувати шляхом їх підтвердження або непідтвердження, наприклад, є питання щодо відповідності рівня його життя наявному в нього та членів його сім'ї майну і одержаним ними доходам та чи не вчиняв суддя корупційні правопорушення. Декларація доброчесності судді також є відкритою для загального доступу через оприлюднення на офіційному веб-сайті ВККС України. За відсутності доказів іншого твердження судді у декларації доброчесності вважаються достовірними і перевірка декларації доброчесності

також можлива лише уразі одержання інформації, що може свідчити про недостовірність (в тому числі неповноту) тверджень судді у декларації доброчесності (ч. 5,6 ст.62) [2].

Отже, проаналізувавши нормативні положення, які регулюють судоустрій України та відображають державну антикорупційну політику, можемо зробити висновок, що, поряд із значними прогресивними зрушеннями у правовому регулюванні, все ще залишаються проблемні аспекти, які потребують правової визначеності. З огляду на викладене вище, цілком слушною є думка О.О. Кравчука, який серед принципів права виділяє принцип належної правової визначеності, який означає, що закон повинен бути доступним для всіх осіб, яких він яких він стосується, і бути достатньо чітко сформульованим. Відсутність належної правової визначеності призводить до зниження ефективності реалізації заходів державної антикорупційної політики [8, с. 93]. Стрімкий розвиток сучасних інформаційних технологій надає широкий спектр можливостей для удосконалення організації органів судоустрою та обмеження впливу «людського фактору» у сферах, де це можливо.

Список використаної літератури:

1. Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
2. Про судоустрій і статус суддів: Закон України від 02 червня 2016 р. № 1402-VIII. *Відомості Верховної Ради*. 2016. № 31. Ст.545.
3. Цивільний процесуальний кодекс України: Закон України від 18 березня 2004 р. № 1618-IV. *Відомості Верховної Ради України*. 2004. № 40-41, 42. Ст.492.
4. Оцінка громадянами ситуації в країні, рівень довіри до соціальних інститутів та політиків, електоральні орієнтації громадян (жовтень–листопад 2020р.). *Разумков центр*: веб-сайт. URL: <https://razumkov.org.ua/> (дата звернення: 07.12.2020).
5. Боротьба з корупцією: Урядовий портал. *Єдиний веб-портал органів виконавчої влади України*. URL: <https://www.kmu.gov.ua/diyalnist/reformi/verhovenstvo-prava-ta-borotba-z-korupciyeyu/borotba-z-korupciyeyu> (дата звернення: 07.12.2020).

6. Про запобігання корупції: Закон України від 14 жовтня 2014 р. № 1700-VII. *Відомості Верховної Ради*. 2014. № 49, ст.2056.

7. Про внесення змін до Закону України “Про запобігання корупції” щодо викривачів корупції: Закон України від 17 жовтня 2019 р. № 198-IX. *Відомості Верховної Ради України*. 2019. № 50, ст.356.

8. Кравчук О. О. Проблема правової визначеності в забезпеченні антикорупційної політики. *Реалізація державної антикорупційної політики в міжнародному вимірі*: матеріали III Міжн. наук.-практ. конф., част. 1, 7 груд. 2018 р. Київ. С.87-93.

Ткачук Т.Ю.

доктор юридичних наук, доцент,
заступник завідувача кафедри
Навчально-наукового інституту
інформаційної безпеки Національної
академії Служби безпеки України

АКТУАЛЬНІ ДОМІНАНТИ СУЧАСНОГО ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Щоразу, коли людина винаходила чи вдосконалювала якийсь засіб для ураження або знищення собі подібних, виникала потреба захисту від нової халепи: щит і меч, металеві обладунки проти стріл та списів, кріпосні стіни та броня проти вогнепальної зброї, протиповітряні установки й бомбосховища проти бойової авіації. Повною мірою це стосується й сучасності: критичне мислення проти інформаційно-психологічної агресії, кіберзахист проти інформаційної зброї й атак у кібернетичному просторі.

Такою є логіка цивілізаційної еволюції людства. І, як не прикро це визнавати, історія переконливо свідчить, що війни зробили значно більше для розвитку технологій, ніж людська цікавість, потяг до побутових зручностей чи естетичного задоволення, ба навіть потреба у хлібі насущному й даху над головою. Ще одним беззаперечним історичним фактом є те, що усі давні цивілізації, які надавали перевагу мирним промислам – землеробству, скотарству, гончарству, виготовленню одягу та іншого реманенту госпо-

дарського чи культурного призначення, мистецтву були зрештою знищені чи підкорені тими, хто здебільшого виготовляв і вдосконалював зброю і промишляв війнами. Аби такого не сталося сьогодні – в епоху бурхливого прогресу інформаційно-комунікаційних технологій, коли у розпорядженні новітніх варварів опинилася інформаційна, кібернетична зброя, до традиційних засобів захисту від агресії слід додати потужний кібернетичний щит, а також здатність до критичного мислення, інформаційну культуру та інформаційну гігієну.

Вказана вище послідовність «напад – захист» характерна і для кіберпростору: лише тоді, коли кіберзагрози й кібератаки вже набули чималих обертів, розпочався пошук та впровадження засобів кіберзахисту та формування систем кібернетичної безпеки. У теперішній час спостерігаємо зародки нових захисних засобів, коли у суспільстві першочергового значення набувають розвиток інформаційної культури, такі категорії, як «критичне мислення споживачів інформації», «екологія інформації», «інформаційна гігієна», а також усвідомлення нагальної потреби навчати цього молодь.

Розвиток інформаційних технологій на початку 21 століття визначив загальні тенденції поступу людства та окреслив характерні проблеми даної епохи, з-поміж яких:

1. Формування нового планетарного простору, де інформаційні й телекомунікаційні технології забезпечують ефективну міжособистісну взаємодію. Основними властивостями таких процесів є безмежність, доступність, гіперзв'язаність, прозорість територіальних кордонів, рух у масштабі часу, розвиток Інтернету речей тощо. У результаті відбувається становлення нового інформаційного суспільства.

2. Уся множина суспільних процесів (соціально-політичних, економічних та ін.) опосередкована застосуванням інформаційних технологій, оскільки вони відіграють вирішальну роль у формуванні навколишньої реальності й мають неабиякий вплив на динаміку та вектори її розвитку.

3. Брак уваги до проблем правового забезпечення інформаційної безпеки з боку урядів і міжнародних інституцій значною мі-

рою спричинив виникнення й надшвидке поширення таких явищ (і відповідних понять у науковому й повсякденному вжитку), як «інформаційна зброя», «інформаційний тероризм» та «інформаційна війна», а також відповідних деструктивних впливів, цими явищами здійснюваних. Нехтування питаннями інформаційної безпеки зумовило непрогнозовані системні безпекові потрясіння в економічній, соціальній, політичній, екологічній та інших сферах. Унаслідок цього проблеми інформаційної безпеки, хоч і зі значним запізненням, вийшли на передній план в усіх сферах життєдіяльності, як на внутрішньодержавному, так і на міжнародному рівнях.

Таким чином, можна стверджувати, що новостворене інформаційне суспільство сформувало й нову дійсність – віртуальну реальність. Ця ж формація продемонструвала новий тип соціального поступу – нелінійний розвиток суспільства, що зробило проблематичними усі прогнози. Формування нової реальності зумовило виникнення нових соціальних цінностей – інформаційних, котрі на цьому етапі еволюції світової спільноти стали визначальними.

Ще одна базова властивість інформаційного світу – інноваційність. Специфікою інформаційної епохи є вибухове зростання нових знань. Його потенціал настільки значний, що чимало фахівців іменують сучасну економіку розвинутих країн «заснованою на знанні», «знанневою» і т.п. Адже сучасність вимагає, щоби здобуті наукою знання негайно втілювалися в техніці, технологіях, виходили продуктом на світові ринки, а базисом будь-якого знання є інформація.

У цьому контексті приєднуємося до думки експерта ЮНЕСКО і Ради Європи в галузі медіаосвіти, одного із лідерів сучасного європейського медіаосвітнього руху Д. Фрау-Майгс, що найліпшим засобом у боротьбі з лавиноподібним інформаційним потоком, найдійовішою «пошуковою службою» є освіта [1, с. 45].

Що стосується особистості, то, крім високої освіченості й загальної культури, для її «вписування» в єдину інформаційну картину світу необхідні такі властивості, як інформаційна компетенція, інформаційна культура, спроможність і бажання кожної люди-

ни не бути лише пасивним «нейтроном» інформаційної взаємодії, а стати її активним, творчим суб'єктом, «електроном» інформаційної соціальності. До єдиної глобальної системи інформаційного світоустрою людина має увійти чинником вільного й творчого особистісного розвою як запоруки відповідного розвитку всієї світової спільноти.

Саме вказані консолідуючі чинники, котрі стосуються не лише суспільства загалом, а й кожної людини, є незаперечними фундаментальними цінностями інформаційного суспільства як сучасного етапу цивілізаційного розвитку людства. При цьому більшість проблем щодо інформаційної безпеки особи й соціуму на етапі інформаційного суспільства розв'язуються за допомогою саме цих незаперечних фундаментальних цінностей.

Література:

1. Frau-Meigs D. Media Matters in the Cultural Contradictions of the 'Information Society'. *Towards a Human Rights-Based Governance Strasbourg: Council of Europe*. 2011. 390 p.

Фокша Л.В.

кандидат юридичних наук, доцент,
доцент Дніпропетровського
державного університету внутрішніх
справ

АНАЛІЗ ПРАВОВИХ ПІДСТАВ ВПРОВАДЖЕННЯ ЦИФРОВОЇ ПОШТОВОЇ МАРКИ В УКРАЇНІ

Інтеграція України в Європейське співтовариство вимагає значної модернізації сфери виробництва та обслуговування. Важливою складовою сфери послуг в будь якій країні є поштові послуги.

Ринок поштових послуг має свої особливості, такі як виключне право національного оператора на видання, введення в обіг та організацію розповсюдження поштових марок, маркованих конвертів і карток, а також виведення їх з обігу; офіційне видання

каталогів і цінників колекційних поштових марок та іншої філателістичної продукції; пересилання простих листів масою до 50 грамів та простих поштових карток. Основою ринку поштових послуг України є діяльність національного оператора – Акціонерного товариства «Укрпошта», державного підприємства поштового зв'язку, підпорядкованого Міністерству інфраструктури України.

Правові засади надання поштових послуг закріплено в Законі України «Про поштовий зв'язок»[1], Постанові Кабінету Міністрів України «Правила надання послуг поштового зв'язку» від 5 березня 2009 р. № 270, Розпорядженні КМУ «Про національного оператора поштового зв'язку» від 10 січня 2002 р. № 10-р, правилах, нормативах тощо.

Оптимізація сфери надання послуг поштового зв'язку, гармонізація законодавства з європейськими стандартами, вимагає нових рішень та реалізації перспективних проектів модернізації поштових послуг.

Одним із напрямів оптимізації послуг поштового зв'язку є проект запровадження електронного знаку поштової оплати, або електронної поштової марки. Можливість впровадження якого визначена в проекті Закону України від 10.11.2020 № 4353 «Про поштовий зв'язок» (далі – Законопроект № 4353).

Згідно Законопроекту № 4353 «Про поштовий зв'язок» електронний знак поштової оплати – графічна інформація, що наноситься на відправлення письмової кореспонденції та забезпечує можливість зчитування її за допомогою технічних засобів та засвідчує факт оплати послуг поштового зв'язку, що надаються призначеним оператором для юридичних осіб[2].

Електронний знак поштової оплати створюється програмно апаратними засобами призначеного оператора поштового зв'язку, обліковується на його балансі та належить йому до моменту нанесення її графічного зображення на листи, поштові картки споживача послуг поштового зв'язку.

Введення електронного знаку поштової оплати дасть можливість розв'язати такі проблемні моменти в діяльності оператора поштового зв'язку:

- фальсифікації знаків поштової оплати;
- оптимізувати процес обробки кореспонденції,
- знизити витрати на виготовлення знаку оплати і, відповідно, на саму послугу;
- підвищити конкурентоздатність послуг оператора поштового зв'язку на внутрішньому та зовнішньому мінімізувати ринку.

Попри значну кількість переваг законодавчого закріплення можливості використання електронного знаку поштової оплати, автори Законопроекту № 4353 не беруть до уваги художню складову поштової марки, та можливість її оцифрування.

В Україні розробляється проект «Цифрова поштова марка», яку слід розглядати як електронний знак поштової оплати, що має певний чітко визначений художній зміст. Кількість випуску цих марок обмежена, що забезпечить їх філателічну цінність.

Реалізація цього проекту дозволить, перш за все, збільшити фінансові надходження оператора поштового зв'язку, оскільки він буде отримувати не тільки доходи при первинному розміщенні електронної поштової марки, але і доходи відтранзакції за продаж марок на вторинному ринку. Також це дозволить розширити ринок збуду марок не тільки вітчизняним споживачам, але й іноземним цінителям.

Процес випуску та обігу електронної цифрової марки має бути побудований за технологією «блокчейн», що дозволить управляти процесами зберігання, передачі електронної марки, та виключає можливість її підробки.

Враховуючи вищезначене, вбачається за необхідне в Законопроекті № 4353 [2] закріпити поряд з поняттям «електронний знак поштової оплати», визначення «цифрова поштова марка», як електронний знак, що виготовлений за певним художнім зразком, із зазначенням номінальної вартості та держави, і є засобом оплати послуг поштового зв'язку з пересилання листів, поштових карток, що надаються призначеним оператором поштового зв'язку.

Список використаної літератури

1. Закон України «Про поштовий зв'язок» від 04.10.2001 № 2759-III// [Електронний ресурс]. – Режим доступу:<https://zakon.rada.gov.ua/laws/show/2759-14#Text>
2. Проект Закону України від 10.11.2020 № 4353 «Про поштовий зв'язок»// [Електронний ресурс]. – Режим доступу:http://search.ligazakon.ua/l_doc2.nsf/link1/JI03632A.html

Новікова О.Ф.

доктор економічних наук, професор
заступник директора з наукової
роботи Інституту економіки
промисловості НАН України

Сидорчук О.Г.

доктор економічних наук, професор
Львівський регіональний інститут
державного управління НАДУ при
Президентіві України

ФОРМУВАННЯ ДЕРЖАВНОЇ АНТИКРИЗОВОЇ ПОЛІТИКИ В УМОВАХ НОВІТНІХ ВИКЛИКІВ ТА НЕБЕЗПЕК ЧЕРЕЗ ЗАЛУЧЕННЯ РЕСУРСІВ ЦИФРОВІЗАЦІЇ

Державна антикризова політика в умовах пандемії COVID-19 має бути сприйнятою суспільством, узгодженою з основними суб'єктами управління та господарювання та забезпечувати консолідацію дій при її формуванні та реалізації.

Забезпечення ефективної діяльності суб'єктів державної політики щодо мінімізації соціально-економічних ризиків та небезпек у сфері праці та зайнятості в Україні в умовах пандемії COVID-19 вимагає додержання певних вимог. Це – наявність комплексного системного бачення всієї сукупності проблем, загроз та пріоритетів, напрямів діяльності щодо політики мінімізації соціально-економічних ризиків та небезпек у сфері праці та зайнятості.

При цьому доцільно для формування цілісного бачення ситуації із COVID-19 не обмежуватись виключно сферою праці та зайнятості, а формувати бачення всієї системи в більш широкому, стратегічному контексті щодо питань забезпечення національної безпеки України. Це дозволить суб'єктам взаємодії більш чітко розуміти свою роль в реалізації державної протипандемійної політики, зону власної відповідальності, вибудовувати ефективні моделі узгодженої взаємодії з іншими суб'єктами, враховувати вплив своєї діяльності на суміжні сфери.

Одночасно необхідним є розуміння кожним з суб'єктів своєї ролі (сфер відповідальності, ключових напрямів діяльності, заходів, тих чи інших питань взаємодії з іншими суб'єктами) у цілісному комплексі концептуальних, стратегічних та програмних напрямів формування (становлення) державної політики мінімізації соціально-економічних ризиків та небезпек у сфері праці та зайнятості в Україні в умовах пандемії COVID-19. У відповідності із зазначеним вище, доцільно реалізувати такий алгоритм:

- 1) здійснити оцінку можливостей захисту національних інтересів України, забезпечення соціальної та економічної безпеки при формуванні та реалізації державної політики, спрямованої на подолання пандемії COVID-19;

- 2) визначити стратегічні напрями та антикризові заходи щодо мінімізації, попередження та подолання соціально-економічних ризиків та небезпек у сфері праці та зайнятості України в умовах пандемії COVID-19 й сформуванню структуровану систему політики реагування. Така система має містити цілісний комплекс ключових засад формування державної протипандемійної політики, які спрямовані на системне подолання негативних наслідків впливу пандемії COVID-19 у сфері праці та зайнятості України. Важливо дотримуватися принципу універсальності при формуванні стратегічних напрямів для розширених можливостей їх застосування не тільки в регуляторній політиці щодо соціальної, трудової сфер, а й у стратегіях національної та економічної безпеки; цифрового та економічного розвитку, інтеграції та адаптації внутрішньо переміщених осіб (ВПО) у

територіальні громади; а також у стратегіях і програмах охорони здоров'я в цілому, у період коронакризи;

3) розробити адресні рекомендації органам виконавчої та законодавчої влади, сторонам соціального діалогу сфери праці як ключовим суб'єктам формування та реалізації державної політики щодо мінімізації соціально-економічних ризиків та небезпек у сфері праці та зайнятості в Україні в умовах пандемії COVID-19.

Такий алгоритм дозволить суб'єктам державного управління більш змістовно визначити пріоритетні напрями діяльності та необхідні практичні заходи при одночасному розумінні всієї сукупності концептуальних, стратегічних та програмних напрямів, реалізації яких потребує формування (становлення) державної політики мінімізації соціально-економічних ризиків та небезпек у сфері праці та зайнятості в Україні в умовах пандемії COVID-19.

Коронакриза простимулювала запит на залучення й використання цифрових технологій в сфері праці, в освіті, медицині, в побуті і повсякденному житті. Тому у стратегічних напрямках державної антикризової політики це має бути враховано. Обґрунтованим стає напрям **«Використання переваг цифрового розвитку для пом'якшення ризиків та небезпек у трудовій сфері в умовах пандемії COVID-19»**. Його реалізація передбачає такі заходи:

- забезпечення адресного розвитку цифрових технологій для розширення можливостей зайнятості населення та запобігання негативним явищам у соціально-трудова сфері в умовах пандемії COVID-19;
- гарантування соціальної безпеки, надання якісних медичних, освітніх та інших соціальних послуг із застосуванням цифрових технологій;
- орієнтація на міжнародне, європейське та регіональне співробітництво щодо інтеграції України до європейських та глобальних цифрових систем та інфраструктур у тому числі для реалізації протипандемічної політики;
- дотримання рекомендацій міжнародних профільних організацій (ООН, Європейської комісії, ОЕСР; вимогам конвенцій МОП, нормам Східного партнерства тощо) з широким

використанням відповідних інтернет-ресурсів, ресурсів міжнародних цифрових платформ глобального партнерства, Східного партнерства для забезпечення соціального захисту працюючих в умовах пандемії;

- формування прогнозів та моніторинг зміни потреб на ринку праці під впливом цифровізації економіки та суспільства в умовах пандемії COVID-19;
- забезпечення дотримання роботодавцем вимог щодо перекваліфікації персоналу при масових звільненнях у результаті цифровізації робочих місць під час пандемії COVID-19;
- забезпечення дотримання соціальних і трудових прав працівників на онлайн-платформах, у тому числі соціальної захищеності дистанційного працівника при укладанні Цивільно-правового договору;
- державна підтримка створення «смарт-сіті», упровадження міжнародних стандартів управління «смарт-сіті», розробка інноваційних екосистем, інноваційної політики територіальних громад в умовах подолання наслідків пандемії COVID-19;
- запобігання міграції ІТ-фахівців за кордон шляхом посилення мотивації працювати в країні (високий рівень оплати й безпека умов праці, гарантованість зайнятості тощо);
- поширення укладання меморандумів про співпрацю між представниками громадськості та органами державної влади, проведення грантових конкурсів у межах державних програм, спрямованих на подолання негативних наслідків цифрових трансформацій, у тому числі інтернет-залежності в умовах поширення дистанційної зайнятості при пандемії COVID-19;
- розробка методології оцінки та прогнозів впливу цифровізації економіки на сферу праці, а також прогнозів перспективних балансів робочої сили для базових галузей економіки з урахуванням цифрових трансформацій в умовах пандемії COVID-19.

