



Комітет Верховної Ради України з питань цифрової трансформації
Національна академія правових наук України
Державна наукова установа
«Інститут інформації, безпеки і права Національної академії правових наук 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

СОЦІАЛЬНА І ЦИФРОВА ТРАНСФОРМАЦІЯ: ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ

МАТЕРІАЛИ ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

2 ГРУДНЯ 2021 РОКУ

Київ – 2021

Рекомендовано до друку:

*вченою радою Державної наукової установи «Інститут інформації,
безпеки і права Національної академії правових наук України»
(протокол № 10 від 9 грудня 2021 р.);
секцією права національної безпеки та військового права
Національної академії правових наук України
(протокол № 10-17/2-Б від 9 грудня 2021 р.)*

С 69 Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання : матеріали Всеукр. наук.-практ. конф., м. Київ, 2 грудня 2021 р. / наук. керівник конф. О. А. Баранов ; упоряд.: В. М. Фурашев, С. О. Дорогих. – Київ-Одеса : Фенікс, 2021. – 324 с.

ISBN 978-966-928-759-5

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

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

Матеріали подано у авторській редакції.

УДК 34:004(477)

ISBN 978-966-928-759-5

- © Комітет Верховної Ради України з питань цифрової трансформації, 2021
- © Національна академія правових наук України, 2021
- © Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України», 2021
- © Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», 2021
- © Колектив авторів, 2020

ЗМІСТ

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ СОЦІАЛЬНОЇ ТРАНСФОРМАЦІЇ ВНАСЛІДОК ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ

Баранов О. А.

ЕКОНОМІКА РЕЗУЛЬТАТУ ТА ІНТЕРНЕТ РЕЧЕЙ:
ПРОБЛЕМА КІБЕРБЕЗПЕКИ. 10

Харитонов Є. О., Харитонova О. І.

ДО ПИТАННЯ РОЗУМІННЯ КАТЕГОРІЇ ПРАВОВОГО
ЗАБЕЗПЕЧЕННЯ 15

Корж І. Ф.

ШТУЧНИЙ ІНТЕЛЕКТ І ПРАВО. 22

Мічурін Є. О.

ШТУЧНИЙ ІНТЕЛЕКТ: ПРАВОВІ АСПЕКТИ 27

Гутюк І. В.

ПРАВОВЕ РЕГУЛЮВАННЯ ЕЛЕКТРОННОЇ ДЕМОКРАТІЇ В
УКРАЇНІ. 32

Нагнибіда В. І.

НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ВІДНОСИН
З ЦИФРОВИМИ АКТИВАМИ ТА ПЕРСПЕКТИВИ ЙОГО
УДОСКОНАЛЕННЯ. 36

Андрощук Г. О.

ЦИФРОВА ТРАНСФОРМАЦІЯ В КРАЇНАХ ЄС НА 2021 РІК 41

Дорогих С. О.

ПОБУДОВА НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ:
ІНОЗЕМНИЙ ДОСВІД 50

Андрієнко О. В.

ПРАВА НА ЕНЕРГІЮ, ІНФОРМАЦІЮ ТА СВОБОДУ
ІНТЕРПРЕТАЦІЇ ЯК МЕТАПРАВА СУБ'ЄКТІВ ФІЗИЧНОГО
ТА ЦИФРОВОГО СВІТУ 54

Марценко Н. С.

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ЦИВІЛЬНОМУ
СУДОЧИНСТВІ 59

Петровська А. О.	
ЦИФРОВА ТРАНСФОРМАЦІЯ У СФЕРІ СУДОЧИНСТВА. . .	65
Кваша Т. К.	
ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ: ПОТЕНЦІАЛ УКРАЇНСЬКОЇ НАУКИ.	70
Усенко Я. О.	
ПРАВОВІ ПРОБЛЕМИ ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ УПРАВЛІННЯ ПЕРСОНАЛОМ В СУДОВІЙ СИСТЕМІ УКРАЇНИ	74
Барсуковський О. Р.	
ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У СФЕРІ СІЛЬСЬКОГО ГОСПОДАРСТВА.	78
Prianykova Polina	
THE USE OF ARTIFICIAL INTELLIGENCE IN MUNICIPAL LAW, INTER ALIA IN LEGAL SYSTEMS INFLUENCED BY THE ROMAN-GERMANIC LEGAL TRADITIONS	82

ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ У СФЕРІ СОЦІАЛЬНИХ КОМУНІКАЦІЙ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Доронін І. М.	
ЗАГРОЗИ БЕЗПЕЦІ ТА ПРАВА ЛЮДИНИ В ІНТЕРНЕТІ: ПОШУК БАЛАНСУ.	87
Фурашев В. М.	
ІНФОРМАЦІЯ, ІНФОРМАЦІЙНЕ ПРАВО, ЦИФРОВІ ТЕХНОЛОГІЇ: ЗВ'ЯЗОК ТА ВПЛИВ НА СОЦІАЛЬНУ ТРАНСФОРМАЦІЮ.	92
Радзівська О. Г.	
ПРАВА ТА БЕЗПЕКА ОСОБИ В УМОВАХ СОЦІАЛЬНИХ І ЦИФРОВИХ ТРАНСФОРМАЦІЙ	96
Заславська Л. В.	
ЦИФРОВА ЕРА: НОВІ МОЖЛИВОСТІ ТА НОВІ ВИКЛИКИ ДЛЯ ЛЮДИНИ І СУСПІЛЬСТВА	101
Еннан Р. Є.	
КУЛЬТУРНА СПАДЩИНА У ЦИФРОВОМУ СЕРЕДОВИЩІ: ОСОБЛИВОСТІ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ МУЗЕЙНОЇ ДІЯЛЬНОСТІ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ . .	105

Борисов О. Ю.

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БАЛАНСУ МІЖ
ІНТЕРЕСАМИ ЛЮДИНИ, СУСПІЛЬСТВА ТА НАЦІОНАЛЬНОЇ
БЕЗПЕКИ В УМОВАХ АКТИВНОГО РОЗВИТКУ І
ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ 109

Нагнибіда А. В.

ПОНЯТТЯ І ЗМІСТ ЦИФРОВОГО СУВЕРЕНІТЕТУ ДЕРЖАВИ
В СУЧАСНОМУ ПРАВІ 114

Андрусенко А. О.

МІСЦЕ ПРАВА НА КІБЕРБЕЗПЕКУ В
СИСТЕМІНФОРМАЦІЙНИХ ПРАВ 120

Моргун А. М.

ПРАВА ЛЮДИНИ І ГРОМАДЯНИНА В ІНФОРМАЦІЙНІЙ
СФЕРІ 123

Дядюша В. В.

СОЦІАЛЬНІ МЕРЕЖІ ЯК НОВИЙ ВИМІР ВЕДЕННЯ
ІНФОРМАЦІЙНИХ ВІЙН 127

Скулинець І. В.

ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ
ІНФОРМАЦІЙНИХ ПРАВ ЛЮДИНИ В СОЦІАЛЬНИХ
МЕРЕЖАХ 130

Супрунович М. Ю.

ПРАВО НА ДОСТУП ДО ІНТЕРНЕТУ 134

ОСОБЛИВОСТІ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ РОЗВИТКУ СУЧАСНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ СУСПІЛЬСТВА

Пархоменко Н. М.

ЗАБЕЗПЕЧЕННЯ ПРАВ І СВОБОД ГРОМАДЯН З ОГЛЯДУ
НА ФУНКЦІОНУВАННЯ СУЧАСНИХ КОМУНІКАТИВНИХ
ПРАКТИК 138

Некіт К. Г.

ДО ПИТАННЯ ПРО ПРАВА НА МАШИННО ГЕНЕРОВАНІ
ДАНІ 143

Кігай В. А., Заблоцька А. О.

ВИКОРИСТАННЯ МУЛЬТИМЕДІЙНИХ ТЕХНОЛОГІЙ ПІД
ЧАС ЗАНЯТЬ З ТРУДОВОГО ПРАВА 148

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ СУСПІЛЬНИХ ВІДНОСИН В СФЕРІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ

Мисливий В. А.

ФОРМИ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ
ЦИФРОВОМУ ВИМІРІ..... 151

Капліна О. В.

ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ ПРОБЛЕМИ КРИМІНАЛЬНОГО
ПРОЦЕСУ УКРАЇНИ В УМОВАХ ЦИФРОВОЇ
ТРАНСФОРМАЦІЇ СУСПІЛЬСТВА 157

Каткова Т. Г.

ПРАВОВЕ РЕГУЛЮВАННЯ NFT..... 161

Костенко О. В.

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЗАСТОСУВАННЯ ЦИФРОВИХ
ОСОБИСТОСТЕЙ ТА АВАТАРІВ 166

Тихомиров О. О.

ДО ПРОБЛЕМИ ПРАВ ЛЮДИНИ В УМОВАХ
СТАНОВЛЕННЯ «ПРАВОВОГО СТАТУСУ» ШТУЧНОГО
ІНТЕЛЕКТУ 170

Грушева М. А.

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ: ШТУЧНИЙ
ІНТЕЛЕКТ І ТВОРЧІСТЬ 175

Мельник А. Я.

ПРОБЛЕМИ ВИКОРИСТАННЯ СИСТЕМИ БЛОКЧЕЙН В
ЕЛЕКТРОННОМУ ГОЛОСУВАННІ 179

Саградян А. Г.

ПОНЯТТЯ ТА СУТНІСТЬ СМАРТ-КОНТРАКТІВ 183

ПИТАННЯ ВДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА З ПИТАНЬ ЗАХИСТУ ПРАВ ЛЮДИНИ В УМОВАХ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ

Смерницький Д. В.

ЗАХИСТ ПРАВ ЛЮДИНИ ПРИ ВИКОРИСТАННІ СУЧАСНИХ
ЦИФРОВИХ ТЕХНОЛОГІЙ: ПРАВОВІ ОСНОВИ 190

Шевченко О. А.

СТРАТЕГІЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ ЯК
ДОРОГОВКАЗ ДЛЯ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ У
СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 195

Марусенко Р. І.

ПРАКТИЧНІ АСПЕКТИ ВИКОРИСТАННЯ ЕЛЕКТРОННИХ
ДОКУМЕНТІВ, ЩО МІСТЯТЬ ВІДОМОСТІ ПРО ОСОБУ .. 199

Тарасенко Л. Л.

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЯК ОБ'ЄКТ ІТ
ПРАВОВІДНОСИН 205

Чорна В. Д., Алексєєнко І. В.

ІНФОРМАЦІЙНІ ПРАВА ЛЮДИНИ В УКРАЇНІ:
ПРОБЛЕМАТИКА ПРАВОВОГО ВИЗНАЧЕННЯ 210

Сероштан М. Г., Алексєєнко І. В.

ПИТАННЯ ВДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА З ПИТАНЬ
ЗАХИСТУ ПРАВ ЛЮДИНИ В УМОВАХ ВИКОРИСТАННЯ
ЦИФРОВИХ ТЕХНОЛОГІЙ (ЗАХИСТУ ПЕРСОНАЛЬНИХ
ДАНИХ, ЗАБЕЗПЕЧЕННЯ ІНФРАСТРУКТУРНОЇ БЕЗПЕКИ,
КІБЕРБЕЗПЕКИ ТОЩО)..... 215

Швед А. С.

ВДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА З ПИТАНЬ ЗАХИСТУ
ПРАВ ЛЮДИНИ В УМОВАХ ВИКОРИСТАННЯ ЦИФРОВИХ
ТЕХНОЛОГІЙ. 220

Чорнобай Е. О.

СИСТЕМИ РОЗПІЗНАВАННЯ ОБЛИЧ: ПРИВАТНІСТЬ ПРОТИ
БЕЗПЕКИ. 225

Зайцева А. В.

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ РОЗПІЗНАВАННЯ ОСІБ У
КОНТЕКСТІ ПРАВ ЛЮДИНИ НА ЗАХИСТ ПЕРСОНАЛЬНИХ
ДАНИХ 230

Максаков О. Ю., Алексєєнко І. В.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ 233

Павлік О. О.

ПЕРСОНАЛЬНІ ДАНІ В МЕРЕЖІ ІНТЕРНЕТ ЧЕРЕЗ ПРИЗМУ
ПРАВОВОГО ЗАХИСТУ ТА РЕГУЛЮВАННЯ. 235

Павлюк А. Ю.	
ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ	240
Радченко К. В.	
ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ МІСЦЕВОГО САМОВРЯДУВАННЯ: ДОСВІД МІСТА БРІСТОЛЬ, ВЕЛИКОБРИТАНІЯ.	245
Галак А. В.	
ПРОБЛЕМАТИКА ЗАХИСТУ ПРАВ ЛЮДИНИ В КІБЕРПРОСТОРІ	250
Пойда Д. О.	
ВПЛИВ СОЦІАЛЬНИХ МЕРЕЖ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ОСОБИСТОСТІ	254
Орел Г. П.	
ЗАХИСТ ПРАВ ЛЮДИНИ В СОЦІАЛЬНИХ МЕРЕЖАХ . . .	258
Данілевич Д. Р.	
ПОРУШЕННЯ ЦИФРОВИХ ПРАВ ЖІНОК У СУЧАСНОМУ СВІТІ	260
Дергачова А. О.	
ВПЛИВ ЦИФРОВИХ ТЕХНОЛОГІЙ НА ПРАВА ЛЮДИНИ. .	264
Голубєва Д. В.	
ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ПРАВ І СВОБОД УРАЗЛИВИХ КАТЕГОРІЙ НАСЕЛЕННЯ (ПІДЛІТКІВ) В ІНФОРМАЦІЙНОМУ ПРОСТОРІ	268
Баюрчак М. І.	
ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ. . .	270
Годлевська В. Ю.	
НАЦІОНАЛЬНИЙ КРИПТОЛОГІЧНИЙ ЦЕНТР В СИСТЕМІ КІБЕРБЕЗПЕКИ ІСПАНІЇ	273
Мурашкіна Я. Ю.	
ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ГАРАНТІЯ ПРАВ ЛЮДИНИ.	277
Свистонюк В. А.	
АДМІНІСТРАТИВНО-ПРАВОВІ ЗАХОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОГО ПРАВОПОРЯДКУ.	281

Власюк Є. П.	ВІДПОВІДАЛЬНІСТЬ ЗА РОЗПОВСЮДЖЕННЯ НЕДОСТОВІРНОЇ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТ ...	285
Лаптева Т. О.	МЕТОДИ ВИЯВЛЕННЯ ТА ПРИПИНЕННЯ РОЗПОВСЮДЖЕННЯ НЕДОСТОВІРНОЇ ІНФОРМАЦІЇ В ІНТЕРНЕТЕ.....	290
Шикір Д. О.	УДОСКОНАЛЕННЯ НАДАННЯ АДМІНІСТРАТИВНО- ІНФОРМАЦІЙНИХ ПОСЛУГ В УМОВАХ ДІДЖИТАЛІЗАЦІЇ .	294
Ворона Ю. С., Миронюк Р. В.	НЕОБХІДНІСТЬ ЗАПРОВАДЖЕННЯ МЕДІАЦІЇ У АДМІНІСТРАТИВНЕ СУДОЧИНСТВО	298
Малиш Н. В.	СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ ПРАВОВОГО РЕГУЛЮВАННЯ ДИСТАНЦІЙНОЇ ПРАЦІ ...	301
Кукурік А. В.	ВТІЛЕННЯ ВІДНОВНИХ ПРАКТИК ПІД ЧАС ПАНДЕМІЇ COVID-19	306
Васько В. А.	ПРОБЛЕМА ВИЗНАЧЕННЯ ЗМІСТУ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ ДЕЦЕНТРАЛІЗОВАНИХ СЕРВІСІВ ОБМІНУ КРИПТОАКТИВІВ	311
Стрельник В. В., Мироненко А. О.	ПРАВА ЛЮДИНИ ЧЕРЕЗ ПРИЗМУ РОЗВИТКУ ШТУЧНОГО ІНТЕЛЕКТУ	317
Алексеева А. Р.	ПЕРСПЕКТИВИ РОЗВИТКУ КІБЕРБЕЗПЕКИ ЯК МЕТОДУ ЗАХИСТУ ПРАВ ЛЮДИНИ	321

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ СОЦІАЛЬНОЇ ТРАНСФОРМАЦІЇ ВНАСЛІДОК ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ

Баранов О. А.

доктор юридичних наук, керівник
Наукового центру цифрових
трансформацій і права Державної
наукової установи «Інститут інформації,
безпеки і права Національної академії
правових наук України»

ЕКОНОМІКА РЕЗУЛЬТАТУ ТА ІНТЕРНЕТ РЕЧЕЙ: ПРОБЛЕМА КІБЕРБЕЗПЕКИ

Останні півтора десятиліття в багатьох країнах реалізуються амбітні національні стратегії та програми застосування в усіх сферах, зокрема, економічної діяльності технологій Інтернету речей (Internet of Things, IoT) та штучного інтелекту (ШІ). Саме завдяки розумінню надзвичайної економічної ефективності та перспектив впровадження технологій IoT та ШІ з'явився та отримує поширення новий концепт трансформації економіки – розвиток *Економіки результату (Outcome Economy)* [1,2].

Економіка результату – це людиноцентристська економіка з величезним ресурсозберігаючим та інноваційним потенціалом, зі зміненою природою екосистем коопераційної взаємодії та конкуренції, з глобальною (міжнародною) соціо-технологічною базою, в якості якої виступають технології IoT. Тому реалізація стратегії розвитку Економіки результату зажадає проведення масштабних соціальних і цифрових трансформацій як на міжнародному, так і на національних рівнях [3].

Широкое застосування цифрових технологій IoT в умовах Економіки результату загострює проблеми кібербезпеки, проте ні

Cisco [4, 5], ні ENISA [6] не наводять вичерпного переліку загроз, пов'язаних із використанням технологій IoT. Очевидно, це пояснюється тим, що загрози безпеці виникають як наслідок кількох основних явищ.

Перше – це розвиток відомих і поява нових технологій та їх складових, комп'ютерних та програмних засобів, зразків робототехніки тощо, що природно має наслідком появу нових видів та типів технічних систем та комплексів, а також їх нового функціонального використання.

У сучасному динамічному процесі поява нового в техніці досить часто базується на старт-ап-івській стратегії та образі дій, в основі яких лежить єдине прагнення – якнайшвидше опанування ринку. Тому все частіше проекти запускаються у масове використання без ретельного опрацювання технічних рішень та без проведення попередніх випробувань, що має наслідком наявність широкого спектру недоробок та недоліків. Підтвердженням поширення такої ущербної стратегії завоювання масового ринку є численні оновлення базового програмного забезпечення різноманітних гаджетів та далеко не самотні випадки відкликання з ринків для подальшої модернізації певних зразків техніки, навіть такої складної як автомобілі.

Експерти вважають, що часто недоробки та недоліки технічних рішень, що проектуються, є джерелом інформаційних загроз (кіберзагроз), про наявність яких розробники навіть не підозрюють. Це так звані погрози нульового дня. Сукупність загроз нульового дня є живильним середовищем для хакерів, що атакують технічні системи та комплекси, які включають комп'ютерні та програмні засоби.

Таким чином, процес розвитку відомих і проектування, виробництва та експлуатації нових технічних систем та комплексів є природним потужним джерелом інформаційних загроз. Як правило, більшість цих загроз мають латентний характер, оскільки вони виявляються лише на практиці, у процесі експлуатації і тому не можуть бути вчасно виявлені на стадії проектування та вичерпно описані.

Друге - цілеспрямована діяльність хакерів з пошуку вразливості в ІКТ, що створює можливості для проведення спеціальним чином підготовлених, організованих та реалізованих атак на технічні системи та комплекси IoT. Цілі таких атак мають різне призначення: від порушення функціонування технічних систем та комплексів для завдання масового збитку до отримання економічної та фінансової вигоди від впливу на конкретні об'єкти. Широко відомо, що засоби нападу (атак) у своєму розвитку (появі) завжди випереджають засоби захисту від них, тому будь-які огляди хакерських загроз принципово не можуть містити їх вичерпний опис.

Третє – поява абсолютно нових методів, способів та засобів технологічних рішень, заснованих на наукових та технічних інноваціях, які раніше не були відомі. Як правило, у цьому випадку розробники пріоритетну увагу приділяють базовому функціоналу технологій, а розгляд проблеми визначення можливих (потенційних) загроз інформаційній безпеці належить до другого плану, якщо вони взагалі розглядаються. Більше того, саме третій напрямок є джерелом появи нових класів та видів кіберзагроз, ідентифікація яких може бути досить тривалою у часі.

Два перших напрямки – це класичні (традиційні) напрямки, наслідком яких є поява джерел інформаційних загроз (кіберзагроз) для будь-яких програмних комплексів та систем будь-якого призначення та будь-якого рівня складності, у тому числі і тих, що входять до складу IoT.

Третій напрямок – це напрямок, який вимагає проведення глибоких комплексних аналітичних досліджень такої конкретної предметної сфери як арена майбутніх соціальних трансформацій, які можуть мати місце внаслідок застосування результатів 4-ї технологічної революції. Організація таких досліджень по широкому колу напрямів дозволяє сподіватися на отримання досить достовірних прогнозів тенденцій і закономірностей розвитку як соціуму загалом, так і технологічної основи його функціонування. Безперечно, складовою цих зусиль мають бути дослідження варіантів та особливостей побудови систем забезпечення кібербезпеки як відповіді на майбутні нові виклики у сфері інформаційної безпе-

ки. Загалом проведення таких досліджень створить сприятливий ґрунт для зменшення сингулярності у розумінні майбутніх соціальних моделей цивілізації, що є дуже критичним для розвитку правової науки.

Зміна змісту національних стратегій кібербезпеки протягом останніх 20 років відбувається еволюційним шляхом одночасно з еволюцією розуміння значення та ролі процесу проникнення інформаційних комп'ютерних та телекомунікаційних технологій у всі сфери соціальної активності.

Аналіз кількох десятків національних стратегій кібербезпеки, які приймалися на найвищому політичному рівні, дозволяє виділити такі етапи формування мети кібербезпеки: 1) мета – захист інформації; 2) мета – захист комп'ютерних систем; 3) мета – забезпечення безперешкодного доступу до послуг, що надаються з використанням мережі Інтернет, та забезпечення цілісності та конфіденційності даних; 4) ціль – забезпечення функціонування критично важливих інфраструктурних систем суспільства; і, нарешті, 5) (сучасний) етап: мета – кібербезпека має стати невід'ємною складовою всеосяжної політики розвитку особистості, суспільства та держави.

Необхідність виділення п'ятого етапу розвитку кібербезпеки обумовлена сучасним розумінням соціальної значущості та масштабності процесів цифрової трансформації розвитку суспільства, зокрема в умовах Економіки результату. Проте, нині ще не сформувалася міжнародна консолідована точка зору щодо зміст мети кібербезпеки п'ятого етапу.

Переваги використання технологій Інтернету речей ґрунтуються на широкому використанні комп'ютерних та телекомунікаційних технологій, технологій штучного інтелекту, хмарних обчислень, обробки великих даних. Експерти практично одноставно стверджують, що ця обставина є причиною необхідності пильної уваги до вирішення проблеми забезпечення кібербезпеки в умовах широкого використання технологій Інтернету речей.

Особливості розвитку технологій IoT як одного з найважливіших напрямів цифрової трансформації створюють сприятливий ґрунт для формування системи різноманітних загроз кібербезпеці.

Класифікація та систематизація як джерел кіберзагроз, так і власне конкретних кіберзагроз є актуальним завданням, вирішення якого може дозволити обґрунтувати структуру та зміст системи забезпечення кібербезпеки. Особливу актуальність має завдання ідентифікації джерел можливих кіберзагроз на етапах проектування, розробки та експлуатації технологій IoT.

Один із дієвих механізмів нейтралізації кіберзагроз це створення системи правового регулювання забезпечення кібербезпеки.

Нагальна необхідність активізації процесів соціальної трансформації та цифрової трансформації на тлі каскаду різних світових і локальних криз, що триває, зумовлює актуальність перегляду парадигми забезпечення кібербезпеки.

Використана література

1. 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 23.11.2021.

2. 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 23.11.2021.

3. О Баранов, Економіка результату як нова парадигма економічного розвитку. Системний аналіз міжнародних економічних відносин: зб. матеріалів наук.- практ. конф., м. Київ, 24-25 червня 2021 р. – Київ : Інститут міжнародних відносин КНУ ім. Т. Шевченка, 2021. – С. 83-85.

4. JFrahim and others, ‘Securing the Internet of Things: A Proposed Framework’ (Cisco White Paper March 2015) <https://tools.cisco.com/security/center/resources/secure_ietf_proposed_framework#1> дата звернення 23.11.2021.

5. W Stallings, ‘The Internet of Things: Network and Security Architecture’ (2015) Vol. 18 4 The Internet Protocol Journal 2 <<http://ipj.dreamhosters.com/wp-content/uploads/2016/01/ipj-v18n4.pdf>> дата звернення 23.11.2021.

6. Looking into crystal ball. A report on emerging technologies and security. VERSION 1.0. January 2018 European Union Agent for Network and Information Security Challenges <<https://www.enisa.europa.eu/publications/looking-into-the-crystal-ball>> дата звернення 23.11.2021.

Харитонов Є. О.

доктор юридичних наук, професор,
завідувач кафедри цивільного права
НУ «Одеська юридична академія»,
Член-кореспондент НАПрН України

Харитонova О. І.

доктор юридичних наук, професор,
завідувач кафедри права
інтелектуальної власності та
корпоративного права НУ «Одеська
юридична академія»,
Член-кореспондент НАПрН України

ДО ПИТАННЯ РОЗУМІННЯ КАТЕГОРІЇ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ

Приступаючи до розгляду проблем правового/юридичного забезпечення об'єктивних та суб'єктивних приватних прав, передусім, необхідно зазначити, що у літературі вираз «правове забезпечення» є широко вживаним у різному контексті: «правове забезпечення підприємництва», «правове забезпечення безпеки життєдіяльності», «правове забезпечення безпеки довкілля» тощо. Однак зазначений вираз вживається, зазвичай, як поняття «*sui generis*», не визначається, не розшифровується і не характеризується спеціально. Натомість, він непрямо розкривається через інші поняття, котрі вживаються як його синоніми: «правове регулювання», «правова база» тощо. При цьому, скажімо, «правова база підприємництва» визначається як сукупність законів, нормативних та інструктивних документів, які визначають порядок створення підприємств, реєстрацію фізичних осіб-підприємців, їхні правові та організаційні форми, порядок організації виробництва, забезпечення його необхідними ресурсами, збут, систему оподаткування, відносини між державою та підприємцями, суб'єктів підприємницької діяльності між собою, а також дають підприємцям певні правові гарантії. Отже, в результаті маємо досить «розмите» уяв-

лення про те, що таке правове забезпечення у цій галузі, а точніше, не маємо його зовсім, оскільки можемо з однаковим успіхом вести мову і про «правове забезпечення», і про правове регулювання», і про «нормативне регулювання» тощо. Тому звернемося до довідкових юридичних видань. І з'ясуємо, що у вітчизняній Юридичній енциклопедії таке поняття не згадується. Проте, тут є визначення поняття правове регулювання, котре «забезпечується за допомогою спеціально створеного державою правового механізму» [1, с. 40]. Не міститься поняття «юридичне забезпечення» (чи «цивільно-правове забезпечення») і у Енциклопедії цивільного права України [2]. Фактично, ототожнюються поняття «правове забезпечення» та «правове регулювання» і у дослідженнях вітчизняних науковців [3, с. 155, 167, 180].

Оскільки нашим завданням не є огляд літератури, не будемо зупинятися на цьому питанні детальніше. Зазначимо лише, що навіть при випадково-вибірковому аналізі впадає в око відсутність розрізнення зовнішньо подібних, але різних за сутністю правових категорій. Можемо констатувати, що підхід, при якому не розрізняються «правове забезпечення» і «правове регулювання», є досить популярним і дає підстави вважати його проявом типового бачення сутності відповідних категорій.

Зустрічаються, щоправда, праці, у яких поняття «правове забезпечення» розглядається як складна категорія, котра не зводиться до правого регулювання якогось виду суспільних відносин. Так, О. В. Вишняков, розглядаючи напрями правового забезпечення зовнішньоекономічної інтеграції України, поділяє їх на загальні та окремі, визначаючи перший як зняття існуючих взаємних претензій між Україною і ЄС і перехід на новий ступінь відноси, і, відносячи до других імплементацію міжнародних договорів України та інших міжнародно-правових документів, регулювання підприємницьких відносин, інвестиційне регулювання та правову охорону іноземної власності, реформу судової системи та захист приватного бізнесу [4, с. 66-132]. Як впливає звідси, автор під ним має на увазі не тільки правове регулювання відповідних відносин, але також і життя, переду-

сім державою, певних організаційно-правових заходів для досягнення певної мети. Проте, і в цьому випадку переважає аналіз вирішення завдань «правового забезпечення» за допомогою того самого правового регулювання.

Отже спробуємо визначитися стосовно поняття «правове забезпечення» та його відмінностей від суміжних, згаданих вище та інших, категорій. При цьому зазначимо, що у літературі йдеться, головним чином про «правове забезпечення». Таке найменування, звісно, можливе, однак з погляду зручності формулювань більш придатним видається термін «юридичне забезпечення», оскільки це дозволяє уникати недолугої конструкції «правове забезпечення права». Разом із тим, враховуючи традицію вживання згаданого позначення, будемо за необхідності послуговуватися й виразом «правове забезпечення».

«Забезпечення» у його повсякденному, побутовому значенні – це створення надійних умов для здійснення чого-небудь. Відповідно, «правове забезпечення» – це створення правовими засобами надійних умов для здійснення чого-небудь, вирішення якихось завдань, що являють інтерес для суспільства (держави) .

У контексті розгляду питання про сутність та значення правового/юридичного забезпечення реалізації приватного права не може бути залишена поза увагою категорія «примус» («державний примус», «публічний примус»), оскільки правовий вплив (реалізація норм) на учасників суспільних відносин, а відтак і виконання забезпечувальної функції останніх здійснюється не тільки і не стільки шляхом переконання (заохочувального стимулювання), скільки шляхом примусу [5, с. 8]. Зокрема, можливість державного примусу до виконання вимог норм права, є однією з ознак, що дозволяє відрізнити їх від інших соціальних норм.

У вітчизняній юриспруденції були спроби розмежування державного та приватного примусу. При цьому називалися наступні відмінності між цими категоріями:

1) сфера застосування державного примусу значно ширша, ніж сфера приватного примусу;

2) суб'єкт реалізації державного примусу не є стороною (учасником) тих відносин, з яких випливає спір. Натомість, особа, яка застосовує приватний примус, як правило, є стороною спірних правовідносин;

3) порядок (процедура) застосування державного примусу врегульована законом, тоді як процедура реалізації приватного примусу визначена в законі приблизно [6, с. 413-418].

Проте, поки що такі пропозиції виглядають недостатньо переконливими. Достатньо, хоча б, згадати про те, що у випадку «не спрацювання» приватного примусу суб'єкти відповідних відносин можуть перенести розгляд спору у суд, після чого їх стосунки продовжують розвиватися у межах «звичайного» правового регулювання. Якщо ж вони до суду не звертаються, то у разі відмови зобов'язаної сторони підкоритися приватному примусу, стосунки учасників таких відносин вибувають за межі правового поля (звісно, якщо при застосуванні приватного примусу не буде вчинено правопорушення).

Крім того, здається невинуватим використання у якості критерію розмежування зазначених понять тієї обставини, що сфера застосування одного з них є ширшою, ніж іншої. Це, радше, можна вважати наслідком реальної потреби у тому чи іншому інституті, яка існує у суспільстві, ментальності, правосвідомості людей тощо.

Тому більш коректним здається вести мову про «державний» примус» та «приватний примус, санкціонований державою», котрі врешті, можуть бути поєднані в узагальнюючому понятті «правовий» (юридичний) примус. Останнє, у свою чергу, фактично, є тотожним поняттю «державний примус».

Сутність державного примусу характеризується через його визначальні ознаки, до яких належить, зокрема, те, що він: здійснюється від імені держави її органами або іншими фігурантами; має правовий характер, оскільки застосовується у визначених законом формах, на законних підставах відповідними компетентними органами; здійснюється у зв'язку з неправомірною поведінкою учасників регулятивних правовідносин; відображає конфлікт

між державною волею, вираженою у нормі права, та індивідуальною волею осіб, що її порушили; являє собою зовнішній вплив на суб'єкта з метою примусити його виконувати правові приписи, не допустити нових порушень тощо шляхом впливу на немайнову або майнову сферу конкретного суб'єкта права; є засобом забезпечення бажаної поведінки учасників правовідносин; здійснюється за допомогою юрисдикційних, правозастосовчих актів.

Грунтуючись на такому розумінні державного примусу, далі виходимо з того, що для забезпечення впровадження цивілізаційних феноменів, яким, зокрема, є концепт приватного права, у певне суспільство, держава, як механізм організації життя цього суспільства, має здійснювати в межах правового поля низку заходів. Таким чином відбувається (має відбуватися) «об'єктивізація» згаданих феноменів (у тому числі, права), перехід їх з абстрактного цивілізаційного рівня на рівень цінностей, категорій, інституцій відповідної держави. Нерідко, від держави вимагаються значні зусилля, щоб впровадити якісь бажані для більшості (або для правлячої еліти) цивілізаційні феномени, ідеологію тощо в життя суспільства. Прикладів такого впровадження можна навести багато. Наприклад, впровадження християнства, а потім визнання його державною релігією у Стародавньому Римі, хрещення населення багатьох європейських держав, хрещення Київської Русі тощо.

Хоча, очевидно, згадані зусилля має вживати не лише держава, а й суспільство в цілому, оскільки без цього процес іноді уповільнюється, а іноді взагалі стає неможливим. Така умова не є обов'язковою. Проте, у випадках, коли державі (самотужки чи з допомогою зовнішніх сил) вдається нав'язати суспільству цінності, котрі суперечать його генетичному коду, ментальності і природному шляху еволюції, існує велика вірогідність зворотності процесу. Прикладом може слугувати історія тих імперій, котрі прагнули (часом досить успішно) поширити на підвладні території свої власні цінності. Такі цінності після розпаду імперії зберігалися тією мірою, наскільки вони відповідали прагненню колишнього підвладного суспільства. Чи не найбільш яскравим прикладом є історія СРСР з його виникненням, піднесенням і загибеллю,

оскільки тут відбувалося щеплення не природних цінностей, а їх адаптованого до комуністичної ідеології варіанту.

У кожному разі, юридичне /правове забезпечення впровадження в життя суспільства ідеї права, як цивілізаційної категорії, не може полягати лише у виданні якихось нормативних актів та більш чи менш постійного та ефективного нагляду за їхньої реалізацією. Цілком очевидно, що зусилля держави є лише одним із засобів форм юридичного/ правового забезпечення. Отже, маємо розрізняти державне та недержавне (громадське) правове забезпечення.

Характеризуючи «державне правове забезпечення», маємо ще раз звернути увагу на необхідність розрізняти у цій галузі (втім, як і у інших) «правове» і «законодавче» забезпечення, що впливає з того, що поняття «право» і «закон» не є тотожними.

Що стосується класифікації діяльності держави (зусиль держави) по юридичному/правовому забезпеченню, то вона може виглядати таким чином:

1) методологічне та доктринальне забезпечення. Розробка концепції, визначення засад правового забезпечення тощо; підтримка певної доктрини права. Можливо, сюди варто віднести й ідеологічне забезпечення, як форму державних зусиль по створенню світоглядного підґрунтя, впровадження нових (обновлюваних) правових феноменів; 2) законодавче забезпечення. Сюди можна віднести видання законів та інших актів законодавства, санкціонування правових звичаїв та норм моралі, що стосуються об'єкта законодавчого забезпечення; 3) забезпечення належної реалізації норм законодавства, які стосуються об'єкта забезпечення, за допомогою відповідних державних інституцій, судової системи; 4) інформаційно-пропагандистське (виховне) забезпечення. Роз'яснення сутності положень, що впроваджуються, мети впровадження тощо. Правова освіта, яка здійснюється у певному напрямку; 5) організаційне забезпечення. Визначається орган (органи), що відповідають за ті чи інші напрями впровадження, їх компетенція, взаємодія тощо.

Що стосується недержавного (громадського) правового забезпечення, то до його форм, передусім, варто віднести: 1) світоглядне забезпечення, яке, очевидно, охоплює й правову мен-

тальність населення суспільства. Цінності, інституції, категорії, поняття, які впроваджуються, мають або бути такими, що не суперечать світогляду більшості суспільства, або адаптованими до визнаних світоглядних засад; 2) доктринальне забезпечення – у тій його частині, що виникає незалежно від завдань держави щодо наукових розробок (і зацікавленості держави у таких розробках). Впровадження правових цінностей, системи права, правових інститутів, державних інституцій має відбуватися за умови забезпечення готовності до такого впровадження з боку правознавців – фахівців у цих та суміжних галузях; 3) правосвідомість населення. Правосвідомість може слугувати як стимулюючим, так і гальмуючим чинником. Цінності можуть впроваджуватися на вже існуюче підґрунтя, але, частіше, така основа формується у процесі впровадження.

Що стосується недержавних форм правового забезпечення, то тут зауважимо можливість існування значного розмаїття у світоглядних засадах, ментальності, поглядах фахівців, рівнях правосвідомості у різних верств населення, у різних регіонах тощо. Але це тема окремого дослідження.

Література:

1. Юридична енциклопедія: В 6 т. /Редкол.: Ю. С. Шемшученко (голова редкол.) та ін. К., Т.5. 2003.
2. Енциклопедія цивільного права України; відп. ред. Я. М. Шевченко. К., 2009. 952 с.
3. Вінник, О. М. Публічні та приватні інтереси в господарських товариствах: проблеми правового забезпечення: Монографія. К., 2003.
4. Вишняков О. К. Правове забезпечення зовнішньоекономічної інтеграції України : Монографія. Одеса, 2007.
5. Яковлев В. Ф. Гражданско-правовые средства обеспечения реального и надлежащего исполнения хозяйственных договоров / В. Ф. Яковлев. Гражданское право, эффективность и качество. Свердловск, 1977.
6. Горайнов А. М. Самозахист як засіб приватного правового примус. *Держава і право*. 2011. Вип. 53. С. 413-418.

Корж І. Ф.

доктор юридичних наук, старший
науковий співробітник, завідувач
наукової лабораторії, ДНУ «Інститут
інформації, безпеки і права
Національної академії правових наук
України НАПрН України»

ШТУЧНИЙ ІНТЕЛЕКТ І ПРАВО

Останнім часом штучний інтелект все більше і більше привертає увагу в соціумі світу. Як зазначає Білл Гейтс, саме ця інновація має найбільший потенціал змінити наше життя на краще, зробити його «продуктивнішим», ефективнішим та загалом легшим [1]. Одночасно і науковці стверджують, що незабаром люди повністю поміняють своє бачення про можливості інтелектуальних технологій, і штучний інтелект запрацює не лише у сфері побуту та надання послуг, а й у найбільш важливих сферах життєдіяльності людини.