Ефективність державної антикризової політики в умовах впливу пандемії COVID-19 вимагає залучення усіх ключових суб'єктів

господарювання до її формування та реалізації, активізації діяльності державних органів і структур законодавчої та виконавчої влади. Органами і структурами державної влади, що відповідають та ініціюють розвиток цифрових трансформацій в Україні є:

1. Міністерство цифрової трансформації України;

2. Міністерство з питань стратегічних галузей промисловості України;

3. Комітет Верховної Ради України з питань цифрової трансформації.

В контексті ключових напрямів та пріоритетів діяльності щодо мінімізації соціально-економічних ризиків та небезпек у сфері праці та зайнятості в Україні в умовах пандемії COVID-19 Міністерству цифрової трансформації України та Комітету Верховної Ради України з питань цифрової трансформації доцільно в першу чергу зосередитись на реалізації таких заходів:

1. Визнати, що одним із найбільш пріоритетних напрямів захисту від поширення коронавірусної хвороби при одночасному збереженні робочих місць є максимальне поширення дистанційних та безконтактних форм роботи. Внести зміни та доповнення до діючої *Концепцію розвитку цифрової економіки та суспільства України на 2018-2020 роки* (із подальшою її пролонгацією) та плану заходів щодо її реалізації; залучення наявного потенціалу інформаційно-комунікативних та цифрових технологій задля створення дистанційних робочих місць.

2. Прискорити процеси розбудови ефективної цифрової сервісної держави, у тому числі з метою подолання і мінімізації ризиків і загроз впливу пандемії COVID-19 в Україні та подальшого постпандемійного відновлення, зокрема – забезпечити постійне удосконалення систем дистанційного надання адміністративних послуг, в тому числі розширення спектру діяльності Єдиного державного порталу адміністративних послуг та порталу державних он-лайн послуг населенню «Дія».

3. Розробити та реалізувати заходи, спрямовані на широке використання ресурсів та інструментів цифровізації для реалізації ефективної антикризової регуляторної політики України для про-

тидії загрозам впливу пандемії COVID-19 та подальшого постпандемічного відновлення.

4. Сприяти забезпеченню можливостей для системного державного стимулювання цифровізації секторів економіки та бізнесу, та внутрішнього ринку споживання ІТ та цифрових продуктів/послуг, впровадження інновацій та створення робочих місць “Індустрії 4.0” в тих секторах економіки, які здатні на цифровий стрибок в період постпандемічного відновлення, впровадження сучасних цифрових послуг на ринку праці.

5. Розвивати інформаційно-комунікативні платформи для реалізації соціального діалогу в сфері праці та зайнятості (на зразок онлайн-порталу «Дія», або онлайн-платформи для взаємодії органів влади та інститутів громадянського суспільства «ВзаємоДія» щодо сфери праці та зайнятості з нормативно-правовим, процедурним та іншим змістовним наповненням;

6. Сприяти забезпеченню технічних можливостей для комунікацій та взаємодії суб’єктів суспільних та соціально-трудових відносин, суб’єктів ринку праці та зайнятості щодо широкого використання ресурсів та інструментів цифровізації, ІКТ, комунікативних он-лайн платформ, соціальних мереж, національних порталів

7. Всебічно сприяти впровадженню смарт-технологій, технологій оптимізації виробничих процесів в напрямі мінімізації безпосередніх контактів між працівниками та розширення можливостей дистанційної та ізольованої роботи – в рамках конкретних спільних проєктів із профільними міністерствами, крупним бізнесом та іншими зацікавленими структурами.

8. Розробити та впровадити активну політику щодо інформаційно-просвітницької підтримки заходів, спрямованих на захист працівників на робочому місці (спільно з профільними міністерствами, Державним центром зайнятості, Державною службою України з питань праці, крупним бізнесом, крупними медіа-структурами та ін.).

9. За підтримки Кабінету Міністрів України та міжнародних партнерів – забезпечити створення сприятливих умов для реалізації програм «Україна – цифровий коридор» та «Україна – Data

Ellysium» та інтеграції із європейськими системами життєзабезпечення (наприклад, e-Health).

10. Створення державної онлайн-платформи нормативно-правових документів щодо забезпечення захисту соціальних і трудових прав працівників-мігрантів з визначенням та виокремленням інформації, необхідної для чіткої зорієнтованості – що саме робити мігранту з України в умовах жорстких карантинних обмежень, у т.ч. при обмеженнях транспортного пересування між країнами.

Панькова О.В.

кандидат соціологічних наук, доцент,
пров. науковий співробітник,
Інститут економіки промисловості
НАН України

Красуліна Я.Є.

провідний інженер
Інститут економіки промисловості
НАН України

УКРАЇНА В КООРДИНАТАХ ЧЕТВЕРТОЇ ПРОМИСЛОВОЇ РЕВОЛЮЦІЇ (ПЛАТФОРМА «ПРАЦЯ 4.0») ТА ПАНДЕМІЙНОЇ СОЦІОЕКОНОМІЧНОЇ РЕАЛЬНОСТІ

Небезпечні, надскладні, невизначені за своїми наслідками явища початку 20-х років ХХІ ст. вимагають усвідомлення того, які сутнісні зміни відбуваються у соціально-трудовій сфері на глобальному, національному, локальному рівнях. На сьогодні соціально-економічні прогнози, програмні документи політичних, урядових структур та інституцій переповнені суперечливими, нерідко полярними оцінками нинішнього та майбутнього світу праці. Так, поширеними є твердження, що розбудова нової (цифрової) економіки у глобальному соціумі може призвести до колапсу у сфері праці та зайнятості. Зокрема, мова йде про співвідношення 20:80, за якого економічна діяльність буде потребувати не більше 20% економічно активного населення, яке може набути статусу за-

йнятих, інші 80% будуть непотрібні. Протилежне «поле» оцінок та прогнозів фокусується на твердженнях, що в новій (цифровій) економіці масове зникнення одних робочих місць буде супроводжуватися появою нових, здатних зняти напругу на ринку праці [1, С. 3-4] і покращити життєдіяльність усіх.

«Вірусний», «епідеміологічний» чинник суспільного поступу-XXI вже змінив і продовжує змінювати усі складові життєдіяльності людей, спільнот, соціуму, людства в цілому; набуває нового формату глобалізація, докорінно змінюються ланцюги створення суспільних продуктів, трансформуються ціннісні орієнтації учасників суспільного виробництва. Симбіоз нових технологій, інститутів організації праці, виробництва та управління; нова структура ресурсів і чинників набуття незаперечних конкурентних переваг та багато іншого докорінно змінюють усі складові соціально-трудової сфери. Йдеться про формування нової платформи соціально-трудового розвитку.

Вітчизняний науковець, засновник школи економістів-трудівників А.М. Колот підводить платформне підґрунтя **«Праці 4.0» – нової соціально-трудової реальності початку XXI століття**, яка формується під комплексним впливом реалій сьогодення. У цій авторській теоретичній конструкції «Праця 4.0» постає насамперед як трудова парадигма, що притаманна новій економіці, мережево-цифровим, технологічним базисом якої є «Індустрія 4.0». Ця трудова парадигма є платформою, інститутом, що забезпечує використання ресурсів праці в координатах, породжених Четвертою промисловою революцією.

Цифровізація, мережизація та інші новітні технології, прискорюють та інтенсифікують формування як нової економіки, так і нової глобалізації. Так зване *перше роз'єднання* стало можливим за створення умов для розвитку міжнародної торгівлі, а саме появи нових транспортних засобів та зниження вартості перевезень. Друге прискорення і продиктоване ним так зване *друге роз'єднання* стало можливим у зв'язку зі 1) створенням та масовим використанням інформаційно-комунікаційних технологій; 2) зниженням вартості переміщення інформації, новітніх технологій; 3) пере-

міщенням робочих місць виробництв за можливості контролю за адміністративно-господарською діяльністю, дистанційною координацією, відеозв'язком тощо; 4) поєднанням технологій «Великої сімки» з низькою заробітною платою в країнах, що розвиваються тощо; до останніх належить Україна. *Третє роз'єднання* – третій етап майбутньої глобалізації – це переміщення не лише товарів, виробництв, інформації, а й людей; це утвердження нового процесу праці. Йдеться про майбутнє чергового етапу глобалізації.

А. Колот, О. Герасименко обґрунтовують, що у найближчій перспективі з'являться як мінімум дві технологічні новації, які створять умови для так званого альтернативного переміщення людей через національні кордони. Перша новація (технологія) – це так звана *дистанційна присутність*, виконання робіт на відстані. Друга новація – це *дистанційна робототехніка*, яка передбачає, що управління роботами, кіберсистемами, іншими системами буде здійснюватися фахівцями на відстані (з іншої країни, континенту) [1, С. 9]. Пандемія прискорює процеси переходу на дистанційну зайнятість – це світовий глобальний тренд, який не оминув Україну. Для цього вже створюється і впроваджується відповідне нормативно-правове підґрунтя.

В новітніх умовах посилення ризиків і загроз пандемії розширення цифрового сегменту ринку праці є вагомим чинником забезпечення стійкості ринку праці та зайнятості, національної економіки в цілому. В умовах жорсткого карантину (березень-червень 2020 р.) українські компанії за можливості максимально перейшли на дистанційний режим роботи та переважно були налаштовані на збереження кількості персоналу. За даними дослідження Соціологічної групи «Рейтинг», 29% зайнятого населення України вже у квітні 2020 р. працювали дистанційно [3]. В Україні відстежується розвиток платформної зайнятості. Так, за даними досліджень, цифрова робота доступна в Україні через більш ніж 40 різних платформ. Очікується, що їх кількість і надалі зростатиме. Ці платформи включають такі, що обслуговують український ринок, а також пострадянський, міжнародний ринки.

Реалізація Україною ефективної державної протипандемічної регуляторної політики із залученням ресурсів цифровізації можлива за умов формування та прийняття відповідного нормативно-правового забезпечення. Своєчасним стало ініційоване українським Урядом прийняття та реалізація положень Закону України «Про внесення змін до деяких законодавчих актів України, спрямованих на забезпечення додаткових соціальних та економічних гарантій у зв'язку з поширенням коронавірусної хвороби (COVID-19)» [4]. У межах цього Закону значущими і доцільними стали норми, пов'язані із врегулюванням *гнучкого режиму робочого часу* при переході на *дистанційну (надомну) роботу*, визначенням умов та порядку оплати часу простою (в тому числі на період оголошення карантину), наданням допомоги по частковому безробіттю для працівників малих та середніх підприємств і для роботодавців; збільшенням мінімального розміру допомоги по безробіттю, посиленням соціального захисту медичних працівників, що ризикують життям у боротьбі з COVID-19 тощо. Такі норми відповідають вимогам забезпечення протиепідеміологічної безпеки на робочому місці, на виробництві, а також зміцнюють перехід української економіки на Платформу *Праця 4.0*.

Нормативно-правове забезпечення реалізації протипандемічної державної політики України та розвитку цифрової економіки включає:

1. **Закон України** «Про внесення змін до деяких законодавчих актів України, спрямованих на забезпечення додаткових соціальних та економічних гарантій у зв'язку з поширенням коронавірусної хвороби (COVID-19)». від 30 березня 2020 року № 540-IX URL: <https://zakon.rada.gov.ua/laws/show/540-20#n280>

2. **Концепція** розвитку цифрової економіки та суспільства України на 2018-2020 роки та план заходів щодо її реалізації. **Концепція:** <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text>, **План заходів:** <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#n250>

3. **Державна програма** стимулювання економіки для подолання негативних наслідків, спричинених обмежувальними

заходами щодо запобігання виникненню і поширенню гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2, на 2020-2022 роки. URL: <https://www.kmu.gov.ua/npas/pro-zatverdzhennya-derzhavnoyi-programi-stimulyuvannya-ekonomiki-534-270520>

4. **Основні напрями** реалізації державної політики у сфері зайнятості населення та стимулювання створення нових робочих місць на період до 2022 року. URL: <https://zakon.rada.gov.ua/laws/show/1396-2019-%D1%80#Text> **План заходів** щодо реалізації Основних напрямів реалізації державної політики у сфері зайнятості населення та стимулювання створення нових робочих місць на період до 2022 року. Затверджений розпорядженням Кабінету Міністрів України №216-р від 3 березня 2020 р. URL: <https://zakon.rada.gov.ua/laws/show/216-2020-%D1%80#Text>

5. **Про встановлення карантину** та запровадження посиленних протиепідемічних заходів на території із значним поширенням гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2 . ПОСТАНОВА КМУ від 22 липня 2020 р. № 641 <https://zakon.rada.gov.ua/laws/show/641-2020-%D0%BF#n40>

6. **Закон України «Про національну безпеку України»** Відомості Верховної Ради (ВВР), 2018, № 31, ст.241 <https://zakon.rada.gov.ua/laws/show/2469-19#Text>

7. **Стратегія національної безпеки України.** Затверджена Указом Президента України від 14 вересня 2020 року № 392/2020. URL: <https://zakon.rada.gov.ua/laws/show/392/2020#n5>

Література:

1. Колот А., Герасименко О. Сфера праці в умовах глобальної соціоекономічної реальності 2020: виклики для України. URL: <http://library.fes.de/pdf-files/bueros/ukraine/16344.pdf>

2. Работать ради лучшего будущего – Глобальная комиссия по вопросам будущего сферы труда / Женева: Международное бюро труда, 2019. – 88 с. URL: https://www.ilo.org/wcmsp5/groups/public/-ddgreports/---cabinet/documents/publication/wcms_662472.pdf

3. Україна на карантині: моніторинг суспільних настроїв. Результати соціологічного дослідження / Соціологічна група «Рей-

тинг», квітень 2020 р. URL: http://ratinggroup.ua/research/ukraine/ukraina_na_karantine_monitoring_obschestvennyh_nastroeniy.html

4. Закон України «Про внесення змін до деяких законодавчих актів України, спрямованих на забезпечення додаткових соціальних та економічних гарантій у зв'язку з поширенням коронавірусної хвороби (COVID-19)». URL: <https://zakon.rada.gov.ua/laws/show/540-20#Text>

Бедрата А.В.

студентка КПП ім. Ігоря Сікорського
Науковий керівник: **Головко О.М.**
к.ю.н., ст. викладач кафедри
публічного права, КПП імені Ігоря
Сікорського

ПРОБЛЕМИ ПРОВЕДЕННЯ ПРОЦЕДУРИ МЕДІАЦІЇ ЗА УМОВИ ВИКОРИСТАННЯ СИСТЕМИ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

У розпал пандемії COVID-19 у світі та Україні люди стикнулися з великою кількістю перепон, обумовлених введенням карантинних обмежень, багато-хто зіткнувся з неможливістю здійснення своїх прав та інтересів. Певних обмежень зазнали і особи, які бажали захистити свої права в судовому порядку: скасування розгляду справ, зупинення процесуальних строків, відсутність правового механізму врегулювання спору в нових умовах тощо. Це також торкнулося і процедури медіації.

Як і в інших сферах суспільного життя, довелося впроваджувати дистанційну форму проведення даної процедури, застосовувати безпечні для здоров'я учасників шляхи здійснення медіації. Одним з найбільш раціональних та ефективних варіантів взаємодії на відстані є застосування системи електронних комунікацій. Зважаючи на особливий характер медіації, постає питання, чи можливе результативне та належне проведення цієї процедури?

Щоб з'ясувати, чи можливо взагалі провести медіацію на відстані, із застосуванням системи електронних комунікацій, треба встановити, що таке системи електронних комунікацій. Відповідно до п. 21 ст. 1 закону України «Про основні засади забезпечення кібербезпеки України», системи електронних комунікацій (комунікаційні системи) – системи передавання, комутації або маршрутизації, обладнання та інші ресурси, що забезпечують електронні комунікації (у тому числі засоби і пристрої зв'язку, комп'ютери, інша комп'ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних [2]. Отже, застосуванням системи електронних комунікацій можна вважати процес використання сервісів проведення відео конференцій на технічних пристроях, яка мають доступ до мережі Інтернет.

Також варто зазначити, які специфічні ознаки має процедура медіації. Від латинського «mediatio» – здійснювати посередництво, або «mediate» – бути посередником [4]. Медіація – конференційна процедура із гнучкою структурою, де незалежна особа (медіатор) допомагає сторонам конфлікту його врегулювати у досудовому порядку, враховуючи інтереси та потреби кожної сторони та обираючи той варіант вирішення спору, який буде прийнятним для кожної сторони.

Медіація ґрунтується на принципах, які можна розділити на дві групи:

- Організаційні принципи: добровільність, неупередженість, нейтральність та поінформованість;
- Процедурні принципи: конфіденційність, рівність учасників, активність та самовизначеність.

Процедура медіації полягає у тому, щоб привести сторін до діалогу та вирішення конфлікту за сприяння медіатора, налагоджуючи контакт між учасниками конфлікту та спонукаючи їх до співпраці, тому необхідними для реалізації мети медіації є створення умов, за яких сторонам буде найбільш комфортно висловлюватися та сприймати інформацію. Краще за все це можна здійснити, пе-

ребуваючи в одному приміщенні, сидячи за «столом переговорів», проте життя диктує свої умови.

На нашу думку, медіація може бути проведена у дистанційному режимі, навіть незважаючи на складнощі із забезпеченням порядку проведення, дотриманням принципів процедури медіації, технічними питаннями та інше.

По-перше, дистанційна медіація є способом реалізації права на доступ до правосуддя, передбачене Конституцією України [1]. Медіація як спосіб вирішення спорів наразі в Україні тільки починає свій шлях розвитку, але не традиційність медіації не анулює право особи на доступ до правосуддя [3, с. 147]. В період пандемії громадяни позбавлені права на розгляд справ у судових засіданнях, але мають можливість здійснити процедури дистанційної медіації задля прискорення вирішення спору. Проте на учасників медіації покладається забезпечення технічної підтримки. Окрім цього, оскільки процедура медіації є добровільною, то учасники мають бути зацікавлені в успішному проведенні і завершенні спілкування.

По-друге, особа перебуваючи у себе вдома та спілкуючись з опонентом та медіатором почувається більш комфортно, спокійно та впевнено, тому здатна об'єктивно оцінювати аргументи іншої сторони та власні. Але водночас постає проблема із забезпеченням конфіденційності та самовизначеності, але вирішити її можливо шляхом пояснення правил поведінки учасників медіації та контролю за відсутністю стороннього впливу та фіксування через пристрої відео зв'язку.

Дотримання організаційних принципів, які більше стосуються ролі медіатора, на нашу думку, навіть може бути краще реалізоване, оскільки медіатор, перебуваючи на відстані від учасників, буде позбавлений впливу з боку третіх осіб, а вірогідність стати на бік однієї зі сторін також знизиться через відсутність суб'єктивної оцінки медіатора та людського фактору підчас зустрічі.

По-третє, у разі успішного завершення медіації учасники мають зафіксувати це в офіційних документах, що ускладнюється дистанційним режимом, проте сучасний розвиток техніки та тех-

нологій дозволяє здійснити оформлення та підписання документів навіть дистанційно, зокрема, з використанням електронного цифрового підпису.

Отже, здійснення медіації за умови використання системи електронних комунікацій є більш ускладненим у порівнянні з проведенням процедури в режимі особистих зустрічей, але не можна сказати, що дистанційний формат є неполадною перешкодою для проведення цієї процедури. До того ж рівень розвитку сучасних технологій дозволяє проводити зустрічі у відео форматі на належному рівні, фіксувати їх хід, а також результати.

Література:

1. Конституція України. Відомості Верховної Ради України від 28 червня 1996 р. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text> (дата звернення: 30 листопада 2020 р.).
2. Про основні засади забезпечення кібербезпеки України: Закон України. Відомості Верховної Ради України № 2163-VIII від 5 жовтня 2017 р. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 3 грудня 2020 р.).
3. Головка О. М. Право на інформацію щодо альтернативних методів вирішення спорів. Інформація і право. 2019. Вип. № 1 (28). С. 144-151
4. Леко Б., Чуйко Г. Медіація: підручник. Чернівці: Книги – XXI. 2011. С.162.

Бруслік А.В.

студент Національного університету
біоресурсів і природокористування
України

Науковий керівник: Хвіст В.О.

кандидат історичних наук, доцент
Національного університету
біоресурсів і природокористування
України

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ В УМОВАХ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ

В останні роки у перспективах розвитку Інтернет-сфери набуває активного поширення словосполучення «Інтернет речей». Як зазначається у понятті «Інтернет речі» (скорочено ІТ, англ. – Internet of Things) розглядається як фізично реальні системи і комплекси, функціонування яких базується на використанні величезної кількості датчиків, комп'ютерних і телекомунікаційних технологій, робототехніки, штучного інтелекту, хмарних обчислень, мережі Інтернет, застосування яких надає можливості за участю або без участі людей приймати і реалізовувати рішення. Завдяки інтернету задовольняються інформаційні, економічні та інші потреби. З появою ІТ у людства з'явилися великі можливості, але з приходом можливостей приходять і велика відповідальність. З'явилась потреба в ефективному правовому регулюванні, що забезпечить безпечне використання ІТ по всьому світу. Метою даної роботи є розгляд можливих проблем правового регулювання в умовах застосування технологій інтернету речей та пошук можливих рішень.

Провідні позиції у світі щодо правового забезпечення використання технологій ІТ займають країни Європейського Союзу, США, Японія, КНР, Італія. Безумовно, правове регулювання має сприяти використанню технологій ІТ в інтересах людей. Але, на жаль, інтереси людей не завжди бувають законними та правомірними. Ознайомившись з працями Баранова О.А. не мож-

на не згадати правові проблеми використання нових технологій які безпосередньо взаємодіють в умовах інтернет речей. Для вирішення таких проблем в першу чергу необхідно встановити правові вимоги, щодо запобігання незаконному перехвату програм, що відповідають за дії тих самих 3D принтерів, дронів, робомобілів тощо [5, с. 10]. Зараз гостро стоїть питання правового регулювання щодо використання людьми ІТ. Погоджуючись з Пилипчуком В. Г., треба дійсно наголосити на тому, що в різноманітних системах Інтернет речей використовується і буде використовуватися багато персональних даних. До ключових проблем Інтернету речей можна віднести саме безпеку і захист персональних даних. Технології Інтернет речей значно посилюють ризики порушення конфіденційності персональних даних внаслідок того, що вони передбачають накопичення, циркуляцію і використання великого, територіально і технологічно розподіленого обсягу інформації (даних) про конкретну людину. Це викликає цілком закономірні питання про надійність зберігання цих даних і правового забезпечення їх захисту від несанкціонованого використання [6, с. 17]. Ще більшою проблемою є правове регулювання всіх процесів в електронній мережі, які здійснює та чи інша персона. На даний момент не існує ефективного, єдиного методу ідентифікації конкретних осіб причетних до незаконних діянь що призвели до втрати персональних даних конкретної особи. Адже лише використання проксі-серверів вже робить користувача анонімним. Згідно основоположних принципів міжнародного права про захист персональних даних, затвердженими першою у світі Конвенцією Ради Європи № 108 від 28.01.81 р. та рядом директив Європейського Союзу, зокрема Директивою Європейського Парламенту і Ради 95/46/ЄС від 24.10.95 р., стосовно захисту персональних даних, захист прав людини у сфері персональних даних передбачає, зокрема, наступне: «Персональні дані, що піддаються автоматизованій обробці: а) отримуються та обробляються сумлінно та законно; б) зберігаються для визначених і законних цілей та не використовуються у спосіб, несумісний з цими цілями; с) мають

бути адекватними, відповідними і не надмірними з точки зору цілей, для яких вони зберігаються» [2, с. 10].

Близько 8 років тому була створена перша криптовалюта світу «біткоїн». Специфічна природа криптовалюти зумовлює те, що відповідне питання не є першочерговим для вирішення. Але необхідність втручання держави в особі її органів була зумовлена тим, що біткоїн став платіжним засобом діяльності Даркнету, анонімна мережа, яка на сьогодні активно функціонує в мережі Інтернет по всьому світу, яка схожа на чорний ринок, де можна придбати зброю, наркотики, людей, фальшиві гроші та документи. США, Німеччина, Японія, Франція, Фінляндія та інші країни не тільки дозволили обіг відповідної валюти, але й законодавчо закріпили чи підкріпили правовий режим, роз'яснили поняття біткоїнів та аналогів сформували відповідну судову практику. На жаль, піддаючись загальній тенденції чимало держав все-таки не встановлює режиму щодо криптовалюти через її специфічну природу. До таких держав відноситься і Україна. Проблемаю, яка є найбільш фундаментальною і очевидною, є правова природа криптовалюти.

З вище описаного можна зробити висновок, що на міжнародному рівні сьогодні відсутня єдність в розумінні правової природи криптовалюти, тому держави по-різному визначають поняття біткоїна і його аналогам. Європейська судова практика по суті прирівняла криптовалюту до законного платіжного засобу, а обмін грошових коштів – «валютно-обмінною операцією». Але все-таки, згідно чинного законодавства ЄС цифрова валюта вважається товаром і підпадає під регулювання Цивільного законодавства і Директиви ЄС про ПДФ як товар, а договір купівлі–продажу щодо криптовалюти є договором купівлі–продажу товару [3, с. 2].

Щодо застосування штучного інтелекту, необхідно буде вирішити дуже багато правових проблем в регулюванні пов'язаних з тією обставиною, що людина – біологічна істота, а робот – ні. Перш за все, це проблеми визначення для роботів понять, критеріїв, змісту та обсягів правоздатності, дієздатності і деліктоздатності; вирішення проблеми встановлення для роботів спеціальної або загальної правосуб'єктності і багато інших. Іншими словами,

роботи розглядаються як людиноподібні суб'єкти, які здійснюють людиноподібні дії в процесі відносин з традиційними суб'єктами. Якщо дії традиційних суб'єктів в таких відносинах підлягають правовому регулюванню, то логічно припустити, що інша сторона також є суб'єктом цих правовідносин. Якщо робот-андроїд або андроїд повинен нести юридичну відповідальність за свої дії, тоді він повинен мати фізичну, юридичну та цифрову ідентичність, подібну людині. І якщо у робота є ті ж юридичні обов'язки, що і у людини, хіба в нього не повинні бути такі ж юридичні права, як у людини? [1, с. 14]

Розглянувши дану тему, можна стверджувати що без чіткого механізму правового регулювання, сучасні технології перетворять наше життя на хаос, за яким може прийти не тільки стагнація, але й війна. Завершити хотілося б словами Річарда Хукера, які як ніколи описують розвиток сучасних технологій: «Будь-яка зміна, навіть зміна на краще, завжди пов'язана з незручностями» [3, с. 1].

Література

1. Інтернет речей: проблеми правового регулювання та впровадження / Баранов О. А. // Інтернет речей (IoT): огляд правових проблем. – 2017. – № 2, 3. – С. 14.
2. Баранов О.А. Інтернет речей (IoT): мета застосування та правові проблеми / О.А. Баранов // Інформація і право. – 2017. – № 2. – С. 7-15.
3. Плита А.І. Есе з права ІТ: криптовалюта: її правовий режим, проблеми застосування. – 2017. – абзац 2-7.
4. Баранов О.А., Захист персональних даних в сфері Інтернет речей. – 2017. – С. 85-91
5. Інтернет речей: проблеми правового регулювання та впровадження / Баранов О. А. // Інтернет речей (IoT): огляд правових проблем. – 2017. – № 3. – С. 11-12.
6. Інтернет речей: проблеми правового регулювання та впровадження / Пилипчук В. Г. // Становлення і регулювання суспільних відносин у сфері новітніх інформаційних технологій. – 2017. – № 2. – С. 17.

Іванів І.Р.

студентка КПІ ім. Ігоря Сікорського

Науковий керівник: **Дубняк М.В.**

к.ю.н. старший викладач КПІ ім. Ігоря
Сікорського

ЦИФРОВА ТРАНСФОРМАЦІЯ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я

Медицина завжди була однією з пріоритетних напрямів реформування на державному рівні. В сучасних умовах, у зв'язку із поширенням вірусу COVID-19, виникла нагальна необхідність в удосконаленні управління цією сферою.

Конституцією України визначено, що людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Саме тому право на охорону здоров'я та медичну допомогу є одним із основоположних невід'ємних прав людини. З огляду на це, впровадження інформатизації в закладах охорони здоров'я є особливо актуальним. Правильно реалізована система управління системою закладів охорони здоров'я сприяє підвищенню рівня реалізації прав пацієнтів, про що свідчить практичний досвід європейських держав та США.

В Україні до цього часу залишаються невирішеними питання нормативного регулювання інформатизації сфери охорони здоров'я: немає повного обсягу необхідних галузевих нормативно-правових актів (у тому числі гармонізованих стандартів із медичної інформатики) щодо розроблення, впровадження, експлуатації та розвитку інформаційних ресурсів, інформаційних технологій і засобів інформатизації; відсутні формалізовані критерії визначення економічної ефективності їх впровадження та експлуатації [1, с. 6].

При цьому, у 2017 році в Україні розпочалась реформа системи охорони здоров'я, що полягає в зміні системи фінансування та запровадженні принципу “гроші ходять за пацієнтом”. Важливим інструментом впровадження реформи є створення сучасної елек-

тронної системи, що дозволить значно підвищити ефективність та прозорість охорони здоров'я, а саме: систему e-Health [4].

Ця система повинна вирішити основні проблеми захисту прав пацієнта та підвищити якість надання медичних послуг. З огляду на це, концепція інформатизації системи охорони здоров'я базується на наступних принципах:

1. Орієнтованість на пацієнта – означає безперервне накопичення та зберігання даних з прив'язкою до облікового запису пацієнта в системі, його ЕМК, надання пацієнту, як суб'єкту персональних даних, можливості керувати власними медичними даними, доступом до них. Реалізація цього принципу призводить до того, що “медичні дані ходять за пацієнтом” при зміні пацієнтом лікаря або закладу, що надає пацієнту медичні послуги.

2. Пріоритет електронної форми – при створенні, обміні та зберіганні даних пріоритет має електронна форма даних, що обробляється із застосуванням ІКТ.

3. Єдиний медичний інформаційний простір – створення умов сумісності/інтеграції та можливості передавати дані між системами в рамках Е-здоров'я, гармонійний взаємозв'язок із суміжними галузями та сферами як на рівні України так і на міждержавному, для подальшої інтеграції з відповідними системами в ЄС. Єдине інформаційне середовище створюється за допомогою міжнародних технічних стандартів обміну інформацією, термінологічних словників, класифікаторів у сфері медицини/охорони здоров'я та технічних рішень [3].

Досвід інформатизації галузі охорони здоров'я в окремих регіонах країни свідчить про те, що впровадження цифрових технологій призвело до підвищення якості управління медичною, адміністративною та фінансовою діяльністю організації охорони здоров'я за рахунок комплексного впровадження електронної медичної картки та електронного талона; скорочення часу оформлення медичної документації; скорочення термінів надання звітів та реєстрів послуг; оптимізація штату медичного персоналу закладу; забезпечення оперативного контролю за показниками роботи, експертизи якості надання медичної допомоги; виключення

ручної праці; підвищення достовірності інформації про показники лікувально-діагностичної роботи та фінансової діяльності; підвищення пропускної здатності амбулаторно-поліклінічних організацій за рахунок скорочення часу роботи з амбулаторною картою та іншими документами, і як наслідок – скорочення черг [2].

Таким чином, як вбачається з вищевикладеного, інформатизація системи охорони здоров'я сприятиме забезпеченню прозорості фінансування цієї галузі, зробить доступною для пацієнта інформацію про стан його здоров'я. Більше того, впровадження таких технологій сприятиме розвитку медичного ІТ-ринку, тобто створить простір для інновацій, що допоможуть автоматизувати роботу медичних закладів в Україні.

Список використаних джерел:

1. О. П. Мінцер Інформатизація охорони здоров'я: проблеми, розв'язані та нерозв'язані. Питання впорядкованості та сингулярності. Медична інформатика та інженерія. 2013. Вип. 2. С. 5-11.
2. Програма «Інформатизація галузі охорони здоров'я м. Вінниці на 2016-2020 роки»: Рішення Вінницької міської ради від 25.12.2015 № 38. – URL: <https://www.vmr.gov.ua/Docs/CityCouncilDecisions/2015/%E2%84%9638%2025-12-2015%20%D0%9F%D1%80%D0%BE%20%D0%B7%D0%B0%D1%82%D0%B2%D0%B5%D1%80%D0%B4%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F.pdf>
3. Розпорядження Міністерства охорони здоров'я України «Про схвалення Концепції реформи фінансування системи охорони здоров'я» від 30 листопада 2016 року № 1013-р.
4. Розпорядження Міністерства охорони здоров'я України «Про схвалення Концепції розвитку системи громадського здоров'я» від 30 листопада 2016 року № 1002-р.

Пономарьов К.С.

студент КПП ім. Ігоря Сікорського

Науковий керівник: **Головко О.М.**

к.ю.н., ст. викладач КПП ім. Ігоря
Сікорського

ПРОЦЕДУРА МЕДІАЦІЇ В УКРАЇНІ В УМОВАХ КАРАНТИННИХ ОБМЕЖЕНЬ

До початку пандемії та запровадження карантинних обмежень в Україні, практика медіації як альтернативного способу вирішення спорів набувала більшої поширеності як на теренах нашої держави, так і в усьому світі. Навряд чи можна виділити єдиний причинно-наслідковий зв'язок між світовими подіями та поширенням медіації, але очевидним є те, що активний розвиток економічної свободи у світі, відкриття кордонів, глобалізація, демократизація та поширення ділової активності протягом останнього часу є одними з ключових факторів, які сприяють зростанню конфліктних ситуацій і суперечок між учасниками різних правовідносин в господарській, цивільно-правовій, трудовій, кримінальній, сімейній та інших сферах.

В результаті у багатьох країнах державні суди перевантажені суперечками різних категорій, часто відсутні або не дотримуються нормативи навантаження, порушуються терміни розгляду справ, знижується реальне виконання судових актів [1, с. 79].

Щодо України, незважаючи на поширення практики медіації в останні роки, судочинство в державних судах було та залишається найбільш звичним і поки найпоширенішим способом вирішення спорів, частково через відсутність належної правової бази для медіації в нашій країні, частково через корупційну складову [2].

Однак, у період введення карантинних обмежень саме медіація може стати новим ефективним способом вирішення спорів. Незважаючи на відносно швидке реагування законодавчої гілки влади та впровадження законодавства, яке мало на меті створення та перезавантаження процесуальних механізмів для вирішення

спорів у суді дистанційно, деякі експерти виділяють недосконалість та непридатність цих механізмів для розвантаження судової системи, що створює нові перспективи поширення практики медіації в Україні [3].

Закон України «Про внесення змін до деяких законодавчих актів України, спрямованих на забезпечення додаткових соціальних та економічних гарантій у зв'язку з поширенням корона-вірусної хвороби (COVID-19)» № 540-IX від 30.03.2020 р., прийнятий 30 березня 2020 року (далі – Закон), мав на меті внесення до процесуальних кодексів додаткових положень з приводу впровадження дистанційного правосуддя. Звернувши увагу на думку експертів та самостійно проаналізувавши деякі з нововведень Закону, можна зробити висновок, що впроваджені зміни не стали ефективним рішенням через низку юридичних прогалин які не тільки не спрощують, але подекуди й ускладнюють судовий процес. Можна виділити та окреслити кілька таких ризиків.

Одним з основних ризиків є положення вищезгаданого Закону про автоматичне продовження строків звернення до суду та процесуальних строків у цивільних, господарських та адміністративних справах на строк дії карантину. Фактично ухвалені зміни перешкоджатимуть суду здійснювати провадження в будь-якій цивільній, господарській чи адміністративній справі, оскільки невчинення однією із сторін будь-якої процесуальної дії (наприклад, неподання відзиву на позов) змушуватиме суд очікувати до закінчення карантину. Такі положення можуть призвести до того, що розгляд цивільних, господарських та адміністративних справ на час карантину повністю зупиняться у разі якщо хоча б одна зі сторін не проявляє активність. Законодавцю слід було би передбачити встановлення на законодавчому рівні повноваження суду за заявою учасника справи визнавати поважною причину пропущення строку, якщо вона зумовлена карантинном, але через те, що таке положення не було передбачене, можна було спостерігати затягнення розгляду справ та ще більше завантаження судів у період послаблення карантинних обмежень.

Крім того, одним із положень Закону у судовому процесі суттєво обмежується один з основоположних принципів судочинства – гласність. Так, суду надається право обмежити доступ в засідання осіб, які не є учасниками процесу, якщо участь у судовому засіданні становитиме загрозу життю чи здоров'ю особи. Дане положення застосовується лише для господарського та цивільного процесу, але не застосовується для адміністративного. Очевидно, що у таких умовах, якщо справи стосуються соціально значимої інформації, суттєво підвищуються ризики зловживань, в першу чергу, через відсутність критеріїв обмеження доступу відвідувачів в судові засідання.

Законом не передбачається ані критерій соціальної дистанції, який би дозволив доступ в засідання при дотриманні такого критерію, ані можливість долучитися до судового засідання як вільний слухач через відео-зв'язок.

Можна передбачити як короткострокові, так і довгострокові тяжкі наслідки обмеження принципу гласності, серед яких можна виділити підвищення корупційних ризиків по справах, які розглядаються саме на час карантинних обмежень та ще більша зневіра громадян в необ'єктивності й неупередженості представників судової гілки влади, що йде на додаток до вже існуючих випадків створення штучних перепон у здійсненні публічного розгляду справ судами [4, с. 15].

Також, одним з нововведень Закону є передбачене положення про право учасників справи брати участь у судовому розгляді в режимі відео-конференції. Дане нововведення доволі важко назвати справді новим, тому що фактично статтею 11 Закону України «Про судоустрій і статус суддів», а також такими процесуальними кодексами як КАС України, ГПК України та ЦПК України, КПК України давно передбачено надання учасникам аналогічної можливості участі в режимі відео-конференції. По суті, вищезгаданий Закон просто дублює вже встановлені положення, але не вирішує актуального для українського судочинства питання впровадження дієвої та всеосяжної системи Електронного суду, яка б знімала навантаження з судової системи.

На даний момент практика проведення відео-конференцій та дистанційного залучення сторін у спорах є доволі розповсюдженою (так, при апеляційному оскарженні ухвал слідчих суддів відео-конференц-зв'язок використовується у 24,7 відсотках випадків). Тим не менш виділяються деякі недоліки, серед яких випадки відкладання засідань через технічні проблеми або з інших організаційних питань, які перешкоджають реалізації права українських громадян на справедливий суд [4, с. 44].

Як вже зазначалося, досі невирішеним є питання впровадження системи Електронного суду, повноцінне створення якої могло б вирішити технічні та організаційні прогалини дистанційного судового процесу. Наразі в Україні діє тестовий режим Єдиної судової інформаційно-телекомунікаційної системи (ЄСІТС), яка б дозволила перевести судовий процес в повністю дистанційний формат. Впровадження цієї системи у найближчий час все ще є неможливим, незважаючи на необхідність викликану пандемією. Хоча деякі елементи ЄСІТС, наприклад електронні звернення вже працюють, остаточний її запуск планується лише на 2023 рік [5, с. 28].

Звернувши увагу на проблеми, з якими стикаються учасники судового процесу під час пандемії та проаналізувавши деякі прогалини національного законодавства, яке мало на меті створення та перезавантаження процесуальних механізмів для ефективного вирішення спорів у суді на момент карантину, можна звернути увагу на те, що в умовах пандемії медіація як альтернативний метод вирішення спорів між сторонами, набуває ще більшої актуальності. Дана процедура в перспективі може стати необхідним механізмом досягнення справедливості на рівні з іншими альтернативними способами вирішення спорів (програми Alternative Dispute Resolution, далі – ADR).

Саме такі переваги процедури медіації як швидкість та економічність, менша зарегламентованість, більша гнучкість та відсутність жорстких процедурних правил в порівнянні з судовими механізмами можуть не просто привести до поширення цієї практики на період пандемії, але й підштовхнути законодавців до вирі-

шення проблеми, яка стоїть на заваді розвитку цієї практики саме в нашій країні – відсутності спеціального закону, який би регулював процедуру медіації.