Насамперед, це стосується сфери медицини. Штучний інтелект вже сьогодні почав потрапляти в лікарські кабінети, а отже, це лише питання часу, коли він стане там звичайним явищем. Від потужних діагностичних алгоритмів до точно налаштованих хірургічних роботів ця технологія робить свою присутність надзвичайно видимою у всіх медичних сферах.

Наразі штучний інтелект досить добре справляється з діагностикою хвороб: так дослідники в шпиталі імені Джона Редкліффа в Оксфорді розробили таку систему діагностики, яка у 80% випадків краще за медиків виявляє хворобу серця, а в Гарвардському університеті вчені навчили «розумний мікроскоп» бачити небезпечні інфекції в крові. В минулорічному дослідженні штучному інтелекту вдалося швидше діагностувати метастатичний рак молочної залози, ніж радіологам, йдеться у статті. Штучний інтелект також проявив здатність визначати ризик розвитку захворювань, пов'язаних із віком, таких як рак і серцеві захворювання, повідомляє The Daily Mail [2].

Для прикладу можна навести наступні факти: хірурги створили катетер-робот, який сам пробрався до необхідного клапана в серці і провів операцію, застосувавши алгоритми машинного навчання, штучний інтелект і камеру. Роботизований катетер розробили вчені Гарвардської медичної школи (США), Університету Страсбурга (Франція) і тайбейський лікарні для ветеранів в Тайвані. Алгоритми дозволяли роботу розрізняти тип тканини, до якого він торкається і куди слід рухатися для досягнення мети, передає Science Daily [3]. Штучний інтелект навчили упізнавати кров, стінки серцевого шлуночка і аортальний клапан. Датчик також аналізував силу тиску на клапан, щоб той не пошкодив серце. Новий катетер випробували під час операції на свинях, яким встановили штучні аортальні клапани, які потребують хірургічного втручання. В одній операції катетер був автономний, в іншій ним керував лікар, а у третій хірург оперував вручну. Автономному роботу треба було трохи більше часу, ніж медику, проте в загальному робот провів 89 успішних операцій з 90.

Нова технологія може запустити початок переходу від роботизованих хірургічних інструментів до операцій за участю роботів. Вона детально описана в журналі Science Robotics [4]. Можна констатувати, що українські кардіохірурги з київського Інституту серця імплантували третє механічне серце. Воно забезпечує пацієнту повну циркуляторну підтримку, коли рідне серце не здатне. Також стало відомо, що київські хірурги навчилися видаляти пухлину мозку за новою методикою.

Згідно дослідження міжнародного аналітичного агентства Global Market Insights, з 2017 по 2024 р. очікується щорічне зростання використання штучного інтелекту у сфері охорони здоров'я аж до 40%. Тобто вплив штучного інтелекту на медицину складатиме майже 50%. Нині штучний інтелект застосовується при діагностиці захворювань, дослідженні генома, розробці лікарських засобів. Вони дозволяють більш якісно надавати відповідні відомості, обслуговувати пацієнтів, економити час та кошти.

Оскільки цифрові технології стають все більш важливою частиною кожного аспекту життя, люди повинні мати можли-

вість довіряти їм. Достовірність також є умовою його реалізації. Це можливість для Європи, враховуючи її тверду прихильність цінностям і верховенству закону, а також доведену здатність створювати безпечні, надійні і складні продукти і послуги від авіації до енергетики, автомобільного і медичного обладнання, – йдеться в передмові до Європейської Білої книги з штучного інтелекту. «Біла книга з штучного інтелекту (ШІ). Європейський підхід до досконалості і довіри» (анг. White Paper on Artificial Intelligence A European approach to excellence and trust), опублікована 19 лютого 2020 р., як і передбачалося, має на меті представити можливі зміни, «які сприятимуть надійному та безпечному розвитку штучного інтелекту в Європі при повній повазі цінностей і прав громадян ЄС». Комісія ЄС запропонувала створити правові засади для штучного інтелекту, засновані на «досконалості і довірі».

Європейський підхід до штучного інтелекту спрямований на просування інноваційного потенціалу Європи в області штучного інтелекту, підтримуючи при цьому розвиток і використання етичного і заслугуючого на довіру ШІ у всій економіці ЄС. ШІ повинен працювати на людей і бути силою, яка працює на благо суспільства...», – йдеться у Білій книзі.

*Завдяки ШІ ми можемо поліпшити якість нашого життя. У будь-якому випадку ця технологія вже використовується і, наприклад, допомагає в більш ранній діагностиці таких захворювань, як рак, що вкрай важливо для людей. Штучний інтелект також може допомогти Європі в досягненні кліматичних цілей завдяки інтелектуальним сільськогосподарським технологіям або інтелектуальному опаленню, які дозволяють скоротити викиди вуглекислого газу в атмосферу, – сказала президент ЄС **Урсула фон дер Лайєн (Ursula von der Layen)** на зустрічі з журналістами.*

*Проте Комісія також підкреслює, що технологія також несе в собі ризик зловживання, тому ЄС повинен ввести правила, що регламентують безпеку його використання. Установи, а також підприємства і жителі повинні довіряти технологіям і відчувати себе в безпеці», – сказав комісар ЄС з питань промисловості та внутрішнього ринку **Тьєррі Бретон (Thierry Breton)**.*

На думку ЄС, штучний інтелект в ЄС повинен бути орієнтований на людину. На практиці це означає, що системи ШІ повинні бути прозорими, користувач повинен знати про їх використання, і вони повинні контролюватися людиною. І саме людина, а не машина, повинна приймати остаточні рішення [5]. Комісія також хоче конкретно контролювати використання ШІ в системах високого ризику, тобто в системах, які можуть порушувати права громадян, наприклад, право на недоторканність приватного життя.

Акцент в цій доповіді зроблено, насамперед, на медичній сфері, оскільки людина продовжує жити в умовах, які з кожним роком для неї ускладнюються : це і забруднене оточуюче середовище; це і зростаючі біологічні та харчові обмеження; це і антропогенні зміни тощо, що негативно відображаються на здоров'ї людини та її житті, а також на генофонді людства. А мати належне здоров'я і життя є одним із основоположних прав і свобод людини, про що засвідчує і міжнародне право, і національне право.

З огляду на зазначене, якщо говорити про правову площину цього питання, то воно не є новим. Ще у 1970-1980-х рр. відбулися перші дослідження та заходи, присвячені аспектам ШІ та права. Так, у 1987 р. відбулася перша Міжнародна конференція присвячена штучному інтелекту та праву, яка від тоді стала регулярною і проводиться що два роки. Вже у 1991 р. було створено Міжнародну асоціацію штучного інтелекту та права, а у 1992 Асоціацією розпочалася публікація «Штучний інтелект та право». Європейський Парламент 16 лютого 2017 р. ухвалив Резолюцію 2015/2113(INL) [6] щодо цивільно-правового регулювання робототехніки з рекомендаціями для Європейської Комісії. «Норми цивільного права про робототехніку». В ній наголошено на неможливості притягнення штучного інтелекту до відповідальності за дії, що спричинили шкоду третім сторонам. Відповідальність за завдання шкоди може бути покладено на одного з так званих агентів (анг. human agent), а саме: на виробника, оператора, власника або користувача штучного інтелекту. При цьому під час установлення обсягу відповідальності з боку «агента» одним із головних аспектів визначено факт доведення можливості передбачення негативних наслідків і запобігання їм.

Загальні перспективи реформування правового регулювання щодо використання штучного інтелекту та його відповідальності за діяння можна згуртувати **навколо трьох основних положень**:

- позиціювання роботів із штучним інтелектом лише як об'єкта суспільних відносин. За такого підходу роботи зі штучним інтелектом сприймаються лише як можлива допомога в суспільних відносинах, де суб'єктами є фізичні та юридичні особи;
- позиціювання роботів із штучним інтелектом лише як окремих суб'єктів правовідносин. За такого підходу роботи зі штучним інтелектом сприймаються лише як окремі самостійні суб'єкти суспільних відносин із можливістю відносно самостійно та в достатньому обсязі усвідомлювати й оцінювати значення своїх дій і дій інших осіб;
- позиціювання роботів із штучним інтелектом як окремих суб'єктів правовідносин, так і можливих об'єктів суспільних відносин.

Висновок. *Незважаючи на те, що окремі провідні європейські держави, як і Японія, готові законодавчо визнати автором твору комп'ютерну програму і поставити штучний інтелект на один щабель з людським, на моє глибоке переконання, правове регулювання має ґрунтуватися на першій гіпотезі: робот зі штучним інтелектом – об'єкт суспільних відносин – власність фізичної або юридичної особи, що не є та не може бути окремим самостійним суб'єктом суспільних відносин. ШІ не є членом соціуму априорі, тому не може бути в правах на рівні з членом соціуму. Штучний інтелект потрібно сприймати як джерело підвищеної небезпеки та розглядати з урахуванням усіх специфічних умов відповідальності за завдану шкоду з боку саме джерела підвищеної небезпеки, що і встановлено нинішніми нормами чинного законодавства України.*

Використана література

1. 10 прикладів, як штучний інтелект може змінити ваш спосіб життя. URL: <https://www.radiosvoboda.org/a/29015231.html> (дата звернення: 17.11.2021 р.)

2. New artificial intelligence can tell you the age of your CELLS – paving the way to personalized medical advice that could extend your lifespan. URL: <https://www.dailymail.co.uk/health/article-5272313/New-artificial-intelligence-age-CELLS.html> (дата звернення: 17.11.2021 р.)

3. A first in medical robotics: Autonomous navigation inside the body. URL: <https://www.sciencedaily.com/releases/2019/04/190424153600.htm> (дата звернення: 17.11.2021 р.)

4. Autonomous robotic intracardiac catheter navigation using haptic vision. URL: <https://www.science.org/doi/10.1126/scirobotics.aaw1977> (дата звернення: 17.11.2021 р.)

5. Єврокомісія опублікувала «Білу книгу з штучного інтелекту». URL: <https://yur-gazeta.com/golovna/evrokomisiya-opublikovala-bilu-knigu-z-shtuchnogo-intelektu.html> (дата звернення: 17.11.2021 р.)

6. Норми цивільного права про робототехніку. Резолюція Європарламенту 2015/2113(INL) від 16 лютого 2017 р. URL: <file:///C:/Users/GARRI6~1/AppData/Local/Temp/Resolution%20and%20Charter%20EU.pdf> (дата звернення: 18.11.2021 р.)

Мічурін Є. О.

доктор юридичних наук, професор,
професор кафедри цивільно-
правових дисциплін Харківського
національного університету імені
В. Н. Каразіна

ШТУЧНИЙ ІНТЕЛЕКТ: ПРАВОВІ АСПЕКТИ

О. А. Баранов відзначає, що побудова інформаційного суспільства характеризується, зокрема, широким використанням інформаційних комп'ютерних технологій в усіх сферах життєдіяльності людини, суспільства і держави [1, с. 3]. Штучний інтелект є одним з продуктів розвитку комп'ютерних технологій. З розвитком ІТ-технологій проблема штучного інтелекту постає у суспільстві взагалі та правовій науці зокрема.

Визначення проблемних аспектів правовідносин в ІТ-сфері має як теоретичне, так і практичне значення. Набуває актуальності проблематика стосовно виявлення правової природи діяльності,

пов'язаної зі штучним інтелектом та відповідальності за шкоду, спричинену через його використання.

Нині стрімко розвивається ІТ право. Утім, потрібним є відмежування приватного ІТ права та публічного ІТ права. Поділ права на приватне та публічне є засадничим. Він склався та є незмінним ще з часів Стародавнього Римського права. Так, видатний юрист Стародавнього Риму Ульпіан вбачав відправну точку розмежування права на публічне та приватне у тому чи стосується воно статусу держави або ж інтересів окремих осіб. Поділ права на публічне і приватне залишився й у сучасному Європейському праві, зокрема існує у праві України [2, с. 15].

Штучний інтелект має окремі особливості, що не дозволяють класифікувати його як виключно віртуальне благо з точки зору об'єктів приватного ІТ-права. Адже як правило віртуальні блага є нематеріальними, не мають уречевленої форми, можуть без втрати властивостей швидко змінювати матеріальні носії. Так, веб-сайти, криптовалюта, інші віртуальні об'єкти у вигляді електронного (цифрового) коду можуть бути переведені з одного серверу на інший, перезаписаними з одного на інший електронний носій [3, с. 71].

Штучний інтелект хоч і є породженням ІТ-технологій, утім він може бути розроблений спеціально під функції, які він здатний виконувати через інсталяцію у певний механічний пристрій (робот). Чи слід тоді вважати, що йдеться про два об'єкти: штучний інтелект та його носій: механічний пристрій? Скоріше йдеться про складний об'єкт, якій має подвійну природу. Адже окремі віртуальні блага мають цінність лише у віртуальному просторі, інші мають подвійну правову природу й можуть мати цінність як у віртуальному просторі, так і у вигляді матеріальних речей [3, с. 72].

Штучний інтелект може бути вмонтованим не лише у робота, але й мати вигляд комп'ютерної програми (зокрема, у комп'ютерній штучній нейромережі). Прикладом комп'ютерної штучної нейромережі є запроваджена у США програма штучного інтелекту для прогнозування місць майбутніх злочинів, яка досягає високої ефективності завдяки здатності аналізувати великий обсяг інформації щодо минулих злочинів. У банківській сфері компанія

ZestFinance (США) розробила та запровадила платформу ZAML, яка збирає й аналізує різні відомості про клієнта фінансової організації, у тому числі вивчає його дії в Інтернеті. На основі отриманих даних алгоритми визначають, наскільки людина заслуговує на довіру банку. Шведська компанія BehavioSec розробила AI систему, яка визначає особистість людини за швидкістю й темпом набору тексту на клавіатурі, за силою натискання на клавіші й іншими показниками. Завдяки такому біометричному аналізу банк може виявити шахрая, який намагається видати себе за іншу людину [4, с.65]. Вже розроблені автомобілі, які не потребують керування людиною, повітряні дрони, що самостійно доставляють товари покупцям інтернет-магазинів [5, с.88]. Такі самокеровані транспортні засоби є оснащеними штучним інтелектом, оскільки здатні підлаштовуватися під окремі ситуації на основі певних алгоритмів.

У науці точаться дискусії щодо віднесення штучного інтелекту до об'єкту чи суб'єкту права. Схиляємося до першого з таких підстав. Вважаємо, що доречною є аналогія штучного інтелекту з твариною. Остання, як відомо, є об'єктом права. Тварина, як і штучний інтелект здатна діяти без безпосереднього вольового впливу людини. Свійська тварина може враховувати волевиявлення людини через дресирування (аналогія – налаштування штучного інтелекту). Утім, тварина є об'єктом права, хоча й наділена природою своєрідним інтелектом, здатна до мислення, навчання, спілкування. Отже, більш коректним є умовне порівняння (аналогія) штучного інтелекту із твариною – об'єктом права, ніж із людиною (суб'єктом права). Відтак, штучний інтелект є об'єктом права й застосування до нього теорії суб'єкта чи квазісуб'єкта права є ані доречним, ані обґрунтованим. Додаткові аргументи на користь позиції про те, що штучний інтелект є об'єктом права вже були наведені раніше [6].

На користь аналогії штучного інтелекту з твариною вказує також історичний досвід розвитку людства. Приручення свого часу тварин зі стану природньої волі й перетворення їх на свійських було продиктовано бажанням людини розвантажити людину на

важких, небезпечних чи рутинних роботах. Тому з'явився такий об'єкт права як тварина. Схожі намагання людства: розвантажити людину на важких, небезпечних чи рутинних роботах на сучасному етапі розвитку технологій призвели до створення штучного інтелекту (роботів і відповідних комп'ютерних програм).

Відтак, штучним інтелектом є об'єкт права у вигляді пристрою або комп'ютерної програми, налаштований на здобуття, обробку та застосування інформації, здатний набувати вміння подібні до тих, що свідомо здійснює людина.

Окрему проблему складає деліктна відповідальність зі спричинення шкоди діяльністю, пов'язаною із штучним інтелектом.

Власник штучного інтелекту зобов'язаний відповідати за шкоду, спричинену джерелом підвищеної небезпеки, якщо його дії порушують рекомендації виробника штучного інтелекту (порушення інструкції). Адже згідно до законодавства про захист прав споживачів якщо для безпечного використання продукції, її зберігання, транспортування та утилізації необхідно додержуватися спеціальних правил, виробник (виконавець) зобов'язаний розробити такі правила та довести їх до продавця або споживача, а продавець – до споживача, якщо відповідними нормативно-правовими актами, у тому числі технічними регламентами, не встановлено інші способи інформування споживачів про певні види ризику чи продукції.

Діяльність з використанням штучного інтелекту є такою, щодо якої нормативно-правовими актами, технічними регламентами мають бути встановлені вимоги стосовно безпеки для життя, здоров'я та майна споживачів і навколишнього природного середовища. Відповідна продукція повинна вводитися в обіг та реалізовуватися з додержанням зазначених вимог. Якщо до спричинення шкоди призвів дефект (налаштування) штучного інтелекту з вини виробника, або він не попередив у інструкції з використання штучного інтелекту про потенційні його шкоданесучі властивості (що призвело до спричинення шкоди), відповідати має, зокрема, виробник за нормами про відповідальність за шкоду, завдану внаслідок дефекту товару (дефекту у продукції). Якщо шкода була нанесена виробом із штучним інтелектом, який був придбаний спо-

живачем мають застосовуватися норми законодавства про захист прав споживачів. Адже за законодавством споживач має право на те, щоб продукція за звичайних умов її використання, зберігання і транспортування була безпечною для його життя, здоров'я, навколишнього природного середовища, а також не завдавала шкоди його майну.

Використані джерела

1. Баранов О. А. Теоретико-методологічні основи правового забезпечення інформаційної сфери України. Автореферат дис... докт. юрид. наук. 12.00.07. Х.: Національний юридичний університет імені Ярослава Мудрого. 2015. – 43 с.
2. Мічурін Є. О. Приватне ІТ-право: навчальний посібник. Х: Право, 2021. – 176 с.
3. Мічурін Є. О. (2021). Віртуальні блага: особливості та ознаки. *Форум Права*, 68 (3), 67–73. <http://doi.org/10.5281/zenodo.5075696>
4. Мічурін І. Є. Застосування систем штучного інтелекту у банківських системах. *Актуальні проблеми розвитку бізнес-технологій в сучасних умовах глобалізаційних процесів: тези доповідей Всеукр. наук.-практ. конф. молодих вчених та учнівської молоді*. Х.: Національний аерокосмічний університет «Харківський авіаційний інститут», 2020. С. 65.
5. Колодін Д. О., Батайлюк Д. Р. Щодо питання цивільно-правової відповідальності за шкоду, завдану роботизованими механізмами зі штучним інтелектом (роботами). *Часопис цивілістики*. 2018. Вип. 33. С. 87–91.
6. Мічурін Є. О. (2020). Правова природа штучного інтелекту. *Форум Права*, 64 (5), 67–75. <http://doi.org/10.5281/zenodo.4300624>

Гутюк І. В.

Студентка НТУУ «КПІ ім. Ігоря
Сікорського»

Науковий керівник: Дубняк М. В.

кандидат юридичних наук, старший
викладач, НТУУ «КПІ імені Ігоря
Сікорського»

ПРАВОВЕ РЕГУЛЮВАННЯ ЕЛЕКТРОННОЇ ДЕМОКРАТІЇ В УКРАЇНІ

Століття, у якому ми живемо характеризується стрімким розвитком інформаційно-комунікативних технологій (далі ІКТ), які проникають у різноманітні сфери нашої діяльності, у тому числі в державне управління. Запровадження та розвиток електронної демократії створює передумови для діалогу громадян з державною владою з використанням ІКТ та реалізації прямої демократії з метою поліпшення суспільно-політичного життя.