Незалежність процесу медіації від роботи будь-яких інституцій та держави дає шанс розвантажити судову гілку влади та, у ширшій перспективі, створити кращі умови для громадян для захисту власних прав та справедливого вирішення конфліктів без затримок та незручних формальностей під час пандемії.

Слід сказати, що завдяки появі нових ризиків, які стають на заваді судочинства, та тим умовам, в яких опинилася держава, громадяни та бізнес під час пандемії створює позитивні передумови для використання перспективного напрямку у формі впровадження процедури медіації на постійній основі із застосуванням можливості її реалізації з використанням дистанційних комунікацій.

Література

1. Медіація у професійній діяльності юриста : підручник / авт. кол.: Т. Білик, Р. Гаврилюк, І. Городиський [та ін.] ; за ред. Н. Крестовської, Л. Романадзе. – Одеса : Екологія, 2019. – 456 с.
2. Матат А. В., Угринович М. А. Дистанційне правосуддя: зараз або ніколи. *Аналітично-адвокаційний центр «Центр демократії та верховенства права* (Електронний ресурс), 2020. URL: <https://cedem.org.ua/analytics/dystantsijne-pravosuddya/> (Дата звернення 05.12.2020).
3. «Ухвалений закон для боротьби з коронавірусом створює ризик “заморожування” правосуддя». *Центр політико-правових реформ* (Електронний ресурс). 30.03.2020. URL: <https://www.pravo.org.ua/ua/news/20874314-uhvaleniy-zakon-dlya-borotbi-z-koronavirusom-stvoryue-rizik-zamorogeuvannya-pravosuddya#> (Дата звернення 05.12.2020)
4. Спеціальна доповідь Уповноваженого Верховної Ради України з прав людини за результатами пілотного моніторингу застосування нового Кримінального процесуального кодексу України судами м. Києва – К.: «Арт-Дизайн», 2015. – 132 с.
5. Наказ Державної судової адміністрації України від 07.11.2019 № 1096 «Концепція побудови єдиної судової інформаційно-телекомунікаційної системи» (Електронний ресурс). URL: https://dsa.court.gov.ua/userfiles/media/media/ECITC_Koncepcia.pdf (Дата звернення 05.12.2020).

Радченко К.В.

магістр міжнародних економічних
відносин, студентка магістратури
Інституту Права Київського
національного університету імені
Тараса Шевченка

ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ ОБІГУ ВІРТУАЛЬНИХ АКТИВІВ

Правова детермінація природи та функціоналу віртуальних активів є надзвичайно актуальним питанням у контексті двох ключових аспектів:

(1.) захисту прав широкого кола стейкхолдерів, що де-факто здійснюють різноманітні активності з віртуальними активами, від проведення трансакцій (ще з моменту появи перших криптовалют) та інвестування до таких новітніх форм, як цифрова ідентифікація, захист авторського права на цифрові об'єкти, тощо;

(2.) виконання рекомендацій FATF (Група розробки фінансових заходів боротьби з відмиванням грошей) та інших міжнародних стандартів, у тому числі спеціальних нормативних актів та рекомендацій ЄС. [6]

Варто відмітити, що дослідники виділяють три найбільш поширених підходи до правового регулювання обігу віртуальних активів, а саме аналогія закону (поширення дії чинних правових актів на відносини щодо обігу віртуальних активів), внесення зміни до чинних правових актів (часткова адаптація до відносин у сфері обігу віртуальних активів), прийняття спеціального нормативно-правового акту, що регулює виключно питання, пов'язані з обігом віртуальних активів. [2]

Серед основних напрямків регуляторних підходів чимало дискусій викликає юридичне визначення терміну “віртуальний актив”, оподаткування операцій з віртуальними активами, захист персональних даних (реалізація положень GDPR, зокрема права на забуття та стирання даних), статус віртуальних активів, як об'єкта цивільних прав, декларування віртуальних активів та інше.

Міністерство Цифрової Трансформації України розглядає віртуальні активи, як один із пріоритетних напрямків формування та реалізації цифрової політики. [1] Із 2017 року велися спроби закріпити статус віртуальних активів на законодавчому рівні (зарєєстровані законопроекти № 7183 про обіг криптовалюти в Україні та № 7183-1 про стимулювання ринку криптовалют та їх похідних в Україні). [5] Перше визначення віртуальних активів було надано у ЗУ 361-9 від 06.12.2019 “Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення”, що віддзеркалювало визначення FATF. [3], [6]

02 грудня 2020 року у першому читанні було прийнято законопроект №3637 «Про віртуальні активи», який визначає правове поле обігу віртуальних активів, права та обов’язки учасників ринку, засади державної політики у сфері обігу віртуальних активів, надає правові дефініції, втілюючи рекомендації FATF. [4] У документі визначається регулятор ринку (Мінцифра, в окремих випадках НБУ та НКЦПФР), міститься перелік професійних постачальників послуг віртуальних активів та відомості про реєстрацію. Віртуальний актив розглядається, як нематеріальне благо, особливості обігу якого визначаються Цивільним кодексом України та цим Законом. [4]

Зважаючи на високе значення прийняття цього законопроекту, варто відмітити його систематичний та комплексний підхід. У той же час, важливо наголосити, що де-факто існують різні категорії токенів, що підпадатимуть під надане визначення віртуальних активів. FINMA, наприклад, робить акцент на необхідності диференціації підходів щодо кожного з видів токенів. [7] Такий підхід використовується у США та Швейцарії, і його було б важливо закріпити на первинному рівні, саме в законопроекті, а не тільки в подальшій діяльності регулятора. Сам перелік професійних постачальників послуг віртуальних активів варто було б розширити, зважаючи на практики провідних країн, що легалізували віртуальні активи та надали набагато ширші переліки. Необхідно звернути більшу увагу на моніторинг імплементації окремих положень

законопроекту, розробку більш детального підходу щодо захисту ПД в операціях з віртуальними активами.

Таким чином, з огляду на фактичну активність на ринку віртуальних активів, необхідність захисту стейкхолдерів, адаптації законодавства до стандартів ЄС та FATF, правове визначення правового поля та “правил гри” є важливим питанням. В Україні спостерігається позитивний тренд активності щодо спроб правового регулювання віртуальних активів. У разі прийняття законопроекту №3637, Україна отримає ряд економіко-правових, що сприятиме діджиталізації, однак автор тез акцентує на важливості первинної диференціації різновидів токенів, розширення переліку та більшому акценті на моніторингу імплементації та підходів до захисту ПД.

Список використаних джерел:

1. Мінцифри – Регулятор Ринку Віртуальних Активів [Електронний ресурс] – Режим доступу до ресурсу: <https://thedigital.gov.ua/news/mintsifra-regulator-rinku-virtualnikh-aktiviv>.
2. Забродська, О. (2020). Правове регулювання обігу віртуальних активів.
3. ЗУ Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення [Електронний ресурс] – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/1702-18#Text>
4. Проект Закону Про обіг криптовалют в Україні [Електронний ресурс] – Режим доступу до ресурсу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62684
5. Проект Закону Про стимулювання ринку криптовалют та їх похідних в Україні [Електронний ресурс] – Режим доступу до ресурсу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62710
6. Financial Action Task Force (FATF). Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris, 2019. [Електронний ресурс] – Режим доступу до ресурсу: <http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf>
7. FINMA – Types of Tokens [Електронний ресурс] – Режим доступу до ресурсу: https://medium.com/@marketing_41605/token-options-4f66af313c18.

Фарадж Д.Ю.

магістр права, військовослужбовець
ЗСУ

Науковий керівник: **Фурашев В.М.**

к.т.н., с.н.с.

ЮРИДИЧНА ВІДПОВІДАЛЬНІСТЬ РОБОТОТЕХНІКИ ЗІ ШТУЧНИМ ІНТЕЛЕКТОМ

В епоху 21 століття наш світ дуже стрімко розвивається в галузі новітніх технологій, а особливо в галузі робототехніки та роботи-зації. Вже давно ні для кого не є новиною такі поняття як: «робототехніка з елементами штучного інтелекту», «робот зі штучним інтелектом «та сам «штучний інтелект».

На сьогоднішній день наука в галузі штучного інтелекту настільки просунулась вперед, що ми можемо бачити як певні речі, які колись здавалися якимись вигадками або казками дійсно існують.

В багатьох галузях життєдіяльності для полегшення людської праці, вже давно почали залучати роботів. Однак, якщо раніше це були такі механізми, як «рука-маніпулятор», які мали одну чи дві функції спрямованих на полегшення тяжкої праці людини, в основному на заводах автомобільної промисловості та на певних інших підприємствах, то на сьогоднішній день вже залучають роботів з такою кількістю функцій, які можуть замінити людину у будь-якій сфері життєдіяльності.

Людина на даний час може вже не виходити з дому, навіть не вставати з ліжка, а робота за неї буде виконуватись. Однак зі стрімким розвитком сфери штучного інтелекту людина може стати просто не потрібною. Особливо це стосується таких сфер забезпечення життєдіяльності де роботи можуть працювати цілодобово, їм не потрібно виплачувати щомісячну заробітну платню, єдиними витратами будуть лише витрати на підтримку їх працездатності. Також багато професій можуть стати не потрібними або заміненими. В такому випадку зросте відсоток безробіття.

На сьогоднішній день технології штучного інтелекту, стрімкого розвитку набули в сфері автомобільної промисловості, тобто маємо на увазі автомобілі «Tesla» компанії «SpaceX» Ілона Маска. На сьогодні ці автомобілі використовуються для пасажирських перевезень, а також планується розробка певних автомобілів цієї ж фірми для вантажних перевезень. Ці автомобілі можуть керуватись без водія автопілотом. Програма штучного інтелекту запрограмована так, що водій в даній машині не обов'язково має бути присутнім.

Так само можна згадати першого робота який отримав громадянство, а саме робот зі штучним інтелектом «Софія», яка на сьогоднішній день являється громадянкою Саудівської Аравії.

Ще є безліч сфер куди запроваджують технології штучного інтелекту. Однак постає питання щодо юридичної відповідальності робота чи системи зі штучним інтелектом. Хто все ж таки має нести відповідальність за правопорушення робота чи системи зі штучним інтелектом які не керувались на пряму людиною, а були запрограмовані на виконання певних функцій ?

Ніхто не застрахований від того що робот зі штучним інтелектом чи система штучного інтелекту може надати збій в роботі. Відповідальність за правопорушення можуть нести фізичні та юридичні особи, але для цього дана відповідальність має бути прописана в нормативно-правових актах, тобто повинні бути розроблені або внесені зміни до вже існуючих нормативно-правових актів, зокрема Кримінального кодексу України та Кодексу України про адміністративні правопорушення, щоб можна було чітко розділяти вид відповідальності, санкцію та хто саме буде нести відповідальність за певне правопорушення.

Зі стрімким розвитком сфери штучного інтелекту, вже скоро всьому людству доведеться поділяти своє існування в середовищі з існуванням роботів зі штучним інтелектом. Тому доцільно було б прискорити розгляд питань, яке вже почалось розглядатися на міжнародному рівні, щодо надання правового статусу майбутнім роботам зі штучним інтелектом, тобто визнання їх суб'єктами правовідносин та надання статусу «електронної особи».

Однак, що стосується правової відповідальності та надання правового статусу роботам зі штучним інтелектом, то це реально запровадити лише у випадку, якщо штучний інтелект не візьме «верх» над людством та не вийде із під контролю.

Якщо наділити штучний інтелект правосуб'єктністю та надати правового статусу, то було б доцільно застосовувати такі ж види юридичної відповідальності, як і до людей, також з санкціями. Максимальна міра покарання була б «юридична смерть» штучного інтелекту, тобто абсолютне припинення діяльності певних функцій штучного інтелекту.

Загорулько В.М.

студент Національного університету
«Одеська юридична академія»

Науковий керівник: **Дробчак А.Л.**
старший викладач Національного
університету «Одеська юридична
академія»

PROBLEMS OF LEGAL REGULATION OF THE USE OF ARTIFICIAL INTELLIGENCE IN IT

In further legal research in terms of regulating public relations related to IP technologies using AI, we propose to use the concept of «robot», in the first approximation, presenting it as the integration of some technical system with AI, which creates real opportunities for objectification in the real world results of the implementation of artificial intelligence of some cognitive functions.

Before proceeding to further research, we note that for the system of law to define a scientifically sound definition of the term «robot», as well as any other terms that have a significant technical content, is important for several reasons.

First, an “incomplete” definition of the term may create risks for the creators of IP technologies with robots due to certain inequalities between entities whose activities will be subject to regulation under the

use of robots of a certain class, and entities that do not will be subject to regulation because they will use another class of robots that is not covered by the definition of the term «robot». In practice, this situation can be a catalyst for distortion of the competitive environment for both manufacturers of IP technologies with robots, and for those who will use them. In addition, it may create certain risks for users of IP technology with works whose operation will not be covered by the relevant legal regulations.

Second, «excessive» definition of the term «robot» may lead to the fact that the robot class will include other technical devices with software that does not meet the characteristics of AI, and therefore the activities associated with such devices will be subjected to excessive legal regulation.

Third, the definition of the term «robot» should be quite flexible and abstract, and not contain unnecessary technical detail. And in order to comply with the principle of technological neutrality in legal regulation, this definition should not contain specific technical details of the implementation of a certain class of robots, which on the one hand can dramatically reduce the universal nature of the definition, and on the other – lead to its constant modernization. technical progress.

Fourth, the definition of the term «robot» should be such that in the process of law enforcement does not provoke disputes, which in their content will be difficult to resolve, especially in the early stages of the use of IP with robots.

Given these conditions, the definition of the term «robot» can help create favorable conditions for legal certainty and, if possible, unambiguous legal regulation of activities based on the use of IP technologies with robots, which, among other things, will have a positive impact on the investment climate in the segment of production and use of IP technologies.

Taking into account the results of previous research and the above requirements, we offer the following definitions of classification definitions:

- simple robot (simple robot) – the integration of applied AI and technical system that allows you to implement one or more

cognitive functions of man in the process of carrying out a particular activity, usually associated with homogeneous objects that have tangible or intangible content;

- robot android (robot android) – the integration of general AI and technical system that allows you to implement many cognitive functions in the process of carrying out any activity without human intervention, associated with various objects that have tangible or intangible content;
- android (android) – the integration of super AI and technical system that allows you to implement a full set of cognitive functions in the implementation of any previously known or unknown activities without human intervention, associated with various known or previously unknown objects having a material or intangible content.

A simple robot is something that humanity has long used and what is commonly called an automatic (autonomous) system. Thus in automatic systems any concrete CF of the person with this or that degree of similarity was realized. There are many examples of automatic systems that are equivalent to human activity, but without his participation. These are: the simplest systems for regulating temperature, voltage, speed, volume, pressure, level or flow; alarm, fire extinguishing or backup power supply systems; washing machines, ATMs or cruise control in the car; moonwalkers and rovers; numerically controlled machines and the first looms and much more.

The robot, in the understanding of I. Azimov, corresponds to the proposed classification of android. We can assume that the android, having a full set of human cognitive functions, as well as possessing feelings, emotions, experiences and consciousness will be a kind of “subject” in the relationship with man and his peers. Android and people can actually form a quality

1 hybrid society, which will function and exist in a new system of law.

The prospect of super AI and androids seems distant to many experts. According to various estimates, it is from two to six decades. At the same time, we see the growing scale of the use of a class of

simple robots, due to the great variety of their species and types, each of which differs either in the set of implemented cognitive functions, or their quality indicators. And, most likely, the success of the use of simple robots will certainly stimulate more and more intensive efforts to develop both general AI and super AI, which automatically means the widespread use of both android robots and androids.

Therefore, we consider it appropriate to listen to the opinion expressed in the Parliament of the European Union: in the context of a new era in human development, when increasingly complex works, bots, androids and other manifestations of artificial intelligence seem to be catalysts for a new industrial revolution. will leave no stratum of society untouched, for the legislature it is vital to calculate the legal and ethical consequences. In the last decade, this or that interpretation has been discussed at numerous world and national forums, congresses and conferences devoted to the Internet of Things, robots or artificial intelligence. However, an unambiguous answer on the ways and means of implementing the recommendations expressed in the European Parliament has not yet been formulated.

Based on the content of discussions on the prospects of legal regulation in the application of IP technology and the use of AI, we can state the existence of three main hypotheses, which actually determine the main content of scientific approaches to improving or reforming legal systems due to the use of robots:

- works are the object of social relations, and hence the object of legal relations;
- works are the subject of social relations, and therefore can be the subject of legal relations;
- works can be both an object and a subject of public relations, and therefore can be both an object and a subject of legal relations.

The third hypothesis is a superposition of the first two, and if these first two hypotheses are true, it will also hold, so in what follows we will consider only the first two hypotheses.

Of course, many researchers of the issue of legal regulation in the use of artificial intelligence, primarily on the basis of centuries of experience, hopefully pay attention to historically proven legal

mechanisms for regulating public relations, suggesting that they will avoid threats that may be caused by the use of robots, and which recently began to talk about the leaders of modern science and technology, and on the other – to create the most favorable conditions for investment and to achieve all the positive that gives a large-scale use of robots. But on the other hand, many scientists, such as MV Karchevsky, suggest that in the near future systems (works) with AI may be the subject of legal relations

Problems of legal regulation of cryptocurrency application

The reasons for granting cryptocurrency and its certain settlement were due to the fact that companies, especially startups, began to use it actively, there were various exchanges, insurance companies that were not afraid of various risks with non-standard money. On the other hand, the need for government intervention in the face of its organs was that bitcoin became a means of payment for Darknet, an anonymous network that is now active on the Internet around the world, which is like a black market where you can buy weapons, drugs, people, counterfeit money and documents, and if necessary, you will even be offered killer services. Unfortunately, following the general trend, many states still do not establish a regime for cryptocurrency due to its specific nature. Authorities are trying to explain the essence of bitcoin and its analogues, but the question of the legal nature is unresolved. These include Ukraine, Chile, Brazil, Denmark, Malaysia and others. In Ukraine, which is in the top 5 in terms of the number of created bitcoin wallets, where the largest agency in the CIS operates Kuna and a very developed community for digital currencies, the legal level is not defined at the legislative level. Although there is an explanation of the NBU on the legality of the use of virtual currency (cryptocurrency), where it is defined as a monetary surrogate, which is not a normative explanation and in principle is subject to criticism. In addition, there is a decision of the Court of Appeal of Kyiv from 12.10.2016 in case № 753/599/16, in which the plaintiff justifies his position that bitcoin is a property right to records in an open blockchain database, its material value is confirmed by their value on the world's online trading platforms, and is subject to legal protection. The court, referring to the above-mentioned

explanation of the NBU, considers that bitcoin is not a thing within the meaning of Art. 179 of the Civil code of Ukraine because has no signs of material world and are not products. In addition, cryptocurrency has no signs of property rights. Thus, some countries use and take certain actions against cryptocurrency, but there are obstacles. It is worth noting that Ukraine and many other countries are in a legal vacuum. In my opinion, it is necessary that every consumer and legislator has open information about the issuer. procedure for issuing and transactions regarding cryptocurrency. Information – any information and / or data that can be stored on physical media or displayed electronically is open to all. rights. First of all, these regulations should be not borrowed from other states, but created individually at present. That the legal regime of cryptocurrency was adjusted to current world events and the real situation in the country.

Горлинський В.В.

кандидат філософських наук, доцент,
доцент КПП ім. Ігоря Сікорського

Горлинський Б.В.

кандидат технічних наук, начальник
управління Адміністрації
Держспецзв'язку

ЦИФРОВА ТРАНСФОРМАЦІЯ УКРАЇНСЬКОГО СУСПІЛЬСТВА: ІНСТИТУЦІЙНО-ПРАВОВІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Однією з важливих особливостей глобальних трансформацій є розгортання цифрової трансформації та створення відкритого інформаційного суспільства. Проте світової і національний досвід свідчить, що реалізація ідей інформаційного суспільства можлива лише за умов функціонування надійної системи кібербезпеки. Ефективність, сталість і захищеність національного кіберпростору являє собою передумову переходу українського суспільства на більш високу ступінь сталого розвитку, важливий чинник на-

ціональної безпеки. Поряд з якісними позитивними зрушеннями, розвиток цифрового світу зумовив виникнення нових небезпек, а глобалізація стала чинником інтернаціоналізації кіберзлочинності. Глобальний кіберпростір, порушуючи національні кордони, стає головною ареною боротьби за владу, ресурси, сфери впливу на суспільство і масову свідомість. На погляд експертів, національний кіберпростір, як складова національної безпеки і досить зберігає певний ступінь уразливості перед реальними і потенційними кіберзагрозами. Перед державою постають питання контролюваності інформаційних потоків, захисту національного кіберпростору від інформаційно-технологічної експансії з боку інших суб'єктів впливу, захисту національних інформаційних ресурсів в інформаційно-технологічних системах від кіберзлочинів. Об'єктами кібератак і кіберзлочинів стають інформаційні ресурси державних і фінансових установ, об'єкти критичної інфраструктури, що мають гарантувати безпеку і захист громадян від надзвичайних ситуацій. Джерелом загроз стають не тільки іноземні спеціальні структури, але і злочинні хакерські групи, терористичні та екстремістські організації.

Отже, розв'язання теоретичних і правових проблем надійного захисту національного кіберпростору, вдосконалення національної системи кібербезпеки, постає одним з актуальних завдань теорії і практики українського державотворення.

Проблеми формування системи захисту інформаційного простору в умовах глобалізації та вільного обігу інформації, були відображені в працях О. Баранова, М. Гуцалюка, Р. Калюжного, Б. Кормича, А. Кузьменка, О. Литвиненка, М. Мазура, В. Остроухова, Г. Почепцова, О. Сосніна, А. Старіша, В. Толубки, М. Швеця, та ін. Безпосередньо, питання забезпечення кібербезпеки, розглядались у статтях Є. Бабича, В. Богуша, В. Бурячка, Д. Дубова, С. Морозюк, І. Діордіци, О. Климчука, О. Корнейки, А. Марущака, М. Ожевана, С. Толюпи, В. Фурашева, В. Шеломенцева. Але, поряд з теоретичними добутками, залишаються питання, що потребують поглиблення і конкретизації, розкриття яких, дозволить покращити рівень захисту національного кіберпростору. Одним з

таких актуальних питань, постає розробка принципових теоретико-правових положень побудови системи кібербезпеки.

Утвердження поняття “кіберпростору” переважно пов’язується з Окінаваською хартією глобального інформаційного суспільства (2000), якої приписується статус “конституції інформаційного суспільства”. У хартії зазначено, що зусилля міжнародного співтовариства, спрямовані на розвиток глобального інформаційного суспільства, мають бути скоординованими, щоб забезпечити безпечний та вільний від злочинності *кіберпростір*. Пізніше, на першому Всесвітньому саміті з питань інформаційного суспільства (Женева 2003, Туніс 2005) вперше на світовому рівні було поставлено питання про запровадження глобальної культури *кібербезпеки*. Забезпечення інформаційної безпеки і безпеки мереж було відзначено як принцип інформаційного суспільства. Відображенням стурбованості світової спільноти ризиками використання комп’ютерних мереж з метою здійснення кримінальних правопорушень, стало прийняття Конвенції про кіберзлочинність (Будапешт, 23 листопада 2001 року), яку було ратифіковано Україною у 2005 році. Конвенція визначила види правопорушень у сфері використання комп’ютерної інформації, повноваження, достатні для ефективної боротьби з кримінальними правопорушеннями, як на внутрішньодержавному, так і на міжнародному рівнях, порядок укладення домовленостей щодо швидкого і надійного міжнародного співробітництва.

Суттєвим кроком, на шляху створення умов для безпечного функціонування національного кіберпростору, стало прийняття Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року, у якій було вперше наведено розуміння кібербезпеки, окреслено основи Національної системи кібербезпеки, визначені принципи, пріоритети та напрями її забезпечення в Україні. Прийняття в 2017 році Закону “Про основні засади забезпечення кібербезпеки України”, дозволило не тільки відокремити у інформаційному просторі – правовий інститут кібербезпеки, але і визначити правове поле розгортання відносин, що функціонують у кіберпросторі, відзначити принципові поло-

ження, поняття і норми, що регулюють правові відносини у цій сфері [1].

У Законі наведено 21 нове або уточнене поняття, що мають важливе значення для побудови системи кібербезпеки, серед яких, такі як кібербезпека, кіберзагроза, кіберзахист, кібероборона, кіберзлочин, кіберпростір, що утворюються на підставі поєднання з прикметником –“кібер”, похідним від дав.-грець. “кібернетика”, за якої розуміється мистецтво управління, керування складними системами різної природи походження. Але відсутність єдиного тлумачення понять, що утворюються прикметником “кібер”, на думку дослідників, здатне породжувати протиріччя, стосовно їх використання. Наукове визначення кібернетики, що сформульовано одним з її засновників академіком В. Глушковим – як науки про загальні закони одержання, зберігання, передавання й перетворення інформації у *складних системах управління*, також не відокремлює технічні та електронні системи управління від соціальних і природних систем. Це один з термінологічних чинників, що зумовлює різні підходи до розуміння всіх понять, що походять від слова кібернетика. Тому, пропонується відрізнати розуміння кібернетики в широкому сенсі слова, що охоплює собою всі можливі інформаційні системи управління та в узькому сенсі, що традиційно застосовується для розуміння тільки електронних систем управління – кіберсистем. В розумінні поняття “кіберсистема” також зберігається двозначність, що потребує розведення смислів за сферами, чи простором функціонування. На цієї підставі, дослідниками пропонується підхід, згідно з яким, поняття інформаційного простору розуміється як сфера функціонування будь яких інформаційних систем, зокрема і кібернетичних, а кіберпростір, є більш вузьким поняттям, що є сферою функціонування власно кіберсистем [2]. Однак, визначення “кіберпростору”, наведене у Законі, за своїм змістом, є більш широким і містить низку конкретних ознак, що розширюють значення похідного поняття – кібербезпека.

Однак і цей підхід не визначає однозначно межі розведення інформаційного і кібернетичного простору у розумінні поняття

“кібербезпека”. Прикладами можуть бути публікації матеріалів з кібербезпеки, що містять ознаки порушення прав на інтелектуальну власність, приниження честі й гідності людини або інші ознаки порушення вимог національної безпеки і норм права. На нашу думку, розведення питань з інформаційної і кібербезпеки має базуватись, не лише на просторової, але і на підставі предметної ознаки правопорушення – стосовно чого скоєно правопорушення. Як що немає протиправного втручання в телекомунікаційну систему, то порушення, скоєне з допомогою електронних засобів, відносити до загроз кібербезпеці не варто. Але визначення кібербезпеки, що сформульовано в Законі, не дає підстав для чіткого розмежування питань, що стосуються власно проблеми несанкціонованого втручання у телекомунікаційну систему, що створює загрозу кібербезпеки, з такими – як порушення закону, скоєному в кібернетичному просторі, але без несанкціонованого втручання в систему. Дану проблему, стосовно розведення питань інформаційної і кібербезпеки, можна було б розв’язати за рахунок застосування поняття “кіберзагроза”, але визначення, наведене в Законі, є настільки широким, що також не дає такої можливості. Отже, доцільно розрізняти поняття “загрози кібербезпеці”, тобто самої системі, з одного боку, та інформаційні безпекові загрози, що виникають у кіберпросторі, або “кіберзагрози” у широкому сенсі поняття, з іншого боку. Поставлене питання є важливим в контексті розподілу функціональної відповідальності між державними структурами підтримання кібербезпеки, що перелічені в Законі, зокрема власниками телекомунікаційних мереж, провайдерами.

З огляду на наведені аргументи, важливим, для розв’язання поставленого питання, є чітко визначене Законом, поняття “кіберзахисту” як сукупності організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем [2]. Це визначення дозволяє розмежувати, не тільки технічні і гуманітарні аспекти у

понятті кібербезпеки, розподілити відповідальність, але і відокремити власно “кіберзагрози” від порушень, скоєних у кіберпросторі. Теоретичною підставою для розмежування поля відповідальності у кіберпросторі є розрізнення об’єкта захисту, що наведений у визначенні інформаційної безпеки – *“життєво важливі інтереси людини, суспільства і держави”* в інформаційному просторі, з одного боку, і об’єкта захисту, згідно з визначенням “кіберзахисту” як *“криптографічного та технічного захисту інформації”*, з іншого. Тобто, в другому випадку захист інформації в кіберпросторі слугує умовою захисту інтересів в інформаційному просторі.

Висновки. Комплексна захищеність інформаційного простору українського суспільства потребує удосконалення теоретичних, правових і організаційних основ забезпечення кібербезпеки та захисту національного кіберпростору. Подальша розробка науково-теоретичних, правових і організаційних питань забезпечення кібербезпеки, є одним з важливих завдань нашої держави на шляху до євроатлантичної інтеграції України.

Література

1. Про основні засади кібербезпеки України. Закон від 05.10.2017. №2163-VIII-ВР. База даних «Законодавство України» /ВР України. URL: <http://zakon.rada.gov.ua/laws/show/2163-19> (дата оновлення: 17.09.2020).
2. Архипов О., Бровко В. Кібербезпека – виникнення, формування, розуміння URL: <https://studfile.net/preview/8127803/> (дата звернення: 24.09.2020).

Пономаренко І.С.

аспірант Національної академії

Служби Безпеки України

АКТУАЛЬНІ ПИТАННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я

Медична сфера досить тісно пов'язана з накопиченням і обробленням значних обсягів інформації. Зважаючи на суттєві зміни, які відбуваються у ході проведення медичної реформи, виникає нагальна необхідність суттєвих змін у чинному законодавстві у частині, що стосується подальшого впровадження електронної системи охорони здоров'я. Адже саме від якості методів роботи з інформацією залежить ефективність надання першої допомоги та подальше лікування пацієнта.

Аналізуючи чинне вітчизняне законодавство зазначимо, що відповідно до ст. 32 Конституції України «Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини» [1]. Права людини щодо захисту її персональних даних передбачено Законом України «Про захист персональних даних» (ст. 1,2) [2]. Статтею 39-1 Основ законодавства України про охорону здоров'я також закріплено право пацієнта «на таємницю про стан свого здоров'я, факт звернення за медичною допомогою, діагноз, а також про відомості, одержані при його медичному обстеженні» [3].

Варто зазначити, що право на здоров'я має комплексний характер і включає: право на інформацію та конфіденційність інформації про стан здоров'я; право на медико-соціальну допомогу; право на згоду на лікування та медичне втручання; право на сприятливе екологічне середовище, яке впливає на стан здоров'я та інше. Наголосимо, що реалізація права на життя неможлива без реалізації права на здоров'я. Захист права на життя гарантовано ст. 2 Конвенції про захист прав і основоположних свобод (далі – Конвенція) [4]. При цьому, згідно зі сталою практикою Європейського суду

з прав людини (далі – ЄСПЛ), це право вважається порушеним не тільки у разі позбавлення життя, але і при серйозних пошкодженнях організму людини, які не спричинили його смерть, але представляли серйозну загрозу його життю [5]. Право на здоров'я – це і право на інформацію та конфіденційність інформації, які передбачені ст. 8 Конвенції. Так, у рішенні ЄСПЛ у справі «М.С. проти Швеції» (від 27.08.1997) вказано, що конфіденційність відомостей про здоров'я є основним принципом правової системи держав-учасниць. Національне законодавство повинно забезпечувати нерозголошення відомостей про стан здоров'я, якщо це не відповідає ст. 8 Конвенції [5].

Відповідно до Директиви про захист персональних даних (ст. 8(1)) та Конвенції № 108 (ст. 6), персональні дані, що стосуються стану здоров'я суб'єкта персональних даних, кваліфікуються як чутливі дані, таким чином вони підлягають суворішому режиму обробки даних. Як бачимо, положення про захист персональних даних пацієнтів досить важливі для забезпечення особі її права, проте, на жаль, на практиці воно не завжди належним чином реалізується працівниками медичних установ. Так, наприклад, у справі «Z проти Фінляндії» (рішення ЄСПЛ від 25.01.1997 «22009/93») за фактом розголошення інформації про те, що особа є ВІЛ-інфікованою, ЄСПЛ постановив, що втручання не вважалось необхідним у демократичному суспільстві, оскільки захист медичних даних має фундаментальне значення для здійснення права на повагу до приватного і сімейного життя, особливо коли йдеться про інформацію щодо ВІЛ-інфекції, враховуючи стигматизацію, яка викликана цією хворобою у багатьох спільнотах. Суд дійшов висновку, що надання доступу до інформації про особу заявника і стан його здоров'я, як це мало місце у рішенні апеляційного суду після завершення 10-річного періоду з часу прийняття рішення, порушувало ст. 8 Європейської конвенції про права людини [6]. Таким чином обґрунтовано необхідність існування гарантій захисту персональних даних в сфері охорони здоров'я, закріплення яких в національному законодавстві є першочерговим для реалізації права людини на недоторканність приватного життя.

Персональними даними у сфері охорони здоров'я, на думку Т.М. Ямненко та І.Ф. Літвінової, слід вважати сукупність відомостей про особу (пацієнта), які дозволяють її ідентифікувати та інформацію про її стан здоров'я, медичні обстеження, лікувальні заходи, прогноз розвитку захворювання, а також відомості, які пов'язані з генетичними даними [7].

Електронна система охорони здоров'я спроектована для роботи з персональними даними з дотриманням кращих світових практик у сфері захисту даних. Система знаходиться на серверах дата-центру в Україні, який має комплексну систему захисту інформації та пройшов атестацію у Державній службі спеціального зв'язку та захисту інформації.

Порядок функціонування електронної системи охорони здоров'я та опублікування відомостей з електронної системи охорони здоров'я передбачено постановою Кабінету Міністрів України «Деякі питання електронної системи охорони здоров'я» [8]. Пацієнт, відповідно до Закону України «Про захист персональних даних» [2], в обов'язковому порядку особисто письмово надає згоду на обробку персональних даних. Таким чином, на законодавчому рівні закріплено, що «доступ до даних про пацієнта, що містяться в електронній системі охорони здоров'я, можливий лише у разі отримання згоди такого пацієнта (його законного представника) у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди». Проте, варто акцентувати увагу на тому, що ч. 2 ст. 11 Закону України «Про державні фінансові гарантії медичного обслуговування населення» передбачено випадки можливо-го отримання доступу до персональних даних без надання згоди пацієнта: наявні ознаки безпосередньої загрози життю пацієнта; неможливо отримати згоду пацієнта чи його законних представників (до моменту можливості отримати згоду); за рішенням суду [9]. Отже, обробка персональних даних у сфері охорони здоров'я без згоди суб'єкта даних буде визнаватись законною лише якщо проводиться в цілях охорони здоров'я встановленим колом осіб.

Однією з реформ у системі охорони здоров'я є введення декларації про вибір лікаря, який надає первинну медичну допомогу

(затверджена наказом Міністерства охорони здоров'я України від 19.03.2018 № 503).Пацієнт (чи його законний представник), шляхом підписання декларації про вибір лікаря, який надає первинну медичну допомогу, підтверджує, що усвідомлює мету збирання і обробки своїх персональних даних [10]. Тобто, підписуючи декларацію з терапевтом, педіатром чи сімейним лікарем, людина погоджується, що її персональні дані (чи дані її дитини/підопічного (недієздатної особи) в електронній системі будуть доступні для обробки лікарем, з яким укладено декларацію, та лікарями, до яких вона буде звертатися за медичною допомогою за направленням свого лікаря.

Персональні дані пацієнтів у електронну систему охорони здоров'я можуть вводити визначені медичним закладом уповноважені особи. Це може бути медичний працівник або інша уповноважена особа закладу охорони здоров'я, лікар-ФОП, який має ліцензію на провадження господарської діяльності з медичної практики та його працівники. На них має поширюватись дія законодавства про лікарську таємницю і вони повинні забезпечувати захист таких персональних даних. Ці працівники зобов'язані не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, крім випадків, передбачених законом [10]. Таким чином, персоналізовані дані (усі дані про пацієнта, які містяться у декларації, а із запровадженням електронного рецепта і електронної медичної картки – медична інформація і призначення) доступні тільки лікарю, з яким підписана декларація та лікарю, до якого пацієнт приходить по направленню.

За заподіяння суб'єкту даних моральної шкоди внаслідок порушення правил обробки персональних даних медичну установу можуть притягнути до цивільно-правової відповідальності. Так, статтею 286 Цивільного кодексу України гарантовано право на таємницю про стан здоров'я, а ч. 3 цієї статті передбачає, що фізична особа, якій стала відома інформація про стан здоров'я, факт звернення за медичною допомогою, діагноз, а також про відомості, одержані при медичному обстеженні іншої особи у зв'язку з

виконанням службових обов'язків або з інших джерел, зобов'язана утримуватися від її поширення [11].

Підсумовуючи, зазначимо, що незважаючи на певні позитивні зрушення, які відбуваються у сфері охорони здоров'я, мають місце проблемні питання у напрямі захисту персональних даних, зокрема: інформаційні ресурси та технології оброблення інформації розробляються без забезпечення необхідного рівня централізації та координації робіт, що свідчить про необхідність удосконалення вітчизняного законодавства у даному напрямі; програмно-технічні комплекси розробляються без належного системного опрацювання питань (позитивного зарубіжного досвіду), із низьким рівнем використання сучасних досягнень в галузі технології створення та супроводу єдиних інформаційних систем; відсутня взаємодія цих інформаційних систем з системами інших регіонів; інформаційні системи охорони здоров'я проєктуються та розробляються як системи з «коротким життєвим циклом», а тому не дозволяють розглядати й аналізувати діяльність системи охорони здоров'я на великих часових інтервалах; заклади системи охорони здоров'я акумулюють значні обсяги інформації, що є конфіденційною, у той же час питання інформаційної безпеки при проєктуванні й експлуатації інформаційних систем охорони здоров'я, як правило, не є пріоритетними. Вищезазначене свідчить про необхідність докорінної зміни підходу до захисту інформації у сфері охорони здоров'я.

Список використаних джерел:

1. Конституція України від 28 червня 1996 року. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
2. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: <http://zakon.rada.gov.ua/laws/show/2297-17>.
3. Основи законодавства про охорону здоров'я: Закон України від 19.11.1992 № 2801-XII. URL: <http://zakon.rada.gov.ua/laws/show/2801-12>.
4. Конвенція про захист прав і основоположних свобод. URL: https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D0%B2%D0%B5%D0%BD%D1%86%D1%96%D1%8F_%D0%BF%D1%80%D0%BE_%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82.

5. Захист права на здоров'я у Європейському суді з прав людини. URL: https://ukrainepravo.com/international_law/european_court_of_human-prava-na-zdorov-ya-u-evropeys%60komu-sudi-z-prav-lyudyny.

6. Рішення Європейського суду з прав людини у справі «Z проти Фінляндії» від 25.01.1997 № 22009/93. URL: http://medicallaw.org.ua/fileadmin/user_upload/pdf/Z_against_Finland.pdf.

7. Ямненко Т.М., Літвінова І.Ф. Кримінально-правові аспекти захисту персональних даних у сфері охорони здоров'я. *Юридичний вісник*. 2019. № 1(50). С. 185–191.

8. Деякі питання електронної системи охорони здоров'я: постанова Кабінету Міністрів України від 25.04.2018 № 411. URL: <https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#n247>.

9. Про державні фінансові гарантії медичного обслуговування населення: Закон України від 19.10.2017 № 2168-VIII. URL: <http://zakon.rada.gov.ua/laws/show/2168-19>.

10. Роз'яснення Міністерства охорони здоров'я щодо заповнення декларації. URL: <https://moz.gov.ua/article/for-medical-staff/jak-medikam-pracjuvati-z-personalnimi-danimi-pacientiv/>

11. Цивільний кодекс України від 16.01.2003 № 435-IV. URL: <http://zakon.rada.gov.ua/laws/show/435-15>.

Ямчук Г.М.