Поставимо собі завдання окреслити поняття електронної демократії, проаналізувати національне законодавство, визначити інструментарій впровадження електронної демократії в Україні та правове регулювання е-демократії.

Поняття „електронна демократія” (electronic democracy) вперше з’явилося в США і досить швидко стало загальновживаним у багатьох країнах світу. В широкому сенсі це означає можливість залучення громадян до активнішої участі у справах суспільства завдяки використанню комп’ютерних приладів та мереж телекомунікацій. У вузькому сенсі термін означає використання громадянами інформаційних, а також телекомунікаційних технологій для участі в конституційно передбачених діях щодо управління справами держави та місцевих спільнотах [1, с. 68].

На нашу думку, такий підхід надає найбільш цілісне уявлення про те, що являє собою е-демократія та застосування ІКТ в цьому процесі.

Аналізуючи у своїй статті роботи В. Дрожжинова й А. Штрика, А. Сіленко, думку британського дослідника Стівена Кліфта

та «Концепція розвитку електронного урядування в Україні», науковець Мезенцев формулює своє поняття е-демократії: електронна демократія – форма організації суспільства, де за рахунок широкого застосування інформаційно-комунікаційних громадяни, громадські організації, представники бізнесу залучаються до прийняття державних рішень і участі в державному управлінні [2, с. 68].

Основним нормативно-правовим актом у сфері е-демократії можна вважати “Концепцію розвитку електронного урядування в Україні”, яка визначає основні засади формування й діяльності е-урядування.

Рекомендації Комітету міністрів Ради Європи [3] надають низку проблем, у зв’язку з якими доцільність запровадження е-демократії збільшується. Зокрема до таких проблем належить те, що сьогодні досить часто рівень довіри громадян до їхніх виборних установ йде на спад, тобто громадяни відчують недостатню прозорість інформації, яку вони отримують; низькі показники явки під час виборів, зниження зацікавленості молоді щодо політики.

Тому органи державної влади ухвалюють різноманітні нормативно-правові акти, пов’язані з е-демократією, за реалізацію деяких із них відповідає Міністерство цифрової трансформації України. Мінцифри є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики: у сферах електронного урядування та електронної демократії [4].

Важливим нормативним актами для запровадження е-демократії в Україні є Концепція розвитку електронної демократії в Україні та план заходів щодо її реалізації. Так, згідно з Планом пріоритетними заходами для запровадження е-демократії в Україні є: удосконалення механізму подання та розгляду електронних петицій; створення нормативно-правових засад для забезпечення належного функціонування електронних інформаційних ресурсів органів державної влади; розроблення нормативно-правових актів для забезпечення електронного голосування; забезпечення розвитку відкритих даних; сприяння підзвітності громадянину

суб'єктів владних повноважень; удосконалення механізму висвітлення інформації про діяльність органів державної влади [5].

Щодо реалізації вказаних у Плані заходів, вважаємо, що одним із найбільш вдалих кроків було запровадження таких інструментів електронної демократії в Україні, як: електронні петиції, електронні консультації, електронні звернення, бюджети участі (громадські бюджети). Варто зазначити, що кожен з цих інструментів застосовується як на місцевому, так і загальнодержавному рівнях.

Правовий механізм реалізації електронних петицій відображений у таких нормативно-правових актах, як: Указ Президента України «Про Порядок розгляду електронної петиції, адресованої Президентові України» ; постанова Кабінету Міністрів України «Про затвердження Порядку розгляду електронної петиції, адресованої Кабінету Міністрів України». Електронна петиція, адресована Президенту України чи Кабінету Міністрів України, розглядається, якщо за три місяці було зібрано не менш як 25000 підписів громадян. Розпорядження Голови Верховної Ради України, яке регулювало питання роботи з петиціями, адресованих Верховній Раді України, визнано таким, що втратило чинність від 08.02.2021. Наразі робота з петиціями, адресованих парламенту регулюється розпорядженням Голови Верховної Ради України «Про деякі питання забезпечення документообігу у Верховній Раді України в електронній та паперовій формах».

Реалізація електронних консультацій забезпечується постановою Кабінету Міністрів України «Порядок проведення консультацій із громадськістю з питань формування та реалізації державної політики». Проведення консультацій з громадськістю має сприяти налагодженню системного діалогу органів виконавчої влади з громадськістю, підвищенню якості підготовки рішень з важливих питань державного і суспільного життя з урахуванням громадської думки [6].

Правовий механізм реалізації електронних звернень забезпечується низкою законів та підзаконних актів. Деякі з них: «Про внесення змін до Закону України «Про звернення громадян» щодо електронного звернення та електронної петиції», Указ Президента

України «Про першочергові заходи щодо забезпечення реалізації та гарантування конституційного права на звернення до органів державної влади та органів місцевого самоврядування» з метою забезпечення реалізації та гарантування закріплених Конституцією України права на звернення до органів Державної влади та органів місцевого самоврядування, права громадян на участь в управлінні державними справами, а також підвищення ефективності роботи органів державної влади та органів місцевого самоврядування зі зверненнями громадян [7].

Щодо громадського бюджету, то це механізм розвитку місцевої демократії щодо зміни міста на краще шляхом розвитку взаємодії між міськими радами та їх виконавчими органами з громадськістю, спрямований на залучення учасників громадського бюджету міста до участі у бюджетному процесі, формування команд громадських проєктів, подання командами громадських проєктів, проведення голосування за проєкти, здійснення контролю за їх реалізацією [8].

За результатами нашого дослідження, можна зазначити наступне: електронна демократія передбачає можливість залучення громадян до більш активної участі в державному управлінні; для регулювання е-демократії в Україні створена нормативно-правова база, яка регулює інструменти електронної демократії на загальнодержавному та місцевому рівні.

Список використаної літератури:

1. Саркісова К. Електронна демократія як форма політичної комунікації в Сучасному суспільстві. *Політичний менеджмент*, №1, 2007 С. 66- 74. URL:<http://www.politik.org.ua/vid/magcontent.php3?m=1532>. (Дата звернення 27.11.2021).

2. Мезєнцев, А. В. (2015). Електронне урядування, електронна демократія—підходи до визначень. *Теорія та практика державного управління*, (1), 64-69. URL:https://scholar.google.com.ua/scholar?hl=uk&as_sdt=0%2C5&q=%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0+%D0%B4%D0%B5%D0%BC%D0%BE%D0%BA%D1%80%D0%B0%D1%82%D1%96%D1%8F&oq=#d=gs_qabs&u=%23p%3D_EZ8CClyyg0J

3. CM/Rec (2009)1 of the Committee of Ministers to member states on electronic democracy (e-democracy). URL: <https://wcd.coe.int/ViewDoc.jsp?id=1410627>

4. Постанова Кабінету Міністрів України «Питання Міністерства цифрової трансформації України» від 18.09.2019. URL: <https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text>

5. Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації» від 08.11.2017. URL: <https://zakon.rada.gov.ua/laws/show/797-2017-%D1%80#Text>

6. Кабінету Міністрів України «Порядок проведення консультацій із громадськістю з питань формування та реалізації державної політики» від 07.05.2019. URL: <https://zakon.rada.gov.ua/laws/show/996-2010-%D0%BF#Text>

7. Указ Президента України «Про першочергові заходи щодо забезпечення реалізації та гарантування конституційного права на звернення до органів державної влади та органів місцевого самоврядування» від 07.02.2008. URL: <https://zakon.rada.gov.ua/laws/show/109/2008#Text>

8. Положення про громадський бюджет міста Києва у редакції рішення Київської міської ради від 06.02.2020 N 4/8174. URL: <https://kmr.gov.ua/uk/provisions-public-budget>

Нагнибіда В. І.

доктор юридичних наук, доцент,
завідувач лабораторії Науково-
дослідного інституту приватного
права і підприємництва імені
академіка Ф. Г. Бурчака НАПрН
України

НОРМАТИВНО-ПРАВОВЕ РЕГУЛЮВАННЯ ВІДНОСИН З ЦИФРОВИМИ АКТИВАМИ ТА ПЕРСПЕКТИВИ ЙОГО УДОСКОНАЛЕННЯ

В останні роки в українському правовому полі відзначається стрімке зростання інтересу до проблематики нормативної регламентації цифрових прав, особливостей здійснення цивільних

прав у мережі Інтернет, встановлення, реалізації та захисту прав на цифрові (віртуальні) активи та споріднених із ними інститутів і категорій. Пов'язані з цим причини носять соціально-економічний характер, впливаючи з об'єктивної картини сучасного світу, який вже неможливо уявити без надбань цифрової епохи, та відображають досягнення певного етапу цифровізації українського суспільства, коли потреба у належному і адекватному відповідним відносинам правовому регулюванні давно назріла. При цьому новації у напрямі впровадження новітніх інструментів цифрової економіки надходять не лише з боку громадянського суспільства і корпорацій, але й держави: у Нацбанку нещодавно анонсували місцеву цифрову валюту (*CBDC – Central Bank Digital Currency*), підкріплену національною у валютою у співвідношенні 1:1 (тобто одна е-гривня дорівнює одній гривні і є її цифровим аналогом), яку планують ввести в експлуатацію наприкінці 2022 року [1].

Чинне вітчизняне законодавство лише фрагментарно торкається питань цифрових прав у межах спеціальних законодавчих актів, присвячених іншим питанням, у той час як закон, предметом якого є регулювання особливостей набуття, здійснення і захисту прав на цифрові активи та загалом створення ринку обігу цифрових активів (Закон «Про віртуальні активи» (законопроект № 3637), ухвалений Верховною Радою України 8 вересня 2021 року [2]) 7 жовтня цього року було повернуто до парламенту з пропозиціями Президента України і його подальше доопрацювання поки здійснюється у залах Верховної Ради.

Якщо не вдаватись до розширювального тлумачення положень Конституції України [3] стосовно поширення її певних приписів і на цифрове середовище (зокрема ч. 2 ст. 34 Основного Закону, згідно з якою кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір, щодо чого у наукових джерелах додається про можливість такого поширення і за допомогою цифрових технологій [4, с. 107]) та інших засадничих приписів і принципів, утілених в нормах українського законодавства (зокрема, у Законах України «Про доступ до публічної інформації» [5], «Про

електронні довірчі послуги» [6], «Про електронні документи та електронний документообіг» [7], «Про телекомунікації» [8], «Про інформацію» [9] та у деяких інших), то питання, присвячені регулювання цифрових прав і, тим більше, цифрових активів, сутнісно не врегульовані у чинному українському законодавстві.

До прикладу, з огляду на визначення, закріплене у абз. 8 ч. 1 ст. 2 Закону України «Про захист персональних даних» [10], поняття обробки персональних даних (це будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, **у тому числі з використанням інформаційних (автоматизованих) систем – виділення наше**), можливо стверджувати й про поширення його дії положень цього Закону на захист персональних даних за допомогою сучасних цифрових інструментів та мережі Інтернет.

При цьому навіть зазначені законодавчі акти не торкаються проблематики регулювання цифрових прав і цифрових активів із точки зору цивілістики і загалом приватно-правових інститутів, визначаючи здебільшого публічні аспекти поширення і збереження інформації в електронному вигляді, захисту персональних даних, функціонування сучасних телекомунікаційних мереж тощо. З огляду на це вбачається, що на системному рівні щодо унормування цивільно-правових питань набуття і здійснення цифрових прав, а також як публічних, так і приватних складових регулювання ринку обігу цифрових активів, існує потреба у одночасному доповненні вже наявних нормативно-правових актів (зокрема Цивільного кодексу України [11] щодо особливостей реалізації цивільних прав у цифровому середовищі) та у розробці нових спеціальних законів та, на основі них та де це буде потрібно, відповідних підзаконних актів.

Щодо регламентації власне відносин, пов'язаних із обігом цифрових активів, здійсненням і захистом прав на них, поділяємо позицію українського законодавця стосовно необхідності приділення уваги цим питанням на рівні окремого закону. У світлі цього

заслуговує ретельного аналізу згаданий Закон України «Про віртуальні активи», стосовно якого направлені пропозиції Президента України. Раніше ми вже висловлювали низку ключових позицій, на які варто звернути увагу при опрацюванні пропозицій до вдосконалення положень цього Закону, зокрема у світлі врахування відображення у терміні «віртуальний актив» не лише економіко-правової, але й технічної сутності, диференціації на забезпечені та незабезпечені, встановлення вартості останніх, специфіки ліцензування діяльності з віртуальними активами, сфери застосування Закону та ін.

Серед основних зауважень до Закону «Про віртуальні активи», висвітлених у пропозиціях Президента України на обґрунтування неможливості його прийняття у нинішньому вигляді є те, що Законом пропонується здійснювати державне регулювання ринку віртуальних активів різними державними органами залежно від виду віртуальних активів, у тому числі шляхом створення нового центрального органу виконавчої влади. Водночас, як наголошується у пропозиціях Президента України, світовий досвід свідчить про те, що регулювання діяльності з організації торгівлі, обміну та зберігання віртуальних активів, які призначені для інвестування, збереження вартості, використання у платіжних або інвестиційних цілях, здійснюється регуляторами фінансових ринків. У зв'язку з цим пропонується регулювання діяльності із залучення коштів та здійснення інвестицій, зокрема питань, пов'язаних із регулюванням діяльності учасників ринку віртуальних активів та емісії віртуальних активів, мають бути віднесені до компетенції вже функціонуючих в Україні фінансових регуляторів, а саме: Національної комісії з цінних паперів та фондового ринку та Національного банку України. Вважаємо, що з такою позицією варто погодитись.

Крім цього, ухвалений парламентом Закон України «Про віртуальні активи» повинен бути доопрацьований і з огляду на таке. По-перше, удосконалення потребує пропоноване вказаним Законом регулювання способів посвідчення факту забезпеченості віртуальних активів майнових прав, зокрема права вимоги на інших об'єк-

тів цивільних прав. Варто передбачити механізм такого посвідчення та основні способи закріплення правового зв'язку між змістом цифрового активу та вказаними майновими правами. По-друге, у ч. 5 ст. 4 Закону пропонується закріпити, що об'єкт забезпечення віртуального активу визначається правочином, згідно з яким такий віртуальний актив створено. Майнові права, зокрема права вимоги, на об'єкт забезпечення віртуального активу передаються набувачу такого віртуального активу. Слід розглянути потребу у закріпленні на рівні ЦК України особливих вимог до змісту, істотних умов та форми такого правочину, порядку його укладення, обміну сторонами офертою та акцептом тощо. По-третє, Закон врегульовує юридичні наслідки розпорядження забезпеченими віртуальними активами, проте досить фрагментарно торкається специфіки обігу незабезпечених віртуальних активів. Враховуючи правову природу останніх у цій сфері дійсно варто уникати зарегулювання, проте доцільно, на нашу думку, закріпити деякі основні принципи встановлення прав і розпорядження ними на незабезпечені цифрові активи.

Список використаних джерел

1. До 2022 року в Україні можуть ввести цифрову валюту. Що це таке і в чому небезпека? URL: <https://zaborona.com/do-2022-roku-v-ukrayini-mozhut-vvesty-cyfrovu-valyutu-shho-cze-take-i-v-chomu-nebezpeka/>
2. Пропозиції Президента до Закону «Про віртуальні активи» (проект Закону України від 11.06.2020 р. № 3637). *Верховна Рада України. Законотворчість*. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69110
3. Конституція України від 28.06.1996 р. *Відомості Верховної Ради України*. 1996. № 30. С. 141.
4. Коваленко А. А. Цифровые права: понятие и правовое регулирование в украинском законодательстве. 2021. С. 105–108. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/10982/Tsyfrovi%20prava%20Poniattia%20y%20pravove%20rehuliuvannia%20v%20Ukrainskomu%20zakonodavstvi_Kovalenko_2021.pdf?sequence=1&isAllowed=y
5. Про доступ до публічної інформації: Закон України від 13.01.2011 р. № 2939-VI. *Відомості Верховної Ради України*. 2011. № 32. Ст. 314.

6. Про електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 400.

7. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 р. № 851-IV. *Відомості Верховної Ради України*. 2003. № 36. Ст. 275.

8. Про телекомунікації: Закон України від 18.11.2003 р. № 1280-IV. *Відомості Верховної Ради України*. 2004. № 12. Ст. 155.

9. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.

10. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481.

11. Цивільний кодекс України від 16.01.2003 р. № 435-XII. *Офіційний вісник України*. 2003. № 11. Ст. 461.

Андрощук Г. О.

кандидат економічних наук, доцент,
головний науковий співробітник НДІ
інтелектуальної власності НАПрН
України

ЦИФРОВА ТРАНСФОРМАЦІЯ В КРАЇНАХ ЄС НА 2021 РІК

Індекс цифрової економіки та суспільства. Європейська Комісія (ЄК) 12 листопада 2021 р. опублікувала результати Індексу цифрової економіки та суспільства (The Digital Economy and Society Index (DESI)) на 2021 рік, який з 2014 року відстежує прогрес, досягнутий у державах-членах ЄС у галузі цифрової конкурентоспроможності та в галузях людського капіталу, зв'язку, інтеграції цифрових технологій підприємствами та цифрових технологій, громадські послуги [1]. Щороку DESI включає профіль країн, які підтримують країни-члени у визначенні сфер, що потребують пріоритетних дій, а також тематичні розділи, які пропонують європейсько-рівневий аналіз у ключових цифрових сферах, необхідний для підтримки політичних рішень [2]. У звітах DESI 2021 представлені дані за перший або другий квартал 2020 р., що дає уявлення про ключові події у цифровій економіці та суспільстві.

стві протягом першого року пандемії. Проте вплив COVID-19 на використання та надання цифрових послуг та результати політики, реалізованої з тих пір, не відображаються у даних та будуть більш помітними у виданні 2022 року. Усі держави-члени досягли прогресу в галузі цифровізації, але загальна картина країн-членів неоднозначна. Попри деяку конвергенцію, розрив між лідерами ЄС і країнами з найнижчими оцінками DESI залишається великим. Незважаючи на ці покращення, усім державам-членам необхідно докласти узгоджених зусиль для досягнення цілей на 2030 рік, встановлених у Європейському десятилітті цифрових технологій (Europe's Digital Decade: digital targets for 2030) [3]. .

Виконавчий віце-президент за програмою «Європа, придатна для цифрової епохи» Маргрет Вестагер заявила: «Індекс цього року позитивний, всі країни ЄС досягли певних успіхів у забезпеченні більш цифрових технологій та підвищення конкурентоспроможності, але можна зробити ще більше. Тому ми працюємо з державами-членами, щоб гарантувати, що ключові інвестиції будуть зроблені через Фонд відновлення та стійкості, щоб надати найкращі із цифрових можливостей усім громадянам та підприємствам».

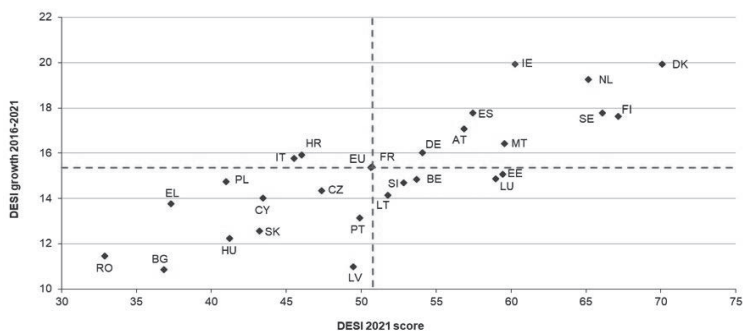
Комісар з внутрішнього ринку Тьеррі Бретон додав: «Постановка цілей на період до 2030 року була важливим кроком, але тепер ми маємо виконати їх. Сьогоднішній DESI демонструє прогрес, але також і в тому випадку, коли нам необхідно колективно стати кращими, щоб європейські громадяни та підприємства, зокрема малі та середні підприємства, могли отримати доступ та використовувати передові технології, які зроблять їхнє життя кращим, безпечнішим та екологічнішим» [1].

DESI 2021 був адаптований для відображення Компасу цифрового десятиліття, в якому викладаються амбіції Європи щодо цифрових технологій, викладаються бачення цифрової трансформації та конкретні цілі на 2030 рік за чотирма основними напрямками: *навички, інфраструктура, цифрова трансформація бізнесу та державних послуг*. Програма політики «Шлях до цифрового десятиліття», запропонована 15 вересня 2021 року, встановлює

нову форму управління з державами-членами через механізм щорічної співпраці між інститутами ЄС та державами-членами для забезпечення їхнього спільного досягнення цілей. При цьому моніторинг цільових показників Digital Decade буде покладено на DESI. В результаті індикатори DESI тепер структуровані довкола 4 основних точок Digital Decade Compass. Звіти DESI за країнами включають короткий огляд цифрових інвестицій та реформ у планах відновлення та стійкості 22 планів, які вже схвалено Комісією. Держави-члени зобов'язалися витратити не менше 20% своїх національних ресурсів з Плану відновлення та стійкості на цифрові технології, і поки що держави-члени досягають або значно перевищують цю мету.

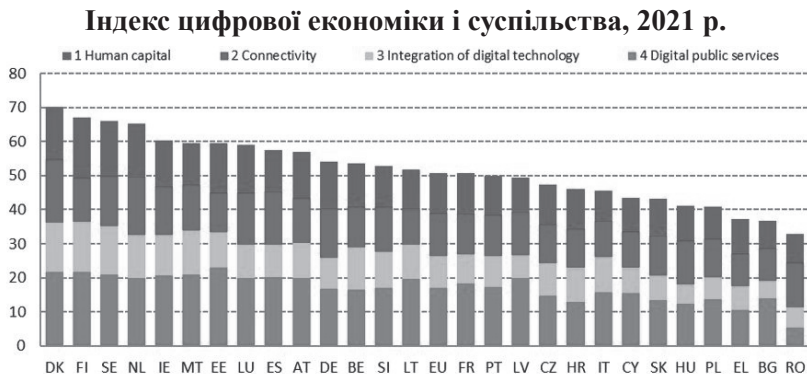
Показники країн-членів ЄС у галузі цифрових технологій за даними DESI 2021. Найбільший прогрес порівняно з минулим роком спостерігається в Ірландії та Данії, за якими йдуть Нідерланди, Іспанія, Швеція та Фінляндія. Результати цих країн також значно перевищують середні показники DESI у ЄС, виходячи з їх оцінок у DESI 2021. Нижче наведено показники Індексу цифрові економіки і суспільства – прогрес держав-членів, 2016-2021 рр. та Індекс цифрової економіки і суспільства, 2021 р.

Індекс цифрові економіки і суспільства – прогрес держав-членів, 2016-2021 рр.



Джерело: DESI 2021, Європейська комісія.

В цілому, Данія, Фінляндія, Швеція і Нідерланди мають найбільш розвинену цифрову економіку в ЄС, за ними слідують Ірландія, Мальта і Естонія. Румунія, Болгарія і Греція мають найнижчі оцінки DESI.



Джерело: DESI 2021, Європейська комісія.

Згідно дослідження можна сформулювати основні висновки DESI 2021 за 4 напрямками [1] : **Людський капітал**. В рамках зобов'язань, сформульованих у Цифровому компасі ЄС на період до 2030 р., цільовий показник цифрових навичок націлений на те, щоб до 2030 року базові цифрові навички мали не менше 80% громадян ЄС. Тоді як у 2019 р. Інтернетом регулярно користувалися лише 56%. Значна частина населення ЄС не має цифрових навичок, але є відмінності в конкретних країнах: Нідерланди та Фінляндія лідирують у цій сфері, а Болгарія та Румунія відстають. Більше того, 56% населення, яке має цифрові навички, – це лише незначне збільшення (2%) з 2015 р., що відповідає щорічному приросту всього на 0,9%. Ці темпи зростання необхідно втричі збільшити, щоб досягти мети 2030 р. на 80%. Згідно з повідомленням про цифровий компас 2030 р., кількість фахівців у галузі ІКТ у ЄС має досягти не менше 20 млн до 2030 р. порівняно з 8,4 млн у 2020 р. (що відповідає 4,3% робочої сили). Хоча з 2013 р. спостерігається стійке зростання, для досягнення

мети потрібне прискорення. Помітними лідерами у цій категорії є Фінляндія з 7,6% та Швеція з 7,5% робочої сили, відповідно, які мають найвищу частку фахівців у галузі ІКТ у робочій силі. ЄК 12.11.21 також опублікувала дані про жінок на цифровому табло (Women in Digital Scoreboard 2021), яке підтверджує, що все ще існує значний гендерний розрив у спеціалізованих цифрових навичках [4]. Жінки становлять лише 19% фахівців у галузі ІКТ та близько третини випускників факультетів природничих наук, технологій, інженерії та математики. Прогресу немає, оскільки останні кілька років ці показники є стабільними. Цифровий компас поставив за мету, щоб до 2030 року в ЄС було 20 мільйонів найнятих фахівців у галузі ІКТ, з урахуванням зближення жінок та чоловіків. Значно менший розрив для використання Інтернету та навичок користувачів Інтернету. 85% жінок регулярно користувалися Інтернетом у 2020 році порівняно з 87% чоловіків. Різницю в 4% можна спостерігати в показниках цифрових навичок: 54% жінок мають принаймні базові цифрові навички (58% чоловіків), 29% вище базових цифрових навичок (33% чоловіків) і 56% принаймні базові навички програмного забезпечення (60% чоловіків) станом на 2019 рік. Жінки найбільш цифрові у Фінляндії, Швеції, Данії, Естонії та Нідерландах. Усі ці країни також дуже добре працюють у DESI. Жінки в Румунії, Болгарії, Польщі, Угорщині та Італії мають найнижчі результати щодо участі жінок у цифровій економіці та суспільстві.

Зв'язок. Цифровий компас 2030 також встановлює мету, що гігабітні мережі повинні бути доступні для всіх до 2030 року. За даними 2020 р., тільки 59% сімей можуть отримати вигоду зі стаціонарної мережі дуже високої пропускної здатності (VHCN). Сільські VHCN також покращилися – з 22% у 2019 р. до 28% у 2020 році. Водночас залишається великий розрив між сільськими та національними показниками. Мальта, Люксембург, Данія та Іспанія є європейськими лідерами із загального охоплення VHCN (понад 90% будинків). Проте, у Греції менше 1 з 5 домогосподарств мають доступ до VHCN. До 2030 р. ЄС прагне забезпечити покриття 5G у всіх населених пунктах. Станом на середину

2020 р. розгортання комерційних мереж 5G розпочалося у 13 державах-членах, а покриття досягло 14% на рівні ЄС. Нідерланди та Данія є найбільш просунутими країнами в цій галузі з 80% охопленням. Попередньою умовою для комерційного запуску 5G є виділення спектру 5G у кожній країні, і до 31 серпня 2021 року 25 держав-членів уже виділили спектр 5G як мінімум в одній із трьох перших смуг 5G.

Інтеграція цифрових технологій. Ціль Цифрового компасу ЄС полягає в тому, щоб до 2030 р. не менше 90% малих та середніх підприємств (МСП) у ЄС використовували цифрові технології на рівні підприємств. У 2020 р. лише 60% МСП запровадили цифрові технології. Данія та Фінляндія вже дуже близькі до цільового показника ЄС (88%), а Болгарія та Румунія відстають (33%). Друга мета на наступні десять років: до 2030 року щонайменше 75% компаній повинні використовувати передові цифрові технології, такі як штучний інтелект (ШІ), хмарні технології та технології великих даних. DESI 2021 демонструє це, хоча підприємства стають все більш цифровими, використання передових цифрових технологій залишається низьким; наприклад, лише одна з чотирьох компаній використовує ШІ чи хмарні обчислення, а 14% використовують великі дані. У цій галузі лідирують за використанням хмарних технологій Фінляндія та Швеція, А Мальта та Нідерланди – за великими даними, Чехія та Австрія – за ШІ. **Цифрові державні послуги.** Цифровий компас встановлює мету, що всі ключові державні послуги для громадян і бізнесу повинні бути повністю онлайн, 2030. Такі основні послуги охоплюють широкий діапазон від вивчення до, покупки автомобіля та для початку бізнесу, серед інших речей. DESI стежить за наданням державних послуг у режимі онлайн, виставляючи кожній державі-члену оцінку того, чи можливо повністю виконати кожен етап надання ключових послуг у режимі онлайн. Найвищі оцінки цифрових державних послуг у DESI мають Естонія, Данія, Фінляндія та Мальта, а найнижчі – Румунія та Греція. У 2020 р. 64% інтернет-користувачів взаємодіяли з державним управлінням у режимі онлайн порівняно з 58% у 2015 році. За останнє десятиліття доступність державних послуг

в Інтернеті неухильно зростала та значно прискорилося внаслідок пандемії COVID-19, під час якої цифрова взаємодія стала переважаючою. Ряд держав-членів вже близькі до цієї мети, але прогрес йде нерівномірно в державах-членах і всередині них, при цьому послуги для громадян з меншою ймовірністю будуть доступні в Інтернеті, порівняно з послугами для підприємств.

Висновки. Щорічний Індекс цифрової економіки та суспільства DESI вимірює прогрес держав-членів ЄС у напрямку цифрової економіки та суспільства на основі даних Євростату та спеціалізованих досліджень і методів збору. Він допомагає державам-членам визначити пріоритетні галузі, які потребують цільових інвестицій та дій. DESI також є ключовим інструментом для аналізу цифрових аспектів у європейському семестрі. З бюджетом у 723,8 млрд євро Фонд відновлення та підвищення стійкості (RRF), ухвалений у лютому 2021 року, є найбільшою програмою в рамках наступного покоління ЄС. Пандемія значною мірою сприяла розвитку цифрових навичок. Перехід до дистанційного навчання збільшив потребу у додатковому обладнанні та зажадав створення чи модернізації цифрових платформ, а також навчання. Аналіз показує, що нестача працівників із просунутими цифровими навичками відчувається у всьому ЄС – до 55% минулого року. Компанії ЄС мають труднощі із набором персоналу. У 2020 р. у галузі ІКТ в ЄС було зайнято 8,4 млн фахівців. ЄС прагне до 2030 р. збільшити кількість професіоналів у галузі цифрових технологій до 20 млн. Для досягнення цифрових цілей та завдань ЄК прискорюватиме запуск багатокраїнних, великомасштабних проєктів, які жодна держава-член ЄС не може розробити поодиночі. Ці проєкти спрямовані: об'єднати інвестиції з бюджету ЄС, у т.ч. з Фонду відновлення та стійкості, від держав-членів та приватного сектору; усунути прогалини у виявлених критичних можливостях ЄС; підтримувати взаємопов'язаний, функціонально сумісний та безпечний єдиний цифровий ринок. Комісія визначила первісний список багатокраїнних проєктів. Він включає такі області для інвестицій, як: інфраструктура даних, малопотужні процесори, зв'язок 5G, високопродуктивні обчислення, безпечний квантовий зв'язок,

державне управління, блокчейн, центри цифрових інновацій та цифрові навички. ЄС може розгорнути мережу операційних центрів безпеки, що працюють на базі ШІ, для прогнозування, виявлення та реагування на кібератаки на національному рівні та рівні ЄС. Європейський консорціум цифрової інфраструктури – це новий інструмент, який допоможе зацікавленим державам-членам прискорити та спростити реалізацію багатокраїнових проєктів.

Цифрова трансформація призвела до багатьох змін у виробництві, способі життя та управлінні, вона має довгостроковий вплив на світовий економічний, політичний та науково-технічний прогрес. Україна має вигідне географічне положення, якісні освітні та наукові ресурси, розвинуту сферу ІТ та сприятливі умови для розвитку цифрової економіки. Вона першою запровадила систему електронних паспортів, запустила Цифрограм для держслужбовців, реалізує проєкт eSignature – систему електронного обміну документами (електронні підписи) між компаніями з України та ЄС, планує запустити 100 офлайн-пунктів підтримки «Дії» у 20 областях України і здобула першість у багатьох напрямках цифрових технологій серед країн Європи. Водночас, згідно експертного дослідження поточного стану розгортання цифрової трансформації на приватному та державному рівнях – Індекс цифрової трансформації, вперше проведеного в цьому році. Європейською Бізнес Асоціацією, основними бар'єрами розвитку цифрової трансформації в бізнесі є: зарегульованість та неефективне законодавство – 45%, недостатнє фінансування-31%, відсутність цифрової грамотності-31%, застаріла ІТ- інфраструктура-28%, проблеми з кібербезпекою та конфіденційністю -25% [5]. Цифрова трансформація України має прискоритись. Відповідний законопроект 28.10.21 схвалив Кабінет Міністрів України. Законопроект містить зміни до Закону України «Про Національну програму інформатизації» який не змінювався з 1998 року. Проєкт закону містить положення щодо: подолання цифрової нерівності; безпеки інформаційної діяльності та кіберзахисту; інтеграції України в світовий цифровий простір; застосування новітніх технологій в державному управлінні. Прийняття законопроекту

має прискорити вирішення питань координації, моніторингу, оцінки результатів та ефективності виконання проєктів із цифровізації та електронного урядування. Цифровізація української економіки та суспільства є одним з важливих складників не лише обраного Україною вектору європейської інтеграції, а й розвитку країни загалом. Наближення законодавства і стандартів України до законодавства і стандартів ЄС зменшить регуляторні розбіжності між Україною та ЄС у цифровій сфері та прискорить цифровий розвиток України. Згідно з дослідженням «Інтеграція України у єдиний цифровий ринок ЄС: потенційні економічні переваги» [6], поступове наближення регуляторного середовища та цифрового розвитку України до рівня ЄС у рамках інтеграції до Єдиного цифрового ринку ЄС вплине на двосторонню торгівлю між Україною та ЄС: зростання експорту з України до ЄС товарів – на 11,8-17% (2,4-3,4 млрд дол. США), послуг – на 7,6-12,2% (302,5-485,5 млн дол. США). Також це вплине на продуктивність та економічне зростання України: зростання ВВП України – на 2,4-12,1% (3,1-15,8 млрд дол. США), добробуту громадян – на 3,6-7,8%.

Література

1.Digital Economy and Society Index 2021: overall progress in digital transition but need for new EU-wide efforts. URL:https://ec.europa.eu/commission/presscorner/detail/en/ip_21_5481

2.Андрощук Г. О. Цифрова трансформація європейської економіки: аналіз технологічних трендів. // Парламентський контроль в умовах децентралізації державної влади та цифрової трансформації в Україні: стан і проблеми : матеріали Першої всеукраїнської науково-практичної конференції, м. Київ, 30 березня 2021 р. / упор.: В. М. Фурашев, С. О. Дорогих. – Київ, 2021. – С.88-95.

3.Europe's Digital Decade: digital targets for 2030. URL:https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

4.Women in Digital Scoreboard 2021. URL: <https://digital-strategy.ec.europa.eu/en/news/women-digital-scoreboard-2021>

5. Європейська Бізнес Асоціація. Індекс цифрової трансформації 2021. https://eba.com.ua/wp-content/uploads/2021/05/digital-index_ukr1.pdf

6. Економічні переваги від інтеграції в Єдиний цифровий ринок ЄС: названі реальні цифри. URL: <https://thedigital.gov.ua/news/ekonomichni-perevagi-vid-integratsii-v-ediniy-tsifroviy-rinok-es-nazvani-realni-tsifri>

Дорогих С. О.

кандидат юридичних наук, старший науковий співробітник ДНУ «Інститут інформації, безпеки і права НАПрН України»

ПОБУДОВА НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ: ІНОЗЕМНИЙ ДОСВІД

За останні два роки світ став свідком стрімкого зростання кількості кібератак. Це загрозливе явище певною мірою пов'язане, зокрема, з тим, що в умовах пандемії значна кількість співробітників працюють у віддаленому режимі. У той же час питання війн у кіберпросторі та поширення кіберзлочинності набуває гостріших форм.

Голова VMware зі стратегії кібербезпеки Том Келлерманн під час інтерв'ю у прямому ефірі Global Security Insights Report наголосив, що «картелі кіберзлочинності посилюються ситуацією, пов'язаною зі специфікою трудової діяльності в умовах пандемії, оскільки традиційна організована злочинність є обмежена можливостями повноцінно працювати через ізоляцію». Значна частина кібер-картелів створили складну структуру квазі-стартапів, до якої входять розробники та групи контролю якості. Дехто з них навіть користується підтримкою міжнародних урядів.

Том Келлерманн зазначив, що деякі країни навіть вважають кіберзлочинців певним національним ресурсом, оскільки окремі уряди часто розглядають ці групи як засоби нейтралізації економічних санкцій та організації своїх довірених осіб для створення своєрідного повстанського руху проти своїх геополітичних ворогів [1].

Ця проблема стала актуальною як для світу в цілому, так і для України. Особливий інтерес для України має досвід розвинених країн. Хотілося б зупинитися на окремих прикладах іноземного досвіду розв'язання питань кібербезпеки на правовому та організаційному рівнях.

Одним із головних питань побудови національної системи кібербезпеки є створення спеціалізованої структури (міністерства чи іншого органу виконавчої влади) у цій сфері.

Деякі країни нещодавно утворили подібні структури та призначили керівників органів, відповідальних за питання кібербезпеки.

У 2018 році уряд Канади заснував Канадський центр кібербезпеки як національний орган країни з кібербезпеки та реагування на кіберзагрози. У межах Національної стратегії кібербезпеки Канади Кіберцентр надаватиме консультації та рекомендації підприємствам, організаціям та громадянам як центральне надійне джерело інформації.

У листопаді 2020 року Об'єднані Арабські Емірати створили нову національну раду задля розробки політики та законів, спрямованих на посилення кібербезпеки. Прем'єр-міністр Рашид Аль Мактум заявив, що безпека у цифровому просторі є такою ж важливою, як і безпека в інших галузях.

У цьому ж місяці 2020 року уряд Великої Британії оголосив, що міністерство оборони, уряд та штаб-квартира комунікацій об'єднали зусилля для створення Національних кіберсил (NCF). Їхньою метою стала допомога підприємствам та урядовим організаціям у захисті від кіберзагроз, включаючи порушення роботи або руйнування систем зв'язку, що становлять загрозу безпеці.

Слід окреслити окремі компетенції, якими повинен володіти голова державного органу з питань кібербезпеки.

Кожна система, що побудована за допомогою інформаційних та комунікаційних технологій, є уразливою для кібератак. У світі комп'ютерні мережі досягли такого рівня складності, що володіння великим обсягом спеціальних знань – є єдиним інструментом, котрий допоможе захистити їхню цілісність від кібератак. Отже, програмування, криптографія, організація безпеки даних та кон-

фіденційності персональних даних мають вирішальне значення для розуміння кібербезпеки та виконання захисної функції.

Управління процесом побудови національної системи кібербезпеки вимагає окремого набору знань, вмінь та навичок і абсолютно нового типу політика в уряді. Нинішнім політикам не вистачає фахової підготовки у сфері ІТ, яка необхідна для розуміння складності сучасного кіберпростору. Проте слід мати на увазі, що кіберпростір складається не лише з інформаційних технологій, а й людей, котрі знаходяться у ньому. А отже керівники державних органів з питань кібербезпеки мають бачити ширше проблему, тобто додатково володіти обсягом таких дисциплін, як суспільні науки, психологія, соціальна психологія та інженерія, для розуміння використання кіберпростору як на користь державі, так і проти неї [2].