студентка Вінницького державного
педагогічного університету імені
Михайла Коцюбинського
Науковий керівник: **Муханов В. М**
кандидат історичних наук, старший
викладач Вінницького державного
педагогічного університету імені
Михайла Коцюбинського

ПРОБЛЕМИ ПРАВОВОГО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

В період розвитку інформаційних технологій доступ до різноманітних каналів комунікації отримали не тільки організації та корпорації, але й окремі особи. У даний період кожна особа має можливість створювати свої власні повідомлення та поширювати інформацію, яка буде доступна необмеженій кількості користувачів. Як результат масового і неконтрольованого доступу усіх членів суспільства до інформаційно-комунікаційних технологій, приватність, яка ще донедавна дозволяла приховувати значну масу особистої інформації від сторонніх, була втрачена. В результаті чого відбулася низка інформаційних скандалів, які привернули увагу до проблеми правового захисту персональної інформації та спричинила широке обговорювання цієї проблеми. Вільний та широкий доступ до інформації, можливість продукувати нову інформацію сприяє створенню можливостей та розвитку особистості, проте стрімкий розвиток інформаційно-комунікаційних технологій потребує розроблення та впровадження адекватних захисних механізмів, спроможних реально захистити персональні права та свободи власників особистих даних.

Для позначення відомостей про особу, які вже зазнали певної обробки людиною, зафіксовані на певному носії, упорядковані і придатні для автоматизованої обробки, уживається термін «персональні дані». [1, с 97]

Таблиця 1

Нормативне визначення поняття «персональні дані»

Нормативний акт	Зміст поняття
Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року (дата ратифікації Україною: 06.07.2010 року, дата набрання чинності для України: 01.01.2011 року) [2].	Персональні дані – будь-яка інформація, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною.
Закон України «Про інформацію» від 02.10.1992 року № 2657-ХІІІ [3].	Інформація про фізичну особу (персональні дані) – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.
Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року [4].	Персональні дані означають будь-яку інформацію, що стосується встановленої фізичної особи чи фізичної особи, яку можна встановити («суб'єкт даних»). Особою, яку можна встановити, є така, яка може бути встановленою прямо чи непрямо, зокрема, за допомогою ідентифікаційного коду або одного чи більше факторів, притаманних фізичним, фізіологічним, розумовим, економічним, культурним чи соціальним аспектам її особистості.

Закон України «Про захист персональних даних» від 1.06.2010 року № 2297-VI [5].	Персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована
Загальне положення про захист даних / EU General Data Protection Regulation (GDPR) [6] (набуває чинності з 25 травня 2018 року).	Персональні дані – вся інформація, що стосується особи, за якою її прямо чи опосередковано можна ідентифікувати.

Джерело, 2, 3, 4, 5, 6

Європейська Конвенція про захист прав і основних свобод людини від 4 листопада 1950 р. конкретизувала право на захист персональних даних проголосивши, що кожна людина має право на свободу дотримуватися своєї думки, отримувати й поширювати інформацію та ідеї без втручання з боку державних органів незалежно від державних кордонів [7]. Міжнародним пактом про громадянські та політичні права від 16 грудня 1966 р. забороняється не лише свавільне, а й незаконне втручання в особисте та сімейне життя людини [8]. Отже, зазначені міжнародні документи узагальнюють основні принципи захисту приватного життя людини.

Комітетом Ради Європи з питань захисту даних були сформульовані принципи захисту від неправомірного збирання, обробки, зберігання та поширення персональних даних. Ці принципи 28 січня 1981 р. отримали закріплення в першій і єдиній на сьогодні міжнародній угоді – Конвенції Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» (відома як Конвенція № 108 Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 28 січня 1981 р. та Додатковий протокол до Конвенції № 108 від 8 листопада 2001 р. згідно з порядком у серії Європейських договорів [9]. З того часу, захист персональних даних, виокремився в самостійний вид діяльності. Конвенція № 108 Ради Європи передбачає дуже важливий момент, згідно з яким збирання, накопичення, зберіган-

ня і поширення персональних даних може здійснюватися лише з дозволу особи, дані про яку обробляються [9, с 8 та 13]. Цій особі надано право знати місце роботи та проживання розпорядника бази персональних даних (відповідального за обробку даних), а також право отримувати відповідні дані без затримки та в зрозумілій формі. У разі відмови зацікавлена особа може звернутися до суб'єкта нагляду за дотриманням законодавства в державі, який мусить забезпечити припинення порушень положень, що зазначені в національному законодавстві.

Законом України «Про захист персональних даних» встановлено детальний порядок реєстрації баз даних [5]. Нажаль, цим Законом регулюються відносини, пов'язані із захистом персональних даних під час їх обробки, але жодною статтею не визначають переліки персональних даних, які мають бути з обмеженим доступом, а які можуть бути відкритими. Закон України «Про захист персональних даних» має загальний характер і передбачає реалізацію його, як системи взаємопов'язаних та взаємопогоджених норм права та механізмів, що забезпечують загальні умови для законності обробки персональних даних, регулювання діяльності суб'єктів у сфері персональних даних.

Вітчизняним законодавством не повністю визначено режим збирання, зберігання, використання та поширення інформації про особу Закон України «Про інформацію» закріплює лише загальні принципи доступу громадян до інформації, що стосується їх особисто [3]. Механізм реалізації зазначеного права належним чином не визначений. Відсутнє й регулювання використання конфіденційної інформації про особу. Різноманітність персональної інформації зумовлює різну значущість цих відомостей для людини. Цим зумовлюються різні підходи і вимоги правового захисту персональних даних.

Аналізуючи чинне законодавство України в частині врегулювання суспільних відносин щодо захисту персональних даних, можна дійти висновку, що формування законодавчої бази з питань захисту персональних даних, насамперед законів України «Про захист персональних даних» та «Про доступ до публічної інфор-

мації», загалом відбувалось з урахуванням досвіду провідних європейських країн та ЄС. Але на сьогодні правове забезпечення суспільних відносин в Україні щодо персональних даних у частині їх правового захисту є недостатнім. Проблема захисту відомостей про особу має розв'язуватися з точки зору права власності конкретної людини на свої персональні дані. Має бути наявне поєднання принципу недоторканності особи з принципом, який свідчить, що основою свободи є власність і замах на неї рівнозначно обмеженню свободи. Аналіз національної нормативно-правової бази з питань захисту персональних даних свідчить, що на сьогодні правове забезпечення суспільних відносин в Україні щодо персональних даних в частині їх правового захисту є недостатнім; законодавству з питань захисту персональних даних України притаманна низка таких суттєвих недоліків, як: фрагментарність, неузгодженість законодавчих актів між собою, недостатня чіткість, конкретність та відповідність європейському законодавству тощо.

Список використаних джерел

1. База персональних даних, володілець бази, розпорядник бази, треті особи: визначимось з поняттям /Матеріали семінару «Організація роботи з виконання вимог Закону України «Про захист персональних даних».- Міжнародний центр фінансово-економічного розвитку. Київ, 2012. с.97.
2. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року. URL: http://zakon3.rada.gov.ua/laws/show/994_326.
3. Закон України «Про інформацію» від 02.10. 1992 року № 2657-XIII. URL: <http://zakon5.rada.gov.ua/laws/show/2657-12>.
4. Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року URL: http://zakon3.rada.gov.ua/laws/show/994_242.
5. Закон України «Про захист персональних даних» від 1.06.2010 року №2297-VI (зі змінами та доповненнями). URL :<http://zakon3.rada.gov.ua/laws/show/2297-17>.
6. EU General Data Protection Regulation (GDPR). URL: <https://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf>

7. Про захист прав людини і основоположних свобод : Конвенція від 4 листоп. 1950 р. – URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

8. Міжнародний пакт про громадянські і політичні права. Міжнародний пакт від 16 груд. 1966 р. – URL: https://zakon.rada.gov.ua/laws/show/995_043#Text

9. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Конвенція Ради Європи № 108 від 28 січ. 1981 р. – URL: https://zakon.rada.gov.ua/laws/show/994_326#Text

Тарасюк А.В.

кандидат юридичних наук, головний
науковий співробітник НДІ
інформатики і права НАПрН України

ПИТАННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ НА СУЧАСНОМУ ЕТАПІ РОЗВИТКУ ГЛОБАЛЬНИХ ІНФОРМАЦІЙНИХ ПРОЦЕСІВ

Нині ні в кого не викликає заперечень, що нормативно-правова база – *головна передумова забезпечення кібербезпеки держави*. А важливою складовою нормативно-правової бази забезпечення кібербезпеки є також сукупність правових норм, що регламентують відносини у сфері функціонування органів держави, які входять до складу систем забезпечення кібербезпеки України. Варто підкреслити, що останнім часом дедалі вагомішого значення набуває взаємодія державних органів із громадськими організаціями та громадянами. У цьому контексті розвиток державно-приватного партнерства має стати одним із пріоритетних завдань державної політики у забезпеченні кібербезпеки.

Інша проблема, яка потребує теоретичного осмислення та практичного вирішення це рівень інформаційно-просвітницької, ідеологічної й освітньої роботи із протидії радикальній ідеології та екстремізму. Така робота потребує значного посилення. Серед найбільших проблем можемо виокремити, зокрема такі:

- брак фахівців у галузі інформаційної протидії екстремізму і тероризму;

- недостатня кількість інформаційної та довідкової літератури стосовно екстремістських і терористичних організацій;
- спостерігається відсутність пропаганди та наочної агітації;
- слабка роль засобів масової інформації у запобіганні та профілактиці екстремізму, а також у висвітленні антитерористичної й антиекстремістської діяльності державних органів.

У розрізі зазначеного ми підтримуємо думку М. Стрельбицького та А. Благодарного, що запобігти екстремізм можна лише спільними зусиллями державних органів та громадськості, спрямованими на підвищення правової і загальної культури населення, поліпшення соціально-економічних умов життя людей, формування позитивного іміджу держави [1, с. 43].

Зважаючи на це, необхідно вживати дієвих заходів із формування потужного ідеологічного корпусу, зміцнення його потенціалу в запобіганні радикалізації й екстремізму, із підготовки фахівців у напрямі інформаційної протидії тероризму й екстремізму, підвищення профілактичної ролі засобів масової інформації та інституційного забезпечення аналітичної, пропагандистської й інформаційної роботи в цій площині. Отже, питання забезпечення кібербезпеки, проблеми зовнішньої та внутрішньої загрози і протидії інформації, де пропагують релігійно-екстремістські і терористичні ідеї та явища в Україні, є одними з найактуальніших завдань суспільства й уряду на найближчу перспективу. Слід наголосити, що в нинішніх умовах радикальна ідеологія активна, ніж будь-коли, і створює серйозну загрозу конституційному ладу держави. Дотепер в Україні таємно ведуть пропагандистську підривну діяльність рухи й організації релігійно-екстремістського напрямку, що містять основну загрозу миру та стабільності як нашої держави такі і становлять загрозу миру і безпеці в Європі.

До найнебезпечніших загроз безпеці в сучасній Україні в зазначеній сфері також належать:

- наявність зовнішніх і внутрішніх центрів політичної, релігійної, міжнаціональної та іншої напруженості у прикордонних районах суміжних Україні країн;

- збільшення на державному кордоні та прикордонній території масштабів розвідувально-підривної діяльності іноземних спецслужб;
- здійснення бандформуваннями бойових дій і терористичних акцій у прикордонній смузі та прикордонних територіях, зокрема проти військ й органів Державної прикордонної служби України;

Отже, з огляду на зазначене вище варто підкреслити, що державним органам необхідно вдосконалювати нормативно-правові акти, які регулюють питання протидії використанню Інтернету в терористичних й екстремістських цілях, а також забезпечують національні інтереси суверенної України в інформаційній сфері.

Іншим важливим напрямом державної політики у сфері правового забезпечення кібербезпеки України на сучасному етапі включення України у глобальні інформаційні процеси є міжнародний чинник.

Не викликає жодних сумнівів той факт, що виникнення нових засобів інформації і комунікації та їхнє поширення у країнах сучасного світу є одним із найвагоміших чинників процесу глобалізації. Стрімке розширення інформаційної та комп'ютерної павутини зменшило відстань між людьми в різних регіонах нашої планети ще більше, ніж розвиток шляхів наземної, повітряної та водної комунікації. Щоб уявити всю глибину інформаційної трансформації, яка відбувається останнім часом, і зрозуміти динаміку, необхідно усвідомити: в умовах глобальної інформатизації зникає географія, стираються межі між зовнішньою та внутрішньою політикою, що неминуче деформує не лише «національну», але й «соціальну» ідентичності. Глобальна інформатизація розкриває багатопланові можливості для соціального інтегрування та транснаціональної взаємодії людей. Інтернет створює інші реалії для вільних контактів між людьми, які мешкають у різних країнах і є членами недержавних об'єднань. Відповідно на першочерговий план виходять питання цифрової рівності населення.

Подолання цифрової нерівності сьогодні стало пріоритетом у багатьох міжнародних організаціях. Проблема особливо посили-

лась з поширенням на планеті коронавірусної інфекції COVID-19 [2]. У цій ситуації ми спостерігаємо й іншу сторону проблеми: протягом останнього року спостерігалось безпрецедентне впровадження цифрових технологій в усі сфери життя. Працівники почали виконувати свою роботу он-лайн, освітні заклади усіх рівнів перейшли на дистанційну форму навчання, що значно підвищено рівень обізнаності інформаційно-комунікаційним технологіям як учителів, викладачів так і тих, хто отримує знання, лікарі та пацієнти звернулися до телемедицини, політичні лідери почали відвідували віртуальні саміти, та багато інших прикладів.

Весь цифровий світ акумулював свої можливості для пошуку дієвих засобів протидії подальшому поширенню хвороби. Цифрові інструменти, такі як програми та дані смартфонів, також використовуються для перевірки розповсюдження вірусу, тоді як технічні компанії, включаючи Alibaba та Tencent в Китаї та IBM, Google і Microsoft в США, почали застосовувати свої високопродуктивні комп'ютерні можливості, щоб допомогти дослідникам у пошуку ліків від цієї хвороби.

Отже, процес глобальної інформатизації, поряд із розмиванням традиційних основ національно-державної ідентичності, може сприяти актуалізації інших форм об'єднання людей. Наслідком нерівномірної та експансіоністської інформатизації може бути посилення релігійної та етнічної ідентичності людей і їхнє об'єднання за ідеологічними принципами. Це, зі свого боку, може створити передумови для появи так званих конфліктів «нового покоління».

Оскільки останнім часом інформація перетворилася в особливий ресурс будь-якої діяльності, отже вона, як і будь-який інший ресурс, потребує захисту в забезпеченні її безпеки, цілісності та збереження. Проведений аналіз доводить, що членство в регіональних організаціях дозволяє Україні виконувати актуальні завдання у сферах політичної комунікації та кібербезпеки. Україна на цій основі має гостру потребу у спільних із розвиненими державами діях, що можуть гарантувати їй безпеку на регіональному та глобальному рівнях. З огляду на це вона здійснює політику «відкритих дверей» та активно співпрацює з міждержавними

об'єднаннями. Такий вектор у жодному разі не конкурує зі стратегічною метою нашої держави – повноправного члена НАТО та Європейського Союзу.

Література:

1. Стрельбицький М.П., Благодарний А.М. Превентивна протидія екстремістським проявам в Україні: правові та організаційні аспекти. Information Security of the Person, Society and State. 2019. № 1 (25). С. 37-45
2. Coronavirus underscores urgency to bridge digital divide. DW. URL: <https://www.dw.com/en/coronavirus-underscores-urgency-to-bridge-digital-divide/a-53070723>

Ткачук Н.І.

кандидат юридичних наук
викладач Національної академії
Служби безпеки України

ІНСТИТУЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНУВАННЯ НАЦІОНАЛЬНОЇ СИСТЕМИ ОЦІНЮВАННЯ РИЗИКІВ І ЗАГРОЗ В УКРАЇНІ

Запровадження національної системи стійкості для забезпечення високого рівня готовності суспільства і держави до реагування на широкий спектр загроз, визначено одним з основних напрямів політики національної безпеки України. У свою чергу, розбудова національної системи стійкості передбачає створення ефективної системи оцінювання ризиків, своєчасної ідентифікації загроз і визначення вразливостей [1]. За цих умов, розробка і реалізація комплексних стратегічних рішень у цій сфері потребує належного наукового обґрунтування, зокрема, питання інституційного забезпечення функціонування національної системи оцінювання ризиків і загроз.

Аналіз геопросторових даних, як сучасний метод оцінювання безпекової ситуації та виявлення загроз, дає можливість поєднувати існуючі в державі бази даних в єдину географічну інформацій-

ну систему [2, с. 38-39]. Нині уряди багатьох країн широко використовують ситуаційні центри (СЦ), на які покладається функція наповнення таких інформаційних систем. Зокрема, Президента США обслуговують чотири СЦ, у Німеччині функціонує “Загальний інформаційно-ситуаційний центр федерального центру та земель”, а Спільний СЦ ЄС є структурою наднаціонального європейського управління [3, с. 141].

В Україні ключовим елементом мережі СЦ центральних органів виконавчої влади визначено Головний ситуаційний центр України, створений відповідно до Указу Президента України від 28 лютого 2015 р. і введений у дію рішенням Ради національної безпеки і оборони України від 25 січня 2015 р. як програмно-апаратний комплекс зі збору, накопичення і обробки інформації, необхідної для підготовки та прийняття рішень у сфері національної безпеки і оборони [4]. Головний ситуаційний центр збирає всю важливу інформацію в одному місці, що забезпечує підтримку прийняття рішень у разі виникнення надзвичайних і кризових ситуацій. Його загальне призначення полягає у прискоренні прийняття ефективних управлінських рішень завдяки їх інформаційній та візуальній підтримці, а також зручності колективної діяльності. У звичайному режимі він здійснює моніторинг ситуації у всіх сферах національної безпеки.

Попри значні досягнення, наразі Головний ситуаційний центр України, за оцінкою фахівців, не виконує важливі функції аналізу, інформування, прогнозування та моделювання кризових ситуацій, раннього попередження та інші, притаманні відповідним структурам розвинених країн, і потребує комплексного реформування [2, с. 49]. Це підтвердило і виникнення ряду гострих проблем у його функціонуванні наприкінці минулого року. Йшлося, по-перше, про впровадження на рівні державних органів та компаній єдиного підходу до процесу збору, передачі та накопичення даних, по-друге, про необхідність накопичення та узагальнення у Головному ситуаційному центрі виключно достовірних верифікованих даних, на підставі яких ухвалюватимуться стратегічні рішення у сфері національної безпеки [5]. Як вважається, робота органів

державної влади оцінюється на основі формальних показників, структурованих даних. Проте, лише їх аналіз не формує цілісного бачення поточної ситуації у відомстві, області чи населеному пункті. Водночас, інформацію, отриману на основі неструктурованих даних, наприклад, коментарів в соціальних мережах (які набувають актуальності у виникненні надзвичайних ситуацій) також не завжди можна вважати достовірною. Окрім зазначеного, в сучасних умовах значно актуалізувала проблема ефекту “великих даних” (BigData). За статистикою, до 90% даних, які зберігаються в сучасних інформаційних системах, просто не використовуються. Їх обсяг настільки колосальний, що практично не піддається обробці. Як відомо, ухваленню рішення, в більшості випадків, передує перетворення даних, що надходять в інформацію, а потім в знання. Не випадково останнім часом зростає попит на так званих “дослідників даних” (DataScientist), які встановлюють взаємозв’язки і перетворюють дані в корисну інформацію. Важливо, щоб подібна робота виконувалася на постійній основі, а не тільки під час кризової або надзвичайної ситуації. Особа, яка приймає рішення, повинна в будь-який момент мати можливість запросити інформацію про поточний стан справ, – інтерактивно або у вигляді звіту. Вирішення таких завдань потребує забезпечення Головного ситуаційного центру належним аналітичним наповненням стосовно оцінювання загроз і виявлення вразливостей. Тому справедливо, щораніше створені технічні спроможності необхідно доповнити аналітичною складовою, яка визначатиме основні завдання для опрацювання в рамках існуючого програмно-апаратного комплексу, а також напрями його розвитку [2, с. 48-49].

З урахуванням зазначеного, як видається, лише якісна колективна аналітична робота із застосуванням сучасних методів і технологій оцінювання ризиків і загроз, моделювання кризових ситуацій, розроблення сценарних прогнозів тощо на майданчику Головного ситуаційного центру, дасть змогу підвищити достовірність отриманих результатів, сформувати широкую доказову базу для подальшого аналізу та підготовки стратегічних рішень у сфері національної безпеки.