Дуже гострим постає питання ведення статистики кіберінцидентів на території країни. Це пов'язано з тим, що для приватних компаній факт кіберінциденту, особливо пов'язаного з витоком персональних даних, є серйозною іміджевою втратою.

У серпні 2021 року у Сполучених Штатах Америки Національний кібер-директор Кріс Інґліс підтримав ідею створення Бюро кіберстатистики при Міністерстві внутрішньої безпеки для збору, аналізу та публікації інформації щодо кіберінцидентів, наданої групами, котрі займаються даною проблемою.

Як реакція на значне збільшення кібератак за останній рік, у серпні 2021 р. група депутатів Палати представників і Сенату подала закон, покликаний допомогти федеральному уряду краще відслідковувати та аналізувати кіберзлочинність у країні.

Закон про покращення вимірювання показників кіберзлочинності (The Better Cybercrime Metrics Act) започаткує процес поліпшення збору даних про кіберзлочинність з боку уряду і правоохоронних органів. Це допоможе виправити ситуацію, коли багато злочинів не реєструвались та не відстежувались, що ускладнювало вжиття відповідних заходів урядом.

У цьому ж законопроекті буде реалізовано кроки щодо включення звітів про кіберзлочини від посадових осіб на всіх рівнях

до Національної системи звітності про інциденти (входить до структури ФБР) та вимога до Державного управління звітності інформувати про поточні заходи щодо кіберзлочинності та їхнє виокремлення від інших видів злочинної діяльності [3].

12 травня 2021 року адміністрація президента Байдена видала «Указ про підвищення кібербезпеки країни». Документ спрямований на посилення здатності федерального уряду реагувати на загрози кібербезпеки та запобігати їм, у тому числі шляхом модернізації федеральних мереж, підвищення безпеки ланцюжка поставок програмного забезпечення федерального уряду, впровадження покращених практик та процедур кібербезпеки у федеральному уряді, а також створення загальнодержавних планів для реагування на інциденти. Указ охоплює широке коло питань і процесів, встановлюючи численні крайні терміни для вироблення рекомендацій федеральними агентствами, приділяючи особливу увагу посиленню захисту федеральних мереж у партнерстві з постачальниками послуг для федеральних агентств. Суб'єкти приватного сектора, включаючи федеральних підрядників і постачальників послуг, матимуть можливість зробити свій внесок у деякі з цих дій [4].

Наведений досвід розвинених країн безперечно становить цінність і для побудови національної системи кібербезпеки України. Слід зазначити що побудова національної системи кібербезпеки потребує від держави системного багаторівневого підходу до фіксації і обробки інформації щодо кіберінцидентів, розроблення системи запобігання та протидії їм; створення відповідних компетентних державних структур, що повинні очолити ці процеси; налагодження співпраці між приватним сектором та державними установами у сфері кібербезпеки.

Використані джерела

1. Radius Staff. Surge in Cyberattacks Targets the Anywhere Workforce VMware, Inc. URL: <https://www.vmware.com/radius/surge-in-cyberattacks-targets-anywhere-workforce>.

2. Anas Chbib. Why every government should have a cybersecurity minister. *BetaNews, Inc.* URL: <https://betanews.com/2021/08/27/government-need-cybersecurity-minister>.

3. Maggie Miller. Lawmakers roll out bipartisan bill to help track cyber crimes. *The Hill*. URL: <https://thehill.com/policy/cybersecurity/566553-lawmakers-roll-out-bipartisan-bill-to-help-track-cybercrimes>.

4. Susan B. Cassidy, Trisha Anderson, Micaela McMurrough, Robert Huffman. President Biden Signs Executive Order Aimed at Improving Government Cybersecurity. *Covington & Burling LLP*. URL: <https://www.insideprivacy.com/cybersecurity-2/president-biden-signs-executive-order-aimed-at-improving-government-cybersecurity/#page=1>.

Андрієнко О. В.

кандидат психологічних наук, адвокат,
заступник директора з правових
питань ДП «ССМ» (Publicis Groupe
Ukraine), член Експертного комітету
з питань розвитку сфери штучного
інтелекту в Україні при Міністерстві
цифрової трансформації

ПРАВА НА ЕНЕРГІЮ, ІНФОРМАЦІЮ ТА СВОБОДУ ІНТЕРПРЕТАЦІЇ ЯК МЕТАПРАВА СУБ'ЄКТІВ ФІЗИЧНОГО ТА ЦИФРОВОГО СВІТУ

Уявіть, що ви присутні в момент Великого вибуху і можете вплинути на те, які фізичні закони будуть діяти у новонародженому фізичному світі. Або спостерігаєте кембрійських вибух і можете задати параметри становлення майбутніх видів та екосистем. Приблизно те ж відбувається зараз, – коли формується віртуальний Метавсесвіт, – байдуже, у версії компанії Мета (екс-Facebook) чи як результат спільних зусиль великих і малих, корпоративних й індивідуальних акторів. Такий Метавсесвіт вимагає становлення законів свого функціонування, що не лише спонукає до переосмислення права на інформацію та інформаційних прав (навіть у тих юрисдикціях, де вони законодавчо не визначені), але й ставить

питання про нормативне закріплення метаправ як основи для віртуальних та цифрових прав.

Перш ніж взятися до правових дефініцій, почнемо з базових понять: інформація, енергія та право. З точки зору фізики, всі явища у Всесвіті можна звести до двох першооснов – інформації (концепція Віллера “it from bit” – «все з біта» [1]) та енергії (знамените ейнштейнівське $E = mc^2$). Якщо енергію можна інтерпретувати як міру активності (руху та взаємодії), то інформація – це усталена у певній кількості вимірів форма (контури) такої активності, на що вказує й латинська семантика цього слова: in-forma-tion. Енергія та інформація постійно перебувають у процесі взаємної трансформації: потоки енергії структуруються, набуваючи форми, а створена форма залучає все більше енергії для збереження та відтворення у просторі та часі. Тому будь-яке явище (сутність) як фізичного (чи реального – від лат. *res*: річ, дійсність), так і віртуального світу можна розглядати як стійкі цикли енергетично-інформаційного обміну. Такі цикли розгортаються у низці вимірів (простір, час, вимір ймовірностей тощо), у різних масштабах (субатомний рівень, атомний, молекулярний, клітинний, організмичний, організаційний, планетарний, галактичний і т.д.) і на різних рівнях віртуалізації (абстракції): явища фізичні, хімічні, біологічні, психічні, соціальні, економічні, правові, цифрові тощо.

Ключовим актором у цьому процесі виступає носій психіки (індивідуальний чи колективний), який слугує гравітаційним ядром для стабілізації циклів інформаційно-енергетичного обміну на різних рівнях віртуалізації. В результаті такої взаємодії між носієм психіки та хвилями енергії та інформації постає сутність (форма), якій актор (індивідуальний чи колективний) делегує частину своєї гравітаційної сили (передусім, шляхом включення такої форми до поля своєї уваги), що дозволяє цій формі самопідтримуватися, розвиватися та самовідтворюватися, здійснюючи експансію не лише у часі, але й у просторі та вимірі ймовірності. Найближча ілюстрація у фізиці – це двощілинний експеримент, у якому частка (елементарна фізична сутність) за відсутності спостереження поводить себе як хвиля, а за його наявності – як частка. У праві

прикладом такого делегування є створення юридичної особи – інституціолізованого віртуального колективного актора, наділеного правосуб'єктністю. Новостворена сутність, як правило, належить до вищого рівня віртуалізації, ніж актори, що її створили: держава порівняно з громадянами, міжнародні організації порівняно з державами тощо.

За такого підходу **право має три значення:**

1) Набір специфічних соціальних інструментів для структурування та регулювання циклів енергетично-інформаційного обміну на певному рівні віртуалізації. Цим інструментам притаманна як інформаційна (набір правил), так й енергетична (механізми заохочення та примусу) складові;

2) Всесвіт явищ особливого рівня віртуалізації – правових феноменів, тобто інтерпретованих у певний спосіб (матеріальне право) та фіксованих певними засобами (процесуальне право) сукупностей циклів енергетично-інформаційного обміну, коли хвилі неоднозначних та багатовекторних соціальних взаємодій (енергії) колапсуються до однозначних часток – юридичних фактів, норм тощо (інформації);

3) Суб'єктивна (внутрішня) та об'єктивна (зовнішня) можливість актора, тобто суб'єкта права, усвідомлено включатися до циклів енергетично-інформаційного обміну та змінювати їх завдяки притаманній актору свободі інтерпретації.

Отже, у будь-якій реальності суб'єкту належить три базові права (**метаправа**): **право на інформацію, право на енергію та право на свободу інтерпретації.**

Право на інформацію та право на енергію включають право на доступ до них, їх безпеку та на засоби маніпуляції ними, а саме право на:

1) доступ до інформації та енергії;

2) **здорове інформаційне чи енергетичне середовище та захист від інформаційного чи енергетичного перевантаження** (право на кібербезпеку, захист від спаму, іонізуючого випромінювання тощо);

3) **право на інформаційну та енергетичну освіту**, котра включає:

- а) освоєння базових навичок **гігієни** – енергетичної (багато з яких охоплюється поняттям здорового способу життя) та інформаційної (критичне мислення, медіаграмотність та ін.);
- б) набуття **грамотності**: від вміння читати та писати – до технологічної та цифрової, тобто освоєння навичок маніпулювання енергією та інформацією й взаємно трансформувати їх.

Право на енергію та право на інформацію є передумовами для реалізації права на **свободу інтерпретації як здатності суб'єкта свідомо обирати**:

а) до яких циклів енергетично-інформаційного обміну (зокрема, соціально-правових відносин) **включатися** та у який спосіб це робити;

б) які сутності (об'єкти чи суб'єкти) **створювати**;

в) за якими параметрами та у яких напрямках **здійснювати експансію** у реальному і віртуальному світі;

г) яким сутностям **делегувати** свою гравітаційну потужність для підтримання певних процесів енергетично-інформаційного обміну, у тому числі делегувати право приймати відповідні рішення (наприклад, обробляти персональні дані чи управляти державою).

Слід підкреслити, що вміння суб'єкта **свідомо** делегувати свою гравітаційну потужність (зокрема, приділяючи увагу, діючи на підтримку чи проти когось чи чогось, утримуючись від дії) набуває критичного значення внаслідок таких причин:

1. Становлення **економіки уваги**, коли найзапекліша економічна боротьба ведеться за увагу конкретної людини і монетизуються звичайні «лайки»;

2. Розвиток інформаційних технологій, особливо у формі **штучного інтелекту**, механіку яких жодна людина як індивідуальний суб'єкт ані фізично, ані інтелектуально не може досягнути, і водночас яким людина з легкістю делегує виконання чимраз складніших завдань із підтримки не лише власного життя, але й життя людства як колективного суб'єкта;

3. Поява **принципово нових колективних людських суб'єктів** за своїми масштабами у просторі та часі, кількістю опрацю-

вуваних ймовірностей (варіантів розвитку подій), кількістю залучених учасників, інтенсивністю та якістю їхньої взаємодії, їхньою колективною гравітаційною і творчою потужністю. Соціальні мережі, блокчейн, віртуальні світи мережеских ігор, штучний інтелект – всі вони є дітьми таких колективних суб'єктів, живляться їхньою увагою і водночас є не просто інструментами, а середовищем для розвитку таких суб'єктів;

4. становлення **принципово нового середовища переважного буття і діяльності людства** як колективного суб'єкта: по мірі зростання матеріального благополуччя, людство мігрує у все даліші шари віртуального середовища, паралельно делегуючи інформаційним технологіям забезпечення фізичного виживання та благополуччя: від виробництва продовольства й електроенергії, охорони здоров'я і навчання – до забезпечення торгівлі, логістики, соціального управління, охорони довкілля й людського дозвілля. Таким чином, відбувається злиття фізичної реальності та численних віртуальних реальностей, створених людьми.

Отже, становлення Метавсесвіту на базі вже існуючих віртуальних реальностей та їх тісне переплетіння з фізичним світом ставлять питання про розширення обсягу прав існуючих суб'єктів права, у тому числі, з урахуванням можливої появи нових сутностей, наділених правосуб'єктністю. Водночас, розмаїття вже закріплених прав потребує узагальнення на метарівні. Це спонукає переосмислити існуючі концепції (від Загальної декларації прав людини до схвалених 24 листопада 2021 року ЮНЕСКО Рекомендацій стосовно етики штучного інтелекту [2]) та виділити метаправа будь-якої сутності, яка визнається чи потенційно може бути визнана суб'єктом (актором чи агентом) як у фізичному чи віртуальному світах, так і на їх перетині – у доповненої реальності.

До вказаних метаправ пропонуємо віднести право на енергію, право на інформацію та право на свободу інтерпретації відповідно до описаних вище дефініцій. Такі метаправа повинні стосуватися будь-якого середовища – як фізичного, так і віртуального, зокрема, цифрового. Вже сьогодні ці метаправа знаходять своє фрагментарне відображення у багатьох правових системах.

У свою чергу, здатність ефективно реалізовувати вказані мета-права одночасно у різних середовищах може слугувати надійним критерієм для визнання тієї чи іншої сутності (окремих людей, колективних людських суб'єктів, суб'єктів на основі колаборації людей та штучного інтелекту, втілених носіїв штучного інтелекту тощо) суб'єктом права.

Література:

1. Wheeler, J. A. Information, physics, quantum: The search for links. // A. J. G. Hey (Ed.), Feynman and computation: Exploring the limits of computers. – Cambridge, MA: Perseus. – 1999. – P. 309-336.
2. UNESCO. The Recommendation on the Ethics of Artificial Intelligence. <https://en.unesco.org/artificial-intelligence/ethics> – дата доступу 29.11.2021.

Марценко Н. С.

кандидат юридичних наук,
доцент кафедри міжнародного
права та міграційної політики
Західноукраїнського національного
університету

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ЦИВІЛЬНОМУ СУДОЧИНСТВІ

Сьогодні юридична практика знаходиться на піку революційних змін, спричинених залученням Штучного Інтелекту (далі – ШІ) у діяльність органів судової влади. Найбільше такі інновації стосуються саме цивільного права та судочинства, які через свою правову сутність регулюють найбільше питань, пов'язаних із запровадженням технологій ШІ. Разом із тим, запуск таких проєктів, що спеціалізуються на розробці нових юридичних послуг, відбувається разом із новими програмами розвитку та вдосконалення професій, переважно для юристів, юридичних служб та страховиків, які дозволяють поглиблювати доступ до судової інформації та

права [1, с.14]. Більше того, низка таких програмних забезпечень ІІІ будує моделі машинного навчання для прогнозування результатів розглянутих справ, використовуючи в якості вхідних даних відповідний прецедент та особливості конкретного випадку.

Без сумніву, залучення технологій ІІІ в масштабі може замінити багато роботи, яку юристи виконують щодня. Зростаюча доступність та практичність технологій ІІІ, таких як машинне навчання та обробка природної мови у юридичному секторі, створила новий клас інструментів, які допомагають правовому аналізу в таких сферах, як юридичні дослідження, вивчення та перегляд документів, перевірка контрактів [2, с.1]. Потенційні програми ІІІ включають корпоративну та фінансову ретельність документації, майнові звіти про право власності, ведення судових процесів, аналіз договорів та звітів. Вже сьогодні діючі програми ІІІ у правовому секторі поділяються на такі основні категорії [3]:

- послуги з проведення “due diligence” (перевірка належної сумлінності) – підтвердження фактів та цифр та ретельного оцінювання правової ситуації [4, с. 267]. Цей процес належної ретельності необхідний для розумного консультування клієнтів щодо того, які є варіанти розвитку справи та які дії вони повинні вжити перед або під час судового процесу. Такий процес є часто дуже трудомістким і виснажливим, адже юристи повинні провести всебічне розслідування та аналіз усіх даних справи. З огляду на це, правники схильні до помилок та неточності під час проведення таких перевірок. Тому вже сьогодні багато зарубіжних юридичних фірм та органів судової влади користуються потужними програмними забезпеченнями машинного навчання, яке аналізує текст у контрактах, даних матеріалів до суду на стадії подачі, а також інших документах. Серед них: Kira Systems (Канада), Levertton (Німеччина), eBrevia (США), JPMorgan (США), Ross Intelligence (США) та інші [3].
- технологія прогнозування – програмне забезпечення ІІІ, що генерує результати, які прогнозують результат судових процесів. Наприклад: у жовтні 2017 року Casecruncher Alpha

[5] (програма ШІ) виграла тижневий конкурс проти комерційних юристів з точністю 86,6% зроблених прогнозів. Правозахисники досягли точності лише 62,3%. Ці результати показують, що якщо питання визначено точно (наприклад, – «чи була ця скарга на незаконний продаж підтримана або відхилена?»), то ШІ може конкурувати, а іноді і перевершувати юристів. У Франції апеляційні суди міст Ренн та Дуе випробували програмне забезпечення для прогнозування правосуддя у різних справах про апеляції у 2017 році [6, с.80].

- юридична аналітика – юристи можуть використовувати дані із минулого судового права, коефіцієнти виграшів / втрат та історію судочинства, для ефективної подальшої діяльності. Яскравим прикладом застосування таких технологій є інновація Данієля Кацця, професора юридичного коледжу в Чикаго Іллінойського технологічного інституту. У травні 2017 року науковець використав базу даних Верховного Суду США, яка має справи, починаючи з 1791 року, для створення алгоритму, призначеного для прогнозування результату будь-якого судочинства. Аналітична модель передбачала понад 240 000 голосів окремих суддів і результати приблизно 28 000 випадків між 1816-2015 рр [7, с.1]. Більше того, ця модель спрацювала, адже досягла 70,2% точності на рівні результатів справи та 71,9% на рівні вироків присяжних. Існують й інші програмні забезпечення подібного характеру, які поєднують машинне навчання та юридичний аналіз але з обмеженим охопленням. Наприклад технологія «Loom» [3], яка містить показники виграшів / програшів та інформацію, яка стосується судочинства, але лише для цивільних справ у окремих провінціях Канади.

Варто зазначити, що сучасні розробки в галузі ШІ в юридичній практиці набувають різних застосувань, які стали особливо актуальними в період глобальної пандемії COVID-19. Як один із заходів щодо запобігання поширенню коронавірусної інфекції, суди у більшості частинах світу тимчасово призупиняли та скасовували

засідання. Водночас економічні наслідки кризи COVID-19 вплинули також і на роботу багатьох юридичних фірм. Зокрема, щоб захистити свої підприємства, юридичні компанії урізали заробітні плати своїм працівникам, зменшували залучення партнерів, деякі навіть звільняли співробітників або ж й зовсім переставали існувати. Натомість багато юридичних фірм, таких як «Luminance» у Великій Британії [8], за короткий час стали одними з найбільш потужних, використовуючи технології ШІ (послуги з проведення “due diligence”). Так само і судова система, керована ШІ, могла б гарантувати безперервне продовження процесів судочинства під час пандемії. Тим не менш, вже сьогодні Міністерство юстиції Естонії планує розробити «суддю-робота», який міг би вирішувати суперечки щодо невеликих позовів [9]. Чиновники сподіваються, що ця система зможе усунути проблеми довгої судової тяганини. Іншим прикладом, того як пандемія вплинула на стрімкий розвиток технологій ШІ у юридичній площині є те, що в Австралії оформляти розлучення тепер буде ШІ, взявши на себе розподіл майна, розробку угоди про реалізацію батьківських прав та реєстрацію свідцтва про розлучення [10]. Видається, використання ШІ у судовій системі може допомогти мінімізувати вплив сторонніх факторів, таких як втома та емоційна нестабільність правників, а зважаючи на останні події у світі – і при надзвичайних ситуаціях масового захворювання.

Проте варто враховувати те, що обробка судових рішень та даних ШІ вимагає інвестицій у підтримку інструментів не лише для системи, але й для юристів, які повинні досягнути усі тонкощі нових технологій. Тому, ресурси, необхідні для створення технологій ШІ щоб підтримувати судову систему, можуть бути недоступними для деяких країн, що розвиваються.

Іншою, не менш важливою, характеристикою використання ШІ в цивільному судочинстві зарубіжних країн – є його правове регулювання. Не зважаючи на значне залучення нових технологій, варто пам'ятати про основні принципи їхнього подальшого застосування. У 2018 році Європейська комісія з ефективності правосуддя Ради Європи прийняла вагомий міжнародний акт – Етичну

хартію по використанню штучного інтелекту у судовій системі та її середовищі [11]. Цей документ складають п'ять основних принципів, які повинні підлягати регулярному застосуванню та моніторингу та з боку державних та приватних суб'єктів з метою постійного вдосконалення практики. Ці правові основи використання штучного інтелекту під час здійснення правосуддя утворюють:

1. Принцип поваги до основних прав людини: забезпечити сумісність із розробкою алгоритмів із основними правами ЄКПЛ, Конвенції про захист персональних даних і т.д.

2. Принцип недискримінації: запобігати розвитку чи посиленню будь-якої дискримінації між окремими особами чи групами осіб, методами обробки даних.

3. Принцип якості та безпеки: який відноситься обробки судових рішень та даних у безпечному технологічному середовищі, використовуючи засвідчені джерела інформації суддів, адвокатів, прокурорів, науковців та інших правників.

4. Принцип прозорості, неупередженості та справедливості: зробити методи обробки даних доступними та зрозумілими, санкціонувати зовнішній аудит.

5. Принцип «під контролем користувача»: виключає рецептивний підхід та гарантує, що користувачі – є проінформованими та контролюють зроблений вибір.

Ринок юридичних послуг – один з найбільших у світі. На краще чи гірше, галузь права є традиційно обмеженою і, як відомо, повільно застосовує нові технології та інструменти. Проте є тенденція того, що це зміниться протягом наступних років. А ШІ більше, ніж будь-яка технологія до цього, кардинально перетворить сутність юридичної професії.

Таким чином, зважаючи на практику зарубіжних країн існує багато переваг застосування технологій ШІ у юридичній професії, а зокрема – у цивільному судочинстві. На даний час, у деяких юрисдикціях процеси автоматизації та роботизації, такі як: послуги з проведення “due diligence”, технології прогнозування та юридична аналітика – вже є звичайними складовими діяльності багатьох міжнародних юридичних фірм та судових органів. На-

разі ці системи розроблені тільки у взаємодії з людиною: тобто юрист переглядає аналіз ШІ та приймає остаточні рішення. Проте прогрес не стоїть на місці і ШІ більше, ніж будь-яка технологія до цього, поступово кардинально трансформує юридичну практику. Водночас, не зважаючи на такий стрімкий розвиток ШІ, його правове регулювання та функціонування у судових органах повинно відповідати основоположним принципам та правам людини.

Література

1. Council of Europe European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment. – Council of Europe, Strasbourg, 2019. 79p. URL: <https://rm.coe.int/ethical-charter-en-for-publication-4-decem-ber-2018/16808f699c>
2. Arruda A., Scherer M. Artificial Intelligence: Will it Replace Lawyers?. – Benchmark Report, Portland, Oregon, 2017. 38p. URL: https://cdn.ymaws.com/www.aclea.org/resource/collection/81118223-16F9-46DB-B5DC-772EF45FB936/6-A4_Artificial_Intelligence.pdf
3. Faggella D. AI in Law and Legal Practice – A Comprehensive View of 35 Current Applications. – Emerj Artificial Intelligence Research, 2020. URL: <https://emerj.com/ai-sector-overviews/ai-in-law-legal-practice-current-applications/>
4. Сігарчук А. Ю. Сутність due diligence і можливості використання в Україні. *Проблеми обліку, аналізу, аудиту і контролю*: вісник Університету банківської справи Національного банку України № 1 (16). Київ. 2013. С. 267-269. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/VUbsNbU_2013_1_51.pdf
5. Cellan-Jones R. The robot lawyers are here – and they're winning. – the BBC, 2017. URL: <https://www.bbc.com/news/technology-41829534>
6. Boring N. France *Regulation of Artificial Intelligence in Selected Jurisdictions* 2019.79-83 p. URL: <https://www.loc.gov/law/help/artificial-intelligence/regulation-artificial-intelligence.pdf> (дата звернення 16.07.2020)
7. Katz D. M., Blackman J., Bommarito M. J. A General Approach for Predicting the Behavior of the Supreme Court of the United States: *article*. Chicago. 2016. 15 p. URL: <https://www.researchgate.net/>

publication/311586220_A_General_Approach_for_Predicting_the_Behavior_of_the_Supreme_Court_of_the_United_States

8. The AI Platform for the Legal Profession *Welcome AI*: веб-сайт. 2018. URL: <https://www.welcome.ai/tech/legal/luminance-smart-legal-platform>

9. NIILER E. Can AI Be a Fair Judge in Court? Estonia Thinks So *Wired*: веб-сайт. 2019. URL: <https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/>

10. Йодченко П. В Австралії оформляти розлучення тепер буде штучний інтелект *Йод.Медіа*: веб-сайт. 2020. URL: https://iod.media/article/v-avstraliji-oformlyati-rozluchennya-teper-bude-shtuchniy-intelekt-6676?fbclid=IwAR3L_OBe81DWGevNIpvr_f_xRNBFToR44nNcA5WCxWS-FP70E5KV51s6iWHA

11. Шемшученко В. Штучний інтелект у правосудді *Центр демократії та верховенства права*: веб-сайт. 2020. URL: <https://cedem.org.ua/analytics/shtuchnyj-intelekt-pravosuddia/>

Петровська А. О.

Студентка НТУУ «КПІ ім. Ігоря Сікорського»

Науковий керівник: Дубняк М. В.

кандидат юридичних наук, старший викладач, НТУУ «КПІ імені Ігоря Сікорського»

ЦИФРОВА ТРАНСФОРМАЦІЯ У СФЕРІ СУДОЧИНСТВА

У світі процес розвитку інформаційного суспільства супроводжується швидким поширенням цифрових технологій в усіх сферах нашого життя, зокрема і в сучасному судочинстві. Сьогодні стрімко розвиваються інформаційно-комунікаційні технології та сприяють цифровій трансформації суду, застосовуючи при цьому найбільш інноваційні методи. Перед дослідженням даної проблеми необхідно визначити термін «цифрова трансформація». Відповідно до Наказу Державного агентства з питань електронного урядування України «Про забезпечення реалізації деяких питань цифрового розвитку», цифрова трансформація – діяльність, що

має на меті використання цифрових технологій для вирішення традиційних проблем інноваційними способами [1].

Актуальною проблемою є правове регулювання цифровізації судочинства та закріплення на законодавчому рівні впровадження різних інформаційно-комунікаційних технологій у сферу правозастосування.

Слід відзначити деякі нормативні акти, які заклали основу для становлення електронного судочинства. Так, Закон України «Про електронні документи та електронний документообіг» поширюється на відносини, що виникають у процесі створення, відправлення, передавання, одержання, зберігання, оброблення, використання та знищення електронних документів. Закон України «Про доступ до судових рішень», який регулює відносини щодо забезпечення доступу до судових рішень, ухвалених судами загальної юрисдикції, та ведення Єдиного державного реєстру судових рішень [2, с.59; с.62]. Указом Президента України «Про Стратегію розвитку системи правосуддя та конституційного судочинства на 2021-2023 роки» передбачено розвиток електронного судочинства з урахуванням світових стандартів у сфері інформаційних технологій, його інтегрування у національну інфраструктуру електронного урядування шляхом:

1. запровадження можливості розгляду онлайн певних категорій справ незалежно від місцезнаходження сторін і суду та інших сервісів електронного судочинства;

2. впровадження сучасного електронного діловодства в суді, електронного ведення справ, електронних комунікацій із судом, кабінету судді та кабінету учасника процесу;

3. удосконалення та розвиток офіційного вебпорталу судової влади України для отримання інформації про суди і справи (провадження) з регулярним оновленням даних судової статистики [3].

Поштовхом для прискорення цифрової трансформації в різних сферах стала пандемія COVID-19. Перед судами постало багато викликів пов'язаних із дотриманням карантинних вимог. Деякі приміщення та будівлі судів були закриті повністю, інші частково, розглядаючи лише «невідкладні» справи. Не всі представники судової влади мали змогу працювати, таким чином відбувалася зміна в пріоритетності та розподілі розгляду справ. Велика кіль-

кість внесених змін до законів та нормативних актів ускладнила оскарження правових викликів у судах, тому відбувся швидкий перехід до роботи в режимі онлайн з метою вирішення проблем, які постали в період пандемії. У складних карантинних умовах ускладнили доступ до судочинства і такі проблеми, як фінансові обмеження, неефективні процедури та нездатність забезпечити швидке здійснення правосуддя [4, с.11-12]. Незважаючи на те, що основним пріоритетом стало збереження життя та здоров'я людини, важливим також залишається забезпечення можливості для кожного доступу до здійснення справедливого судочинства, а тому необхідним є також проведення реформи у даній сфері та прискорення діджиталізації суду на законодавчому рівні.

Законом 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 30.03.2020 р, у процесуальні кодекси були внесені зміни щодо проведення судових засідань з використанням власних технічних засобів, поза межами приміщення суду. Завдяки таким змінам вже більше року учасники справ мають можливість брати участь у судових засіданнях, фактично не виходячи з дому та користуючись власними технічними засобами. Такий порядок проведення судових засідань не тільки дозволяє не порушувати режим карантину та самоізоляції, але й суттєво економить час учасників справ, нівелює необхідність відряджень у інші міста України, зменшує фінансові витрати [5].

В аспекті впровадження європейських стандартів цифрово-го правосуддя в національну судову систему, слід зазначити, що Україна є однією з перших країн-партнерів ЄС, яка імплементує положення та засади Європейського кодексу електронних комунікацій. Це є прогресивним кроком, адже чинна нормативно-правової бази у цій сфері є застарілою, не відповідає сучасним реаліям та вимогам ринку. Мова йде про ухвалення 30 вересня 2020 року Верховною Радою України закону «Про електронні комунікації», який наближує Україну до утвердження європейських стандартів у галузі електронних комунікацій [6, с.101].

Україна активно впроваджує новітні технології в процес розгляду судових справ, що позитивно впливає на рівень ефективності та відкритості судочинства, а також забезпечує можливість для покращення всіх характеристик здійснення правосуддя.

На сьогодні не припиняється цифрова трансформація суду. Актуальним у сфері реалізації електронного судочинства є оголошення Вищої ради правосуддя відповідно до якого з 5 жовтня 2021 року починають офіційно функціонувати три підсистеми (модулі) ЄСІТС: “Електронний суд”, “Електронний кабінет” підсистема відеоконференцз’язку [7].

Варто зазначити про пілотний проєкт Мінцифри, який передбачає функціонування сучасного судочинства із документами у смартфоні. За допомогою тимчасового QR-коду відбувається перевірка дійсності таких документів, таким чином можна потрапити у будівлю суду. Також використання електронних документів застосовується для ознайомлення із матеріалами справи, для запису на особистий прийом до керівництва або для участі в судових справах. Тестування спрощення доступу до правосуддя за цифровими документами у застосунку Дія розпочалося на базі П’ятого апеляційного адміністративного суду.[8].

Отже, можемо зробити висновок, що на даному етапі активно здійснюється правове регулювання впровадження цифрових технологій у сферу здійснення судочинства. Під час пандемії цей процес пришвидшився, почався активний розвиток системи «Електронний суд», також в судах почали застосовувати відповідне технічне обладнання, щоб за допомогою засобів відеоконференцз’язку кожен мав можливість брати участь у судових засіданнях. Тому наразі Україна активно рухається в напрямі спрощення доступу кожної особи до суду та оптимізації здійснення правосуддя.

Список використаної літератури:

1. Наказ Державного агентства з питань електронного урядування України «Про забезпечення реалізації деяких питань цифрового розвитку» URL: <https://zakon.rada.gov.ua/rada/show/v0024883-19#Text>

2. Сердюк Л. Р. Організаційно-правові основи впровадження електронного судочинства в Україні : дис. на здобуття наук. ступеня юр. наук: 12.00.10 / Приват. вищий навч. заклад «Львівський ун-т бізнесу і права» Львів, 2017. 164 с.

3. Указ Президента України «Про Стратегію розвитку системи правосуддя та конституційного судочинства на 2021-2023 роки» від 11.06.2021 URL: <https://zakon.rada.gov.ua/laws/show/231/2021#Text>

4. Базовий посібник. Особливості функціонування судів в умовах пандемії COVID-19 URL: <https://www.osce.org/files/f/documents/9/0/483854.pdf>

5. Марина Корнієнко Цифрова трансформація судового процесу. Юрист&Закон, №17-18, 29 квітня 2021 р. URL: https://www.asterslaw.com/ua/press_center/publications/digital_transformation_of_litigation_process_in_ukraine/

6. Паскар А. Л. Електронне судочинство: Європейські стандарти VS українські реалії. Матеріали IV Міжнародної науково-практичної конференції «Сучасні виклики та актуальні проблеми судової реформи» (Чернівці, 16 жовтня 2020 року) URL: <https://law.chnu.edu.ua/wp-content/uploads/2020/12/Zbirnyk-16.10.20.pdf>

7. Прес-центр Державної судової адміністрації України. В Україні починають офіційно функціонувати підсистеми (модулі) ЄСІТС URL: <https://dsa.court.gov.ua/dsa/pres-centr/news/1188679/>

8. Прес-офіс Міністерства та Комітету цифрової трансформації. Доступ до П'ятого апеляційного адміністративного суду за цифровими документами у Дії. Міністерство та Комітет цифрової трансформації України URL: https://thedigital.gov.ua/news/dostup-do-pyatogo-apelyatsiynogo-administrativnogo-sudu-za-tsifrovimi-dokumentami-u-dii?fbclid=IwAR0N5q_U8Q-OwS39ndKXXH41JPcxqKqgXuZYHITkTKdl7c8fgzJAd0EZOmE

Кваша Т. К.

завідувач відділу Українського
інституту науково-технічної
експертизи та інформації

ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ: ПОТЕНЦІАЛ УКРАЇНСЬКОЇ НАУКИ

Планом пріоритетних дій Уряду України на 2021 рік (№276-р від 24.03.2021) поставлене широке коло завдань у сфері інформатизації суспільства, створення електронних реєстрів, розвитку ІТ-бізнесу, штучного інтелекту, тощо. Організації системи ООН наголошують на важливій стратегічній ролі форсайту, який генерує уявлення про майбутні виклики та нові ідеї для розробки політики [1, 2].

З огляду на сказане зростає актуальність технологічного форсайту на підтримку цифрової трансформації економіки та суспільства України.

Українським інститутом науково-технічної експертизи та інформації (УкрІНТЕІ) розроблено Методику здійснення форсайтних досліджень із визначення нових пріоритетних напрямів наукової та інноваційної діяльності України на 2022-2026 рр. і проведено ці дослідження за 7 напрямками або сферами:

- енергетика;
- інформаційно-комунікаційні технології;
- індустрія (нові матеріали, машинобудування, транспорт, будівництво);
- раціональне природокористування;
- науки про життя (сільське господарство та медицина);
- соціально-гуманітарна сфера;
- національна безпека.

Методика здійснення форсайтних досліджень включає 5 етапів, один з яких представляє собою збір пропозицій від представників наукових організацій та закладів вищої освіти (“науковці”) щодо дослідних робіт із розроблення нових технологій. На другому етапі експерти-практики вибирали ті пропозиції науковців, які є потрібними для їх організацій та які можна впровадити.

Аналіз анкетування науковців дозволяє визначити потенціал української науки у цій сфері.

Результати. Розроблення нової системи пріоритетних напрямів розвитку науки та інноваційної діяльності було розпочато наказом МОН від 15.02.2021 № 196 щодо створення Робочої групи, якою рекомендовано здійснювати цю роботу шляхом об'єднання зусиль законодавчої, виконавчої влади, широких кіл наукової спільноти і реального сектору економіки.

Залучення до форсайтних досліджень широкого кола представників наукової та бізнес-спільноти забезпечило неупередженість вибору пріоритетних напрямів розвитку досліджень і розробок та інновацій. Загалом в обговореннях взяло участь понад 2,5 тис. учасників, в тому числі 1556 експертів-науковців та 1062 експерти-практики.

За напрямом «інформаційно-комунікаційні технології» на I етапі опитування 148 експертами-науковцями надано 231 пропозицію. У складі 148 експертів-науковців – 40 представники науково-дослідних інститутів академій наук України, 82 – представники університетів, 3 – представники навчально-наукових інститутів та центрів.

За кількістю пропозицій найбільшу питому вагу займає група «Нормативно-правове та методичне забезпечення ІКТ», що охоплює загальні питання з розвитку сфери ІКТ, які надано у вигляді методичних рекомендацій, стратегій, концепцій – 17,5% (40 пропозицій). Із цих 40 пропозицій 16 стосуються: державної стратегії розвитку телекомунікаційної мережі загального користування України, національної стратегії і тактики побудови інформаційного суспільства (суспільства знань), концептуальної моделі цифрового інклюзивного суспільства в Україні, концептуальної моделі формування креативної економіки країни та інституційних і фінансових механізмів самореалізації людського потенціалу в умовах цифрової трансформації, концепції розвитку телекомунікацій в Україні, розроблення рекомендацій щодо розвитку нормативної бази сфери телекомунікацій України, розроблення концепції формування системи правового забезпечення проектування, вироб-

ництва та застосування базових складових технологій цифрової трансформації тощо. Пропозиції із методичного забезпечення стосувалися методик використання ІКТ для освіти і навчання та методики опрацювання розміщення об'єктів транспортної інфраструктури відповідно до геологічних факторів впливу.

Крім того, за напрямом Медицина отримано ще 15 пропозицій щодо застосування ІКТ технологій для телемедицини, формування реєстрів та 8 пропозицій із застосування штучного інтелекту для діагностики захворювань і створення нових ліків. Лише одна пропозиція стосується розроблення моделі комунікативної діяльності в публічному управлінні охороною здоров'я.

У соціально-гуманітарній сфері також надано пропозиції із використання ІКТ в управлінні, освіті, інших сферах життя, які об'єднані у групи під назвами "Організаційний та методологічний супровід функціонування системи інформаційно-аналітичного забезпечення діяльності органів управління і моніторингу її ефективності", "Цифровізація професійної освіти", "Цифровізація різних сфер життя", "Цифровізація культурної спадщини і використання великих даних", які включають 16, 26, 27 та 4 пропозиції відповідно.

До таких пропозицій, наприклад, відноситься розроблення:

- Комплексної концепції підвищення комунікативної компетентності сучасних студентів в умовах цифровізації сучасного суспільства.
- Становлення та розвиток інституту електронних петицій в Україні. Запровадження та розвиток інституту референдумів та виборів за допомогою інформаційно-телекомунікаційних технологій.
- Методики оцінки впливу цифровізації на виробничий процес суб'єкту підприємницької діяльності на базі «великих даних».
- Прогнозування динаміки соціально-економічного розвитку міст ОТГ і областей у зв'язку із цифровізацією економіки, змінами на регіональному ринку праці та у відповідності зі стратегіями розвитку зазначених адміністративно-територіальних одиниць.