Література

1. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 р. № 392/2020. URL : <https://zakon.rada.gov.ua/laws/show/392/2020#n12>.
2. Резнікова О. О., Войтовський К. Є. Лепіхов А. В. Національні системи оцінювання ризиків і загроз: кращі світові практики, нові можливості для України : аналіт. доп. Київ : НІСД, 2020. 84 с.
3. Пристайко В.В. Ситуаційні центри як ключовий інституційний механізм державного антикризового управління: зарубіжний досвід. Вчені записки ТНУ імені В.І. Вернадського. Серія: Державне управління Том 30 (69) № 3. 2019. С. 138-142.
4. Про рішення Ради національної безпеки і оборони України від 25 січня 2015 р. «Про створення та забезпечення діяльності Головного ситуаційного центру України» : Указ Президента України від 28 лютого 2015 р. № 115/2015. URL: <http://zakon3.rada.gov.ua/laws/show/115/2015/paran2#n2>.
5. Панченко Д. УРНБО взяли за вдосконалення Головного ситуаційного центру. Інформаційне агентство «Українські Національні Новини». URL: <https://www.unn.com.ua/uk/news/1839464-u-rnbo-vzyalis-zavdoskonalennya-golovnoho-situatsiynogo-tsentru>.

Кухрівський Д.В.

студент КПІ ім. Ігоря Сікорського

ПИТАННЯ ВДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА З ПИТАНЬ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ, ІНФРАСТРУКТУРНОЇ БЕЗПЕКИ, КІБЕРБЕЗПЕКИ

Сьогодні Україна в умовах інформатизації суспільства протистоїть найсерйознішому виклику своїй національній безпеці. Загострення економічної кризи, ведення проти України гібридної війни, зростання рівня злочинності – все це впливає на рівень безпеки в Україні. Саме тому важливою складовою є створення ефективної нормативно-правової бази задля забезпечення безпеки країни.

Захист персональних даних в Україні регулюється Законом України “ Про захист персональних даних”. Існувала Державна служба України з питань захисту персональних даних. Потім вона була ліквідована і на сьогоднішній день питанням захисту персональних даних займається Уповноважений Верховної Ради України з прав людини та суду. Були також сформовані Великою Палатою Верховного Суду принципи обробки персональних даних, зокрема це: відкритість і прозорість, відповідальність, адекватність, не надмірність їх складу та змісту стосовно визначеної мети обробки, і підстави для обробки персональних даних (згода суб’єкта персональних даних).

Сьогодні web- сайти дуже часто пропонують зареєструватися на сайті, що передбачає надання згоди на обробку персональних даних. Однак мало хто цікавиться де, як і ким будуть оброблюватися персональні дані. Адже може бути витік персональних даних. І тому в українському законодавстві існує безліч проблем з цього приводу.

Текст згоди персональних даних однотипний. Тобто якщо ти надаєш згоду на обробку персональних даних, ти отримаєш послугу, якщо ні, ти відповідно її не отримаєш. Законодавством не врегульовано питання, щодо альтернативи вибору, чим і порушуються конституційні права такої особи. Адже державні послуги мають здійснюватися без примушування людини до надання згоди на обробку персональних даних. Взагалі обробка персональних даних повинна діяти на підставі законів і нормативно-правових актів України, відповідно до яких виникають правовідносини між громадянином та державою. При цьому, людина, яка відмовилася від обробки персональних даних повинна мати альтернативу. Якщо врахувати всю кількість згод, що надав користувач послуги, то важко відслідкувати куди передаються твої дані. І в цьому питанні наше українське законодавство є неефективним.

Взагалі нещодавно стався витік персональних даних, а саме водійські дані. І підозра впала на додаток «Дія». Хоча влада заперечувала свою причетність, все ж таки були порушені права користувачів. Тому доречним було б питання видалення вже наданих

персональних даних. Законодавством це передбачено, але зробити не просто. Потрібно отримати рішення суду, а така процедура може тривати місяць.[1]

Зважаючи на те що захистити всі об'єкти інфраструктури практично не можливо, багато країн світу концентрують свою увагу саме на об'єктах критичної інфраструктури, тобто на тих об'єктах, знищення яких матиме дуже негативні наслідки. До об'єктів критичної інфраструктури належать транспортні магістральні мережі, нафто – та газопроводи, морські порти, канали швидкісного та урядового зв'язку, системи життєзабезпечення (водо- та теплопостачання) мегаполісів, утилізації відходів, служби екстреної допомоги населенню, підприємства військово-промислового комплексу. В українському законодавстві досі не визначено терміну “критична інфраструктура” і саме це створює перешкоди для посиленої охорони об'єктів енергетики та критичної інфраструктури.[2]

Також маємо і неефективну правову базу, яка регулює кібербезпеку України Адже Закон України» Про захист інформації в інформаційно-телекомунікаційних системах ” та інші документи вже давно застарілі. Вони зобов'язують органи державної влади впроваджувати Комплексну систему захисту інформації, яка є неефективною. Також погано працює система кіберрозвідки.[3]

Отже потрібно вносити зміни до нашого законодавства, вносити поправки та доповнення до законодавства з питань захисту персональних даних, кібербезпеки, захисту об'єктів критичної інфраструктури.

Список використаних джерел

1. Юридична газета online : Проблеми захисту персональних даних: досвід України та інших країн.

URL: <https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/problemi-zahistu-personalnih-danih-dosvid-ukrayini-ta-inshih-krayin.html> (дата звернення : 29.03.2020)

2. Д.С. Бірюков. «Про проблеми вдосконалення системи захисту критичної інфраструктури в Україні». Аналітична записка // Національ-

ний інститут стратегічних досліджень. – 2018. URL : <http://old2.niss.gov.ua/articles/1477/> (дата звернення : 29.03.2020)

3. Олексій Янковський. “Україні потрібна нова кіберстратегія”// Українська правда. – 2019 URL: <https://www.pravda.com.ua/rus/columns/2019/09/14/7226291/> (дата звернення:29.03.2020)

Моргун Г.В.

студентка КПП ім. Ігоря Сікорського
Науковий керівник: **Чепульченко Т.О.**
к.ю.н., доцент КПП ім. Ігоря
Сікорського

СУТНІСТЬ ПАТЕНТНОГО ТРОЛІНГУ ЯК ПРАВОВОГО ЯВИЩА ТА ЙОГО ВПЛИВ НА СФЕРУ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Швидко збільшення кількості патентів і, як слідує з цього, поширення такого явища, як патентний тролінг спричиняє актуальність вивчення даного питання, а також шляхів протидії патентному тролінгу як одному з видів порушення прав на об'єкти інтелектуальної власності. Незважаючи на велику кількість наукових праць у досліджуваній сфері, дане питання не втрачає своєї актуальності, адже не є до кінця вирішеним на теоретичному та практичному рівнях, тому зумовлює подальше дослідження патентного тролінгу та розроблення шляхів його подолання.

Завдання, які ставляться до даного дослідження: визначити поняття патентного тролінгу, розглянути сутність патентного тролінгу, описати особливості патентного тролінгу в Україні, визначити шляхи протидії зазначеному явищу.

Вивчаючи будь-яку проблему, перш за все варто зосередитися на характеристиці понять, що дозволить більш повно усвідомити сутність правового явища, що досліджується. Отже, у чому полягає зміст поняття «патентний тролінг»?

Поняття «патентний тролінг» запровадив Пітер Деткін, який на той час перебував корпоративним юристом компанії Intel. Патентний – це юридична особа або суб'єкт підприємницької діяль-

ності, чий бізнес полягає виключно в отриманні з добросовісного виробника товарів (який їх своєчасно не запатентував), ліцензійних послуг або інших платежів за використання належних тролів патентів. Зазвичай, патентний троль тільки володіє одним ключовим патентом або портфелем з кількох патентів, але не виробляє ніяких товарів, не надає жодних послуг і не веде конкретних досліджень, пов'язаних зі своїми патентами. Але при цьому троль, після проведення відповідних маркетингових досліджень, активно захищає свій патент, судячись з фірмами, які використовують належні йому винаходи чи корисні моделі.

В Україні діяльність патентних тролів має інший зміст. Відомий випадок – реєстрація торговельної марки «Гоу Огле», яка дозволила тролю зареєструвати домен UA (google.ua). Все закінчилося тим, що компанія Google змогла довести, що реєстрація торгової марки не є добросовісною і її скасували в судовому порядку.

За українським законодавством корисним моделям та промисловим зразкам надається правова охорона за результатами формальної експертизи, тобто під відповідальність самого заявника, тобто кваліфікаційна експертиза в ході якої перевіряють об'єкт на відповідність критерію новизни не здійснюється. Згідно із буквою закону, уповноважений орган у сфері інтелектуальної власності в Україні, попри очевидність застосування заявлених на охорону прав інтелектуальної власності та загальну відомість останніх на ринку протягом десятиліть чи століть, не має права відмовити заявникові у наданні правової охорони та видачі охоронного документу, а митні органи – відмовити у внесенні права, на який виданий охоронний документ, до митного реєстру на цій підставі.

Оскільки на законодавчому рівні немає чітко сформованого визначення поняття «патентний тролінг», звернімося за його встановлення до думок науковців та спеціалістів у сфері інтелектуальної власності.

І. Коросташова вважає, патентний тролінг – шкідливе явище, що набуває в Україні все більших масштабів, полягає у зловживанні правами інтелектуальної власності на корисні моделі та промислові зразки, реєстрація яких стає можливою у зв'язку з

певними прогалинами та суперечностями в національному законодавстві. [1, с.27] К. Шуртаков під патентним тролінгом розуміє отримання патенту на винахід не для подальшої комерціалізації і практичного використання нового технічного рішення, а для пред'явлення позовів до суб'єктів господарювання, які нібито незаконно використовують запатентовану розробку [2, с. 293].

В Україні патентний тролінг має деякі особливості й відмінності від патентного тролінгу за кордоном. Ця особливість в Україні полягає в реєстрації в патентному відомстві України патентними троями на своє ім'я прав інтелектуальної власності на неоригінальні або навіть абсурдні (давно та широковідомі) об'єкти (наприклад, вішала, лампи розжарювання, протектори шин, зовнішній вигляд ноутбука із закругленими кутами, кузовів автомобілів, пальчикових батарейок тощо) [1, с. 26]. Ситуація ускладнюється ще й тим, що аналіз практики патентних суперечок показує, що за володіння спеціальною термінологією, знаючи процедуру розгляду патентної заявки і нюанси, пов'язані з експертною оцінкою, можна отримати патент на відоме технічне рішення. Водночас ознака, властива вже відомій продукції або технології, робиться основною відмінною ознакою для якогось нового «винаходу». Ризик таких маніпуляцій мінімальний (патент просто не буде отриманий), покарання за спробу запатентувати вже відомий винахід не передбачено (заявник міг помилитися щодо новизни пропонованого рішення), а потенційний дохід великий [2, с. 294]. Очевидно, що вказані особливості спричинені недосконалістю чинного законодавства України у сфері інтелектуальної власності, тому зумовлюють необхідність удосконалення правової бази, яка б протидіяла появі патентного тролінгу та сприяла притягненню винних у ньому до юридичної відповідальності.

Потреба у протидії патентному тролінгу неодноразово звучала на теоретичному та практичному рівнях. Так, І. Коросташова одним із перших кроків у боротьбі з патентним тролінгом в Україні вважає надання права Апеляційній палаті Міністерства розвитку економіки, торгівлі та сільського господарства України «на скасування за прискороною процедурою патентів на корисні моделі

та промислові зразки, що отримані недобросовісними заявниками під їх відповідальність, і насправді не відповідають критерію новизни» [1, с. 27]. У такому разі винні суб'єкти будуть нести адміністративну відповідальність за порушення ст. 15 Закону України «Про захист від недобросовісної конкуренції».

На думку А. Нікончук, одним із нововведень, яке б ускладнило здійснення патентного тролінгу, є введення обов'язковості використання об'єкта патентування, а також накладання відповідальності за патентний тролінг. В той самий час необхідні ретельно виважені механізми ідентифікації саме патентних тролей, адже за формальними ознаками їхня діяльність, як і зловживання в подачі судових позовів із захистом відповідних прав, багато в чому схожі з абсолютно добросовісною господарською діяльністю. Саме тому доцільним вбачається створення спеціалізованих патентних судів, які б мали можливість використовувати єдині критерії для визначення патентних тролів та недобросовісності їхньої діяльності [3, с. 31].

У зв'язку із наведеним, підтримую пропозиції, які висловлюються в юридичних публікаціях, і приєднуюся до думки, що для України можливі такі шляхи вирішення цієї проблеми:

1. Запровадити відповідальність недобросовісних патентовласників за зловживання правами інтелектуальної власності та відшкодування збитків добросовісного бізнесу від дій тролів, якщо буде доведено безпідставність їх вимог.

2. Встановити відповідальність осіб, які свідомо сприяють недобросовісному отриманні правової охорони на промислові зразки і корисні моделі, починаючи з експертів патентного відомства й закінчуючи патентними повіреними.

3. Після проходження заявкою на патент стадії формальної експертизи передбачити її електронну публікацію, що дасть змогу заінтересованим особам протягом двох місяців надати заперечення проти реєстрації прав на заявлений зразок.

4. Передбачити механізм в адміністративному порядку (без судового розгляду) визнання недійсним виданого патенту, якщо будуть подані достовірні відомості (докази) невідповідності запатентованого об'єкта критеріям патентування.

тентованого об'єкта умові новизні, залишивши можливість оскарження такого рішення в судовому порядку.

Підводячи підсумок, можна сказати, що для патентного тролінгу як одного з видів порушення прав на об'єкти інтелектуальної власності характерне використання прогалин у законодавстві для отримання патенту на певний об'єкт, який не відповідає вимогам патентоздатності. У зв'язку із цим в Україні виникає нагальна потреба в удосконаленні законодавчої бази, пов'язаної із протидією патентному тролінгу, адже чинне законодавство не передбачає дієвих інструментів і механізмів впливу на недобросовісних заявників, що тим самим створює сприятливі умови для поширення патентного тролінгу. Водночас удосконалення законодавства має обов'язково передбачати закріплення посиленої відповідальності за патентний тролінг; проведення комплексної експертизи об'єкта, що патентується; розгляд справи в адміністративному та судовому порядку. Протидія цьому негативному явищу актуалізується потребою покращення інвестиційного клімату та євроінтеграційними процесами, що відбуваються.

Список використаних джерел:

1. Коросташова І. Патентний тролінг як прояв недобросовісної конкуренції: поняття, ознаки, причини. Вісник Академії митної служби України. Серія «Право». 2015. № 1 (14). С. 23–28.
2. Шуртаков К. «Патентные тролли»: анализ зарубежной и российской практики. Экономика науки. 2016. № 4. Т. 2. С. 293–303.
3. Нікончук А. Правові засади протидії патентному тролінгу в Україні. Зовнішня торгівля: економіка, фінанси, право. 2014. № 4 (75). С. 25–33.

Фурашев В.М.

кандидат технічних наук, старший
науковий співробітник

ОСОБЛИВОСТІ ОСВІТНЬОГО ПРОЦЕСУ ПІДГОТОВКИ ПРАВНИКІВ ДЛЯ РОБОТИ В УМОВАХ СОЦІАЛЬНОЇ ТА ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Не буває у природі чогось однобічного. У реальному житті – також такого не буває. У чомусь виграєш, а чому – програєш.

Сучасна соціальна та цифрова трансформація, як наслідок прискореного, у порівнянні з минулими періодами розвитку загальносвітового суспільства, науково-технічного прогресу, також має всі ознаки двобічності – позитивізму та негативізму.

Одним з головних наслідків негативізму сучасного науково-технічного прогресу можна вважати те, що людство вже приречено назавжди «йти по життю як сіамські близнюки» з питаннями забезпечення інформаційної безпеки.

Може виникнути питання – чому саме «інформаційною безпекою», а не «кібербезпекою»?

Відповідь дуже проста – поняття «інформаційна безпека» більш широке поняття ніж «кібербезпека». Кіберпростір – штучне утворення, наслідок діяльності людини у природному інформаційному середовищі. Кіберпростір, є невід'ємною складовою інформаційного простору.

Цілком зрозуміло, що правила поведінки з інформацією на всіх стадіях її життєвого циклу не залежать від виду простору її обороту. Саме інформація зі своїми властивостями, поведінки з нею, здійснюють вирішальний вплив на світогляд людини та суспільства в цілому.

В умовах соціальної та цифрової трансформації все більше зростає роль інформації, інформаційних суспільних відносин, питань забезпечення належного рівня інформаційної безпеки на всіх рівнях – людини, суспільства, держави та світу в цілому. Це – загальносвітова проблема. Самотужки жодна країна світу, в умовах глобалізованого інформаційного простору, не спромож-

на вирішити це питання, навіть шляхом встановлення «залізного завісу».

Неможливо повністю усунути всі проблеми, пов'язані з інформаційною безпекою тому, що «отрута» породжує «протиотруту», а не навпаки. «Отрута» завжди випереджає «протиотруту». Засоби та методи несанкціонованого втручання в процеси здійснення обороту інформації, особливо у кіберпросторі, з урахуванням напрямів розвитку науково-технічного прогресу, людського фактору, цілій та завдань, завжди будуть випереджувати засоби та методи їх протидії. Але можна суттєво зменшити негативні наслідки несанкціонованого втручання у процеси обороту інформації та підвищити рівень інформаційної безпеки. Питання полягає у тому, як швидко спроможне суспільство реагувати на це.

Шляхів скорочення часу реагування на вказані виклики загрози достатньо багато. Один з таких шляхів окреслено у ст. 17 Конституції України: **“Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу”**.

Реальна реалізація цього положення можлива лише в умовах масової обізнаності населення щодо шляхів, методів та цілій інформаційних загроз та шляхів їх запобігання, підготовки кваліфікованих спеціалістів всіх спеціалізацій у сферах інформаційного права, інформаційної безпеки та кібербезпеки.

Процеси обізнаності населення щодо шляхів, методів та цілій інформаційних загроз та шляхів їх запобігання, на наш погляд, треба починати зі школи, шляхом введення відповідних навчальних дисциплін, на кшталт – “Інформація та поведінка з нею”, “Введення до інформаційної безпеки” або “Основи інформаційної безпеки”, “Вступ до кібербезпеки” або “Основи кібербезпеки” та інше.

Дана пропозиція обумовлена тим, що вже зараз процеси соціалізації людини, а відповідно і суспільства, переміщуються у кіберпростір зі всіма наслідками, як позитивними, так і негативними. Причому, яких більше – покаже час та детальні наукові досліджен-

ня. Одне відоме вже зараз – у подальшому цей процес буде лише поширюватися та поглиблюватися. Це не відкидає інших способів та методів масової просвітницької діяльності.

Необхідно також констатувати, що сучасність вимагає докорінного перегляду підготовки професіональних спеціалістів, спроможних аналізувати, класифікувати процеси та дії, які відбуваються в інформаційному просторі та кіберпросторі, знаходити методи та засоби оперативного запобігання або усунення негативних, з точки зору забезпечення інформаційної безпеки та кібербезпеки цих процесів та дій.

На формальному рівні, на даний час, начебто, ця потреба розуміється. У низці вищих навчальних закладів України відкрити та функціонують кафедри з інформаційного права, інформаційної безпеки, але це функціонування наштовхується на майже відсутню спонукальну мотивацію.

На жаль, необхідно констатувати, що досить у багатьох представників, які приймають рішення на державному рівні, у правничому середовищі та у середовищі роботодавців, відсутнє, у силу різних обставин, чітке розуміння спрямованості та вимог соціальної та цифрової трансформації, яка вже спостерігається та надалі буде лише поширюватися, та поглиблюватися, охоплюючи всі сфери життєдіяльності окремої людини, суспільства, держави та світу. Саме тому, майже відсутнє державне замовлення та запит роботодавців на підготовку правників, які відповідали б вимогам сучасності, зокрема, у сферах поведінки з інформацією (інформаційне право), інформаційної безпеки та кібербезпеки. Саме тому, навчальні дисципліни з даних напрямів, під час підготовки правників відносять до “вибіркових”, а не “обов’язкових” з мінімізацією часу їх викладання та доручення цих дисциплін викладачам, які не мають реального наукового та практичного досвіду у цих напрямках. Саме тому, у студентів-правників відсутня спонукальна мотивація опанування даними напрямками правничої діяльності.