- Приймання-передавання документів в електронній формі на постійне зберігання.
- Оцифрування аудіовізуальних документів.
- Інтелектуальна технологія кібербезпеки і т.д.

Таким чином, українська наука пропонує багато досліджень і технологій із використання цифрових технологій у всіх сферах життя, при цьому частина пропозицій стосується саме правового забезпечення соціальної трансформації внаслідок використання таких технологій. Ці пропозиції стосуються розроблення стратегій, концепцій і рекомендацій щодо розвитку нормативної бази сфери телекомунікацій і цифрової трансформації України. Все сказане свідчить про наявність значного наукового потенціалу України для її цифровізації і правового забезпечення побудови інформаційного суспільства.

В то й же час, широкий розподіл пропозиції по ІКТ у розрізі всіх напрямів дослідження свідчить про нагальну потребу багатьох сфер, зокрема, освіти, охорони здоров'я, енергетики, промисловості, а також на місцевому рівні надолужити відставання у цифровій трансформації їх діяльності.

Список посилань

1. Strategic foresight for the post-2015 development agenda. Report of the Secretary-General. Commission on Science and Technology for Development Eighteenth Session. Geneva, 4–8 May 2015. E/CN.16/2015/3.
2. Foresight Manual. Empowered Futures for the 2030 Agenda. UNDP Global Centre for Public Service Excellence Singapore, January 2018. – С. 5.

Усенко Я. О.

аспірант ДНУ «Інститут інформації,
безпеки та права Національної
академії правових наук України»

ПРАВОВІ ПРОБЛЕМИ ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ УПРАВЛІННЯ ПЕРСОНАЛОМ В СУДОВІЙ СИСТЕМІ УКРАЇНИ

Сьогодні кваліфіковані працівники судової системи – це пріоритетний ресурс, тому його дефіцит може ослабити її потенціал, що призведе до негативних наслідків.

Належна організація управління персоналом у судовій системі є одним з основних факторів підвищення якості правосуддя, побудови конкурентоспроможності держави, розвитку її економіки та передумовою європейської інтеграції, що є логічним та закономірним явищем. З цією метою необхідно створити професійну, результативну, ефективну систему управління людськими ресурсами. Така перебудова системи кадрового менеджменту дозволить зміцнити позиції держави не тільки у міжнародних рейтингах, а й матиме велике суспільне значення для підвищення рівня довіри громадян до держави.

Характерними ознаками сучасного правового забезпечення кадрової роботи є: затвердження та реалізація судової реформи, посилення громадської участі у формуванні якісного суддівського корпусу; підвищення вимог до дисциплінарної поведінки суддів; підвищення антикорупційних стандартів у державі щодо державних службовців та патронатної служби.

Кадровий підхід до побудови системи управління персоналом зазнав змін завдяки усвідомленню того, що сучасний стан реформування судової системи неможливий без якісного складу суддів та персоналу, який забезпечує функціонування судової гілки влади. Нині організація роботи служб управління персоналом та підрозділів апарату судів з організації кадрового менеджменту також зазнала суттєвих змін. Таким чином, діюче законодавство України в повному обсязі не відповідає вимогам до управління персоналом в судовій системі України.

Основоположні засади кадрової роботи встановлені в Законі України «Про судоустрій і статус суддів». Зокрема, встановлено кадрову автономію для апеляційних палат вищих спеціалізованих судів, передбачено «кадрову» роль Національної школи суддів України як державної установи, яка забезпечує підготовку висококваліфікованих кадрів для системи правосуддя [1]. Суттєві зміни та вплив на зміст кадрової діяльності в судових органах відбулись у результаті проведення судової реформи та прийняття базових змін до законодавства про судоустрій та діяльність суддів. Насамперед очевидним є розширення кадрових процедур на етапі відбору суддів.

Значним кроком на шляху впровадження інформаційних технологій в роботу судів, органів та установ системи правосуддя, а також автоматизація їх діяльності стало впровадження Стратегії реформування судоустрою, судочинства та суміжних правових інститутів на 2015-2020 роки (далі – Стратегія), схваленої Указом Президента України від 20 травня 2015 № 276. На виконання вимог Стратегії внесено низку суттєвих змін до законодавства щодо організації діяльності судів, органів та установ системи правосуддя, а також порядку забезпечення їх функціонування.

Також, певні зміни, що стосуються автоматизації здійснення правосуддя, прийнято Законом України від 03.10.2017 №2147-VIII «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів», який набрав чинності 15 грудня 2017 року. Відповідно до вимог цього Закону в судах, Вищій раді правосуддя, Вищій кваліфікаційній комісії суддів України, Державній судовій адміністрації України, Службі судової охорони, їх органах та підрозділах забезпечується функціонування Єдиної судової інформаційно-телекомунікаційної системи (далі – ЄСІТС). На перехідний етап до впровадження ЄСІТС рішенням Ради суддів України від 02.03.2018 № 17 внесено зміни до Положення про автоматизовану систему документообігу суду, якими вже передбачено запровадження ряду інструментів електронного правосуддя.

Так, ЄСІТС передбачає автоматизацію ділових процесів, включаючи процеси документообігу, розгляд судових справ, складання оперативної та аналітичної звітності, надання інформаційної допомоги суддям, а також процесів, які забезпечують фінансові, майнові, організаційні, кадрові та інформаційно-телекомунікаційні потреби органів судової влади.

ЄСІТС має забезпечити ведення електронного діловодства, в тому числі рух електронних документів у межах відповідних органів та установ та між ними, реєстрацію вхідних і вихідних документів та етапів їх руху; централізоване захищене зберігання документів та інформації в єдиній базі даних; обмін документами та інформацією (надсилання та отримання документів та інформації, спільна робота з документами) в електронній формі між судами, іншими органами системи правосуддя; автоматизацію роботи судів, органів та установ системи правосуддя, в тому числі, автоматизоване формування в режимі реального часу основних аналітичних показників діяльності; автоматизацію процесів ведення бухгалтерського, статистичного, кадрового обліку, формування та консолідації фінансової, статистичної та управлінської звітності; автоматизацію процесів планування та виконання бюджетів; формування і ведення суддівського досьє (досьє кандидата на посаду судді) в електронній формі та інше [2].

Суттєве пришвидшення процесів розвитку передових технологій сприяє значному посиленню їх проникнення в усі сфери економічного та соціального життя, зокрема у процеси управління організаціями та ведення бізнесу. При цьому цифрові перетворення змінюють способи здійснення управлінської діяльності, трансформують процеси управління змінами, ведуть до появи цифрового мислення та революціонізують досвід працівників, вимагаючи актуалізації існуючих HR-технологій.

Діджиталізація управління персоналом передбачає зміни, що відбуваються у трьох напрямках:

1. цифрова робоча сила (залучення працівників з інноваційним типом мислення, ліквідація цифрового розриву у нави-

чках, забезпечення постійного удосконалення знань, вмінь, навичок за допомогою сучасних технологій);

2. цифрове робоче місце (створення робочого середовища, що забезпечує високу продуктивність праці, можливості збору інформації щодо виконання завдань, використовує сучасні засоби комунікацій та підтримує зворотній зв'язок з працівниками);
3. цифровий HR (трансформація функцій управління персоналом на основі новітніх комп'ютерних технологій, використання цифрових інструментів, програмних продуктів) [3].

Таким чином, незважаючи на те, що цифрова трансформація бізнесу впливає на управління персоналом, діджиталізація цього процесу відбувається також кількома способами: від етапів залучення та набору персоналу до автоматизації процесів управління персоналом та керування даними. При цьому ефективний процес цифрової трансформації управління персоналом в установі передбачає врахування існуючих можливостей та загроз і вироблення на цій основі ефективної стратегії діджиталізації [4].

Зважаючи на вишевикладене пропонується переглянути низку нормативно-правових актів, що стосуються впровадження інформаційно-комунікаційних технологій, а також розробити нові, якими визначити поняття інформації, яка відноситься до сфери управління персоналом. Тому необхідно розробити Положення про інформаційну політику та відповідні документи для організації захисту персональних даних. Здійснити порівняльний аналіз та підбір спеціалізованих програмних продуктів для спеціалістів по роботі з персоналом, а також порівняльну характеристику автоматизованих робочих місць фахівців з управління персоналом. Зважаючи на стрімкий розвиток діджиталізації доцільно підготувати нормативні документи, що впорядкують процедури застосування кваліфікованих електронних підписів та порядок дій у разі їх компрометації [5]. Також доцільно розробити правову регламентацію використання комп'ютерного поліграфу під час прийняття на роботу, відеофіксації процесу роботи персоналу, проведення конкурсів на заміщення вакантних посад тощо [6].

Література

1. Шевченко А. До питання про правове регулювання кадрової роботи в судовій системі. Актуальні проблеми правознавства. – 2020. – Вип. 3. – С. 115-120.
2. Послуги з доставки абонентам судових повісток в електронному вигляді. Інформація щодо обґрунтування технічних та якісних характеристик. URL: <https://hr.court.gov.ua/tu21/inshe/dergzac/b8>.
3. Digital Transformation and the Evolution Of HR Trends. URL: <http://infosystems.mu/digital-transformation-and-the-evolution-of-hr-trends>.
4. Козак Т. М., Копитова І. В., Особливості управління персоналом на підприємствах в умовах діджиталізації економіки. URL: <https://conf.ztu.edu.ua/wp-content/uploads/2021/01/136.pdf>.
5. Костенко О. В. Компрометація особистого ключа електронного підпису (правовий аспект) / Journal of Innovative Technologies in Economy. 2018. – № 3(15). – С. 15-22.
6. Клименко К. О., Костенко О. В. Інформаційна діяльність та інформаційне забезпечення діяльності адвоката в Україні. WORLD SCIENCE RS GlobalVol.4, March 2020. № 3(55). С.4-7. DOI:https://doi.org/10.31435/rsglobal_ws/31032020/6971.

Барсуковський О. Р.

курсант Дніпропетровського
державного університету внутрішніх
справ

Науковий керівник: Ярошенко А. С.

кандидат юридичних наук, доцент
кафедри цивільного права та процесу
Дніпропетровський державний
університет внутрішніх справ

ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У СФЕРІ СІЛЬСЬКОГО ГОСПОДАРСТВА

В інноваційних цифрових технологіях 21 століття прихований величезний потенціал для економічного зростання завдяки точності, автоматизації та новим можливостям управління. Знач-

ною мірою цифрова трансформація застосовується до сільського господарства особливо на підставі технологічного розмаїття сільськогосподарського виробництва та культур, пов'язаних з різноманіттям та трудомісткістю виробничих процесів.

Внаслідок обмеженості ресурсів (нерухомого характеру земельних ресурсів як фактора виробництва, регіональних кліматичних умов, збільшення екстремальних метеорологічних явищ) у фермерів у разі підвищення продуктивності виникають конфлікти цілей, наслідком яких є, наприклад, ерозія ґрунту, забруднення водоймів через внесення добрив або засобів захисту рослин або викидання в атмосферу речовин, що забруднюють довкілля.

Потенціал цифровізації полягає саме в ослабленні цільових конфліктів при можливості ефективної розробки процесів виробництва, організації та управління. Цей результат досягається на основі інноваційних технологій шляхом вузькоспеціалізованого та цілеспрямованого застосування відповідних індивідуальних ресурсів зростання виробництва. Водночас, завдяки своїй можливості багатопланового застосування, цифрова трансформація дає основу для сталого розвитку у разі одночасного підвищення продуктивності у процесі виробництва. Цей аргумент має силу не тільки для процесу виробництва, а й для подальшої переробки: на підставі отримання та обробки даних з'являється можливість надходження цінної актуальної інформації про виробничий процес та використання її для відповідної оптимізації.

Стандартизація та створення мережі даних полегшують двосторонній обмін інформацією та сприяють ефекту взаємодії між представниками однакових та різних рівнів виробництва, учасників ринку (споживачів) та державних установ. В результаті зростаючого загального тиску конкуренції все більшого значення набуває питання: хто із зацікавлених учасників зможе краще розвинути та використовувати потенціали цифровізації. [1]

Цифрову трансформацію не слід розглядати як самоціль, але як засіб, застосовується з інноваційної оптимізації наявного потенціалу. Вже намічене розмаїття сфер застосування вимагає розробки способів цифрових рішень, орієнтованих на потреби та проблеми,

у тісній прив'язці до практики. Завдання держави має полягати у створенні оптимального нормативного регулювання для розвитку цифровізації та її застосування. Для цього необхідні стабільні та надійні правові основи, як наприклад, дієвий та прозорий закон про захист даних, а також патентне право. Крім того, послуги, які тільки у разі їх централізованого надання за допомогою держави мають економічний сенс, та підтримка є важливими державними завданнями. [2] До цього належать такі заходи, як стимулювання підприємств, які впроваджують інновації, створення певної інфраструктури даних або націлена держпідтримка досліджень та розвитку системи підготовки та підвищення кваліфікації кадрів, орієнтованої на практику [3].

Сільськогосподарське виробництво має свої специфічні особливості, які диктують широке застосування ЦТ, як у жодній іншій сфері народного господарства, це: – участь у технологічному процесі живих організмів, зв'язок режимів роботи технічного обладнання з рослинами, тваринами та людьми, що призводить до випадковим змінам диктуючих параметрів процесу виробництва та невизначеності контролю та управління в об'єктах сільгосп-призначення, різноманітність та складність виробничих процесів, що забезпечуються ЦТ, розподіл контрольованих параметрів по великій площі, випадковий характер їхньої природи, технологічне різноманіття сільгоспвиробництва та культур [2].

Таким чином, основними аргументами на підтримку цифровізації сільськогосподарського виробництва є необхідність виконання наступних проблемних завдань, пов'язаних з нашим відставанням від передових країн світу: збільшення кількості та якості врожаю, мінімізація вкладень капіталу, зниження трудомісткості та підвищення продуктивності сільськогосподарського виробництва, зменшення шкідливого впливу на навколишнє середовище, зниження залежності від людського фактора в сільському господарстві та девіації по урожайності. Цілями є: збільшення вкладу галузі в економіку країни, зростання експортної виручки, створення, диспетчеризація та агрегація потоків даних для створення наскрізних ланцюжків та технологій від виробництва сільгосп-

продукції до споживання з глибокою інтеграцією у суміжні галузі цифрової економіки для підвищення продуктивності праці у сільському господарстві та максимізації прибутку підприємств галузі.

Список використаних джерел:

1. Подольчак Н. Ю., Білик О. І., Левицька Я. В. Сучасний стан цифровізації в Україні. Ефективна економіка. 2019. № 10. URL: http://www.economy.nayka.com.ua/pdf/10_2019/6.pdf

2. Шерстюк Л. М., Нездойминога О. Є. Цифрове сільське господарство: зарубіжний досвід та особливості впровадження й використання в Україні. Економічний, організаційний та правовий механізм підтримки і розвитку підприємництва: колективна монографія; за ред. О. В. Калашник, Х. З. Махмудова, І. О. Яснолоб. Полтава : Видавництво ПП «Астроя», 2019. С. 310–318.

3. Ilchenko, O.; Brusakova, O.; Burchenko, Y.; Yaroshenko, A.; Bagan, Y. The role of a defence industry in the system of national security: a case study. *Entrepreneurship and Sustainability Issues*. 2021. 8 (3). 438–454. [https://doi.org/10.9770/jesi.2021.8.3\(28\)](https://doi.org/10.9770/jesi.2021.8.3(28)).

Prianykova Polina

2nd year Student of the Law Faculty,
Head of the Juridical Scientific
Department Zaporizhzhia National
University, International Human Rights
Defender on AI

Scientific supervisor: Omelianchyk Serhii

Candidate of Legal Sciences, associate
professor, Zaporizhzhia National
University

THE USE OF ARTIFICIAL INTELLIGENCE IN MUNICIPAL LAW, INTER ALIA IN LEGAL SYSTEMS INFLUENCED BY THE ROMAN-GERMANIC LEGAL TRADITIONS

In today's world saturated with novelties and cutting-edge services that appear and are being developed in quantum jumps, miscellaneous spheres are affected and hence, require the relevant amelioration and the regulation thereof. In this scientific article we are going to give prominence to the subject which has evolved from the stage of being futuristically characterized as a 'buzz-word', to the acceptance of its imminent and consequential deployment – Artificial Intelligence (henceforth referred to as 'AI'). The Municipal law has always been considered to constitute a specific connection between the state power and the people's authority per se. Thus, as the social relations have already been given a great impact by the implementation of AI, creating even new and unprecedented public relations, the branch of law aforementioned is being altered and has to be harmonized with the corresponding innovations – this specifies ***the relevance of our scientific work.***

That is why ***the primary purpose of our research*** is to put the emphasis on the enlightening of the changes AI has brought to the Municipal law and highlight the realms it has already been implemented into or may be used in the nearest perspective.

Presentation of the main body of the article. The prevalence of various technologies in modern times is apparent and witnessed these

days. As such processes as digitalization accompanied by the concurrent environmental protection and preservation are gaining their relevance and are considered to be of the paramount importance, many respective strategies and visions of how to face the corresponding issues that arise are being put forward. Besides, on our political and simultaneously economic agenda we encounter with challenges pertaining to the clear understanding of innovations and the provision of the latters' judicious application and hence, some criteria and implications may not have been considered in the aforementioned policies.

Hence, it is vital to put the emphasis on the fact that AI, almost being a ubiquitous and inseparable element of novel digital projects, has to be estimated properly by applying a consequential granular approach – that is one of the aspects enlightened in our previous research [1]. Undoubtedly, the European Union has contributed to define the notion of AI, characterizing it not only from the vista of technology, but as a scientific discipline in particular [2].

From the perspective of information technology, AI represents a sophisticated system or, as prescribed in the European Commission's Proposal for the Artificial Intelligence Act, even a 'family of technologies' which include different learning algorithms able to optimize the functioning of a wide spectrum of spheres and industries, especially the economics is viewed to be provided with an upgrade never known before. Taking into consideration the natural interest of the EU in maintaining high-ranking leadership positions in the branch of technologies, it has adopted measures to achieve its long-term goals and expressed an opinion to provide a pertinent regulation in order to adhere to Union fundamental rights and principles [3]. Beyond the shadow of a doubt, as municipalities are designated for establishing of the direct connection with people, the deployment of novel intelligent systems bears a great impact on the society's level of trust towards the local authorities and the government itself, and, without a question, on the development of the whole area this technological implementation encompasses.

In such a state of affairs, we shall focus on voluminous spheres where AI, as a spark of fire that has remained untamed thus far, burst into.

Advisory case processing. That is how this aspect of AI was named in the corresponding study by the Nordic Council of Ministers [4]. Besides, the Nordic region is also characterized as one of the most digitally advanced in the world, including a well-developed network of municipal institutions. The main aim of the applicable AI technology lies in giving people advice concerning the cases the municipality officers have to solve on a daily basis and make responsible decisions thereon. In the Nordic region, new and less experienced case officers were introduced with such novel tactics first as the municipalities thought that AI could advise them by forming specific algorithms and building its strategy on precedents. However, such procedure may raise a certain controversy. In the event of an excessive reliance on AI which provides the officers with the analysis of previous decisions in cases, eventually, a situation that would lead to the impossibility of the progress on the municipal level may happen, entailing the eradication of individuality and unambiguity. If the aforementioned practice was established and applied in particular, it would become the start of the obsolescence and the increscent emergence of the claw-back provisions that no longer comply with modern realities; in addition, it could result in the decrease of the level of professionalism and competency of municipality's employees and the violation of the EU values.

Hence, in order to strike a balance, provide the people with a just resolution and preserve working spaces