На нашу думку, вищевикладене є однією з головних причин незадовільного стану правового забезпечення інформаційної без-

пеки країни у частині правозастосовної та правоохоронної діяльності. Це є недалекоглядною позицією з досить загрозливими наслідками.

Клименко К.О.

аспірант НДІ інформатики і права
НАПрН України

ПРАВОВІ АСПЕКТИ ЗАСТОСУВАННЯ АДВОКАТСЬКОЇ ТАЄМНИЦІ ЯК СКЛАДОВОЇ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ АДВОКАТА

Один із ключових правових інститутів, що забезпечує діяльність адвокатів, в тому числі і інформаційну діяльність адвокатів, є адвокатська таємниця. Законодавством надано визначення адвокатської таємниці, яке повинно забезпечити можливість адвокатам здійснювати свою професійну діяльність та захист прав і законних інтересів фізичних та юридичних осіб. Фактично Законом України «Про адвокатуру та адвокатську діяльність» встановлюється спеціальний правовий режим заборони доступу до інформації, яка використовується адвокатом під час надання юридичної допомоги. У загальному розумінні адвокатська таємниця – це масив інформації, який містить дані у цифровому виді (е-документи, медіа матеріали (фото, аудіо, відео), програмні продукти тощо) та друкарському виді (офіційні та приватні документи, учбова, художня, нормативна спеціалізована література та документація тощо), а також весь цикл роботи адвоката із клієнтом від факту звернення особи за правовою допомогою і навіть після припинення договору про надання професійної правничої (правової) допомоги.

Саме види відкритої інформації визначені в статті 18 Закону України «Про інформацію», а статтею 30 цього ж закону встановлено особливості регулювання відносин пов'язаних із державною таємницею. Інформацію, що складає адвокатську таємницю і визначена частиною 1 статті 22 Закону України «Про адвокатуру та адвокатську діяльність», в свою чергу можливо поділити за ре-

жимом доступу, а саме: на відкриту інформацію і інформацію з обмеженим доступом. Інформація із обмеженим доступом може містити державну таємницю, банківську таємницю, комерційну таємницю, персональні дані та інше [1].

Статтею 2 Закону України «Про захист персональних даних» визначено, що персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [2].

На сьогодні предметом активних юридичних дискусій є проблеми забезпечення адвокатської таємниці та персональних даних, отриманих під час здійснення професійної діяльності адвокатів, які остаточно не врегульовані у правозахисній діяльності через тлумачення сутності адвокатської таємниці та персональних даних. Закони України «Про адвокатуру та адвокатську діяльність» та «Про захист персональних даних» дають можливість розширено трактувати і відносити інформацію до адвокатської таємниці, а значить і до персональної інформації. Водночас, як показала практика, таке трактування зовсім не означає можливості розширеного розповсюдження системи захисту адвокатської таємниці [3].

На нашу думку персональні дані, як невід’ємна складова предмету адвокатської таємниці, можливо розділити на: персональні дані клієнта та персональні дані інших осіб, які отримує адвокат під час надання професійної правничої (правової) допомоги клієнту. В свою чергу персональні дані доцільно поділити на ідентифікаційні дані (конкретна інформація за якою можливо точно встановити особу) та персональні дані загального характеру (інформація, яка потребує додаткових даних для точного встановлення особи).

До ідентифікаційних даних особи доцільно віднести сталі дані закріплені в документах, перелік яких встановлено частинами 1 та 3 статті 13 Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» Також до ідентифікаційних даних особи можливо віднести дані визначені в п.п.4, 6-14 статті 1 цього ж закону [4].

Законодавство України в питаннях адвокатської таємниці та персональних даних нині не досягло максимальної точності у текстах законів, а застосовується більш або менш неконкретизовані формулювання і тлумачення, застосування яких залежить від практики та правових позицій Верховного Суду України та Конституційного Суду України.

Вважаємо за доцільне на законодавчому рівні здійснити модернізацію законодавства та запровадити перелік персональних даних, які є обов'язковими ідентифікаційними даними особи і потребують додаткового правового режиму захисту. Це дозволить конкретизувати роботу багатьох державних інституцій із персональними даними, застосувати дієві правові та технічні механізми їх захисту, суттєво поліпшити якість захисту адвокатської таємниці.

Література

1. Баранов О. А. Основи класифікації інформаційного законодавства. / О. А. Баранов // Правова інформатика. – 2006. – С. 25–32. <http://ippi.org.ua/sites/default/files/06bokiz.pdf> С-25-32 (дата звернення 01.12.2020)
2. Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI/ Законотворчість: база даних / Верховна Рада України URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення 02.12.2020).
3. Ілля Костін. Адвокатська таємниця. Трагедія у 4 частинах /І.Костін// URL:<https://radako.com.ua/news/advokatska-taiemnicya-tragediya-u-4-chastinah> (дата звернення 01.12.2020).
4. Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI/ Законотворчість: база даних / Верховна Рада України URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення 02.12.2020).

Сай В.І.

аспірант КПП імені Ігоря Сікорського

РЕГУЛЮВАННЯ ОНЛАЙН-МЕДІА В КОНТЕКСТІ ЗАКОНОПРОЕКТУ ПРО МЕДІА

02 липня 2020 року у Верховній Раді зареєстрували доопрацьований законопроект «Про медіа» №2693-д.

Одна з головних змін, яку може принести в український медійний простір закон «Про медіа» в разі його ухвалення – регулювання онлайн-медіа та платформ спільного доступу до інформації (соціальних мереж).

Законопроект дає визначення онлайн-медіа. Базовий критерій для визначення – це редакційний контроль. Детальніші критерії, кого відносити до онлайн-медіа, вироблятиме Національна рада з питань телебачення і радіомовлення разом із органом співрегулювання галузі (який має бути створено). Для онлайн-медіа передбачена добровільна реєстрація. Однак як зареєстровані, так і незареєстровані онлайн-медіа мають виконувати вимоги закону й нести відповідальність за їх порушення. А це вимоги щодо прозорості власності, захисту неповнолітніх, спростування та права на відповідь, щодо заборони поширення незаконного контенту, обмеження російського та проросійського контенту.

Платформи спільного доступу до інформації (тобто соцмережі) та їхній різновид – платформи спільного доступу до відео (YouTube та інші) – не є онлайн-медіа. Тут ключовим критерієм є відсутність редакційного контролю з боку власника платформи. Але для них теж передбачене окреме регулювання. Їхня реєстрація є добровільною. Відповідальність за порушення нестимуть лише платформи спільного доступу до відео – як зареєстровані, так і незареєстровані, але якщо вони підлягають українській юрисдикції (законопроект вказує кілька ознак для її визначення).

Провайдери платформ спільного доступу до відео мають низку обов'язків: розміщувати умови користування сервісом, передбачити в них заборону поширення користувачами незаконного й піратського контенту, а також порядок реалізації права на відповідь

або спростування недостовірної інформації, забезпечити перевірку віку користувача й можливість встановлення системи батьківського контролю, створити дієвий механізм отримання й розгляду звернень і скарг користувачів, не обробляти персональні дані дітей із комерційною метою.

Експерт Ради Європи з Бельгії Жан-Франсуа Фурнемон радить не включати регулювання онлайн-медіа до регулювання аудіовізуальних медіа.

Схожу думку висловлює й консультантка Ради Європи з Угорщини Крістіна Розгоній. Вона нагадала, що Європейська Комісія тільки почала роботу на Актом про цифрові сервіси (Digital Services Act), тобто Європа тільки приступає до регулювання онлайн-сфери. У Німеччині нині серйозно придивляються до свого закону, який регулює онлайн-платформи, а у Франції нещодавно визнали неконституційним [1] новий закон щодо мови ворожнечі на інтернет-платформах.

Позиція розробників законопроекту «Про медіа» поки що однозначна: онлайн-сферу потрібно регулювати.

Розробники законопроекту запевняють, що з регулювання виключено приватні сторінки людей у соціальних мережах – регулюванню підлягають тільки сторінки медіа. Якщо буквально читати запропоноване визначення онлайн-медіа та винятки, на кого не поширюється закон, то виходить, що під його дію потраплять і приватні користувачі соціальних мереж.

Частково таке тлумачення норм закону підтвердила Віта Володовська [2]: закон може поширюватися на блогерів, але лише на тих, які самостійно зареєструються як онлайн-медіа або відповідатимуть ознакам «медіа», визначеним у законі та в акті спільного регулювання.

Стаття про право на відповідь і спростування є занадто деталізованою, вважає Жан-Франсуа Фурнемон. У ній дуже розширюється право на відповідь і фактично переходить у сферу захисту від дифамації (приниження честі, гідності та ділової репутації), яка регулюється в судовому порядку. Експерт рекомендує переписати цю статтю у відповідності до Резолюції ПАРЕ щодо медіа відповідальності [3].

У статті 117 законопроекту є положення, що суб'єкти у сфері онлайн-медіа не несуть відповідальності за інформацію, яка є дослівним відтворенням матеріалів, опублікованих іншим зареєстрованим медіа або іноземним медіа – із посиланням на них.

Ще одне застереження до законопроекту стосується незареєстрованих онлайн-медіа.

Логіка творців законопроекту – створити мотивацію для реєстрації (тому законопроект передбачає певні преференції для зареєстрованих онлайн-медіа). Не хочеш реєструватися – працюй собі далі, веди господарську діяльність відповідно до Господарського й Податкового кодексів, отримуй статус журналіста через вступ у професійні та творчі спілки. Але тоді постає питання: тобто права в зареєстрованих та незареєстрованих онлайн-медіа будуть різні, а обов'язки – однакові? При цьому багато хто з користувачів соціальних мереж навіть не здогадуватиметься, що його занесли до онлайн-медіа.

Пропозиція регулювання незареєстрованих онлайн-медіа є однією з розбіжностей між розробниками й тими, хто в цілому підтримує законопроект, але з правками. Наприклад, фахівці Інституту масової інформації вважають, що регулювання для онлайн-медіа на даному етапі треба поширити лише на тих, хто добровільно зареєструється, тобто свідомо візьме на себе певні зобов'язання. Щодо інших пропонується застосовувати загальні норми законів «Про інформацію», «Про доступ до публічної інформації» тощо.

Список використаних джерел

1. <https://www.nytimes.com/2020/06/18/world/europe/france-internet-hate-speech-regulation>
2. <https://detector.media/rinok/article/178630/2020-07-09-regulyuvannya-onlain-media-rozysnennya-klyuchovikh-polozhen-doopratsovanogo-zakonoproektu-pro-media>
3. <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21960 &lang=en&fbclid=IwAR2kAnOUYLYUIDsn0kq5CwZhUfl-27rDzT8-xSOAqqipqII aujqJFp8RSYA>

Баранов О.А.

доктор юридичних наук, старший науковий співробітник., професор КПП імені Ігоря Сікорського»

Головко О.М.

кандидат юридичних наук, старший викладач КПП імені Ігоря Сікорського

Дубняк М.В.

кандидат юридичних наук, старший викладач КПП імені Ігоря Сікорського

ЦІЛІ, ЗАВДАННЯ ТА ПЕРСПЕКТИВИ ПРОЕКТУ «ЄВРОІНТЕГРАЦІЯ: ЗАКОНОДАВСТВО ТА ІНТЕРНЕТ РЕЧЕЙ» (EULIOT)¹

На конкурс проєктів Європейської комісії по програмі Еразмус+ було подано 1447 конкурсних пропозицій, серед 38 переможців з України секції модуль Жан Моне є і наш. Проект – це курс з навчальної дисципліни «Євроінтеграція: законодавство та ІоТ» (скорочена назва проєкту – EULIoT).

Політика Європейського Союзу щодо поширення цінностей цифрової трансформації суспільства, зокрема, у частині впровадження технологій Інтернету речей (Internet of Things, далі – ІоТ), як надважливого важеля розвитку економіки, є довготерміновою, системною та багатоаспектною, про що свідчить сталість та значущість досягнень в багатьох сегментах суспільства, таких як економіка, промисловість, сільське господарство, публічний сектор, медицина, освіта тощо.

¹ Дослідження проведено в межах виконання міжнародного проєкту в сфері освіти «European Integration: legislation and the IoT» («Європейська інтеграція: законодавство та Інтернет речей») у межах напрямку Жан Моне «Модуль» програми «Erasmus+» №620017-EPP-1-2020-1-UA-EPPJMO-MODULE (спільний проєкт КПП ім. Ігоря Сікорського, Еразмус+ Жан Моне Фонду та Виконавчого агентства з питань освіти, аудіовізуальної діяльності та культури за підтримки ЄС)». Підтримка Європейською комісією випуску цієї публікації не означає схвалення змісту, який відображає лише думки авторів, і Комісія не може нести відповідальність за будь-яке використання інформації, що міститься в ній.

Актуальність проекту для України пов'язана з визнанням високого теоретичного та практичного рівня законодавства ЄС різної галузевої спрямованості та впевненість у необхідності гармонізації з ним національного законодавства, зокрема в питаннях впровадження IoT. Тому для зменшення законодавчих бар'єрів та створення сприятливих умов для майбутніх з ЄС інвестиційних та інноваційних програм і проектів в рамках інтеграційних процесів модуль передбачає вивчення та дослідження низки європейських регламентів та директив або їх проектів. Насамперед, з питань кібербезпеки та критичної інфраструктури, захисту персональних даних, ідентифікації суб'єктів та наданні довірчих послуг, встановлення правового режиму відкритих даних, з правового регулювання застосування роботів та штучного інтелекту тощо. Вочевидь, зміни, які внаслідок впровадження IoT відбуваються у законодавстві, потребують від правників оновлення, іноді, кардинального, юридичних знань і навиків.

Модуль Жана Монне «Євроінтеграція: законодавство та Інтернет речей» (EULIoT) призначено, насамперед, для студентів, які вивчають магістерську програму з інформаційного права та правового забезпечення бізнесу інформаційних технологій, що є вагомим для їх професійної кар'єри. Причина того, чому цей навчальний курс є настільки важливим, полягає в тому, що він надає специфічні знання, які поєднують одночасно знання з юриспруденції та необхідні початкові знання з досить складної технологічної сфери.

Формування нового покоління юристів з такими інноваційними знаннями та навичками вкрай необхідне для майбутнього України на шляху економічного зростання в процесі інтеграції до ЄС, особливо в галузях де ефективно впроваджуються технології IoT, таких як: економіка, промисловість, сільське господарство, рітейл, будівництво, транспорт, державний сектор, медицина, освіта тощо.

Отримання знань із законодавчого забезпечення впровадження IoT буде корисним і для студентів та науковцівне юридичних спеціальностей, політикам, державним службовцям, представни-

кам громадських організацій таширокої громадськості в частині усвідомлення переваг інтеграції в ЄС, узгодженості європейських правових стандартів та ефективності європейського законодавства, яке створюється на основі поєднання інтелектуального та практичного досвіду всіх держав Євросоюзу.

Крім того, проект спрямовано на надання молодим викладачам і науковцям першого досвіду з викладання актуальних питань з законодавства, що регулює базові напрями розвитку ЄС, зокрема, в частині застосування IoT.

Модуль заснований на міждисциплінарному підході, що поєднує знання та результати дослідження як із загальних технічних питань функціонування передових технологій, так і з правових питань, пов'язаних із трансформацією змісту та форм соціальних відносин завдяки використанню сучасних технологій IoT у певних сектори соціальної діяльності.

Міждисциплінарна особливість проекту забезпечується тим фактом, що НТТУ «КПІ імені Ігоря Сікорського» має унікальну освітню можливість поєднувати політехнічну, юридичну та соціальну галузі знань. Більшість студентів технічних факультетів отримують спеціальності, пов'язані з цифровізацією соціальних процесів. В університеті зростає кількість технічних спеціальностей, лабораторій та досліджень в галузі IoT. Однак при цьому не охоплюються теми, пов'язані із законодавчою базою використання IoT, зокрема, беручи до уваги європейський досвід. Більше того, в інших університетах також не вистачає освітньої та наукової бази для вивчення як правових, так і технічних питань впровадження IoT у процесі європейської інтеграції.

Учасники команди Головки О.М. (координатор проекту) та Дубняк М.В. (менеджер проекту) мають ступінь кандидата юридичних наук в галузі інформаційного права та є експертами з питань інтелектуальної власності та медіабезпеки, мають досвід запровадження креативних методик викладання навчальних дисциплін.

Академічний керівник проекту Баранов О.А., професор кафедри інформаційного права та прав інтелектуальної власності має

не лише багаторічний викладацький досвід і досвід організації та реалізації на державному рівні проектів з цифрової трансформації суспільства, а й низку сучасних науково-дослідних юридичних робіт на тему проекту.

Завдяки творчому та гармонійному об'єднанню зусиль, учасники проекту отримають та поширять досвід викладання курсу з правових питань впровадження IoT, тісно пов'язаного з процесом європейської інтеграції в Україні.

Цілі навчального курсу: 1) продемонструвати загальну характеристику та правові питання впровадження IoT; 2) забезпечити глибоке розуміння законодавства ЄС у галузі IT; 3) з'ясувати результати порівняльно-правового аналізу законодавства ЄС та національного законодавства у сфері IoT. Це передбачає вивчення змісту, складу, особливостей, системних ризиків та бар'єрів використання IoT, а також роз'яснення політики ЄС щодо його розвитку. Центральними темами курсу є юридичні питання забезпечення кібербезпеки, пов'язаної з IoT, в контексті захисту критичної інформаційної інфраструктури, персональних даних та ідентифікації суб'єктів та об'єктів, що стосуються технологій IoT, використання роботів та штучного інтелекту, технологій хмарних обчислень та оброблення великих даних, застосування смарт-контрактів.

Проект базується на інноваційних формах навчання. Це сприяє набуттю навичок самостійного пошуку, виявлення та вирішення юридичних проблем, пов'язаних із використанням IoT. У цьому проекті також впроваджений інноваційний мультидисциплінарний підхід. Це дозволяє поєднувати знання з технічних питань та правових аспектів IoT. Це стає можливим завдяки унікальному поєднанню професіоналів з політехнічних та юридичних дисциплін.

Зміст дисципліни базується як на досягненнях європейської юридичної науки в цій галузі, сучасного європейського законодавства, так і на результатах власних досліджень учасників Проекту. Ці умови заохотять студентів до творчості, включаючи підготовку наукових робіт, статей, рефератів та вивчення справ у правовому регулюванні використання цифрових технологій.

Очікувані результати включають: створення спеціального курсу з правових проблем використання IoT крізь призму європейського законодавства; створення онлайн-курсу; видання навчального посібника, проведення тематичних конференцій, дискусій, семінарів; публікацію наукових праць; створення веб-ресурсу проекту; поширення інформації в соціальних мережах.

Дидактична та методологічна основа курсу має відповідати сучасним змінам вимог до знань та навичок майбутніх юристів. Курс створить певні умови для здобуття студентами:

- 1) знання про майбутні механізми правового регулювання застосування технологій IoT;
- 2) навички творчого, критичного мислення щодо правового регулювання нових суспільних відносин в умовах цифрової трансформації;
- 3) здатність пропонувати правові способи вирішення соціальних, технічних, економічних, організаційних та інших проблем, пов'язаних із використанням IoT.

Передбачається, що набуті знання та навички в процесі викладання такого інноваційного курсу стануть основою для формування курсів з інших правових тем, пов'язаних з європейською інтеграцією.

Наукове видання

**СОЦІАЛЬНА І ЦИФРОВА ТРАНСФОРМАЦІЯ:
ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ ПРОБЛЕМИ
ПРАВОВОГО РЕГУЛЮВАННЯ**

**МАТЕРІАЛИ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
10 ГРУДНЯ 2020 РОКУ**

Підписано до друку 05.01.2021.

Формат 60x84/16. Ум-друк. арк. 15,81.

Зам. № 2101-01.

Видано в ПП «Фенікс»

(Свідоцтво суб'єкта видавничої справи ДК № 1044 від 17.09.02).

Україна, м. Одеса, 65009, вул. Зоопаркова, 25.

Тел. +38 050 7775901 +38 048 7959160

e-mail: fenix-izd@ukr.net

www.feniksbooks.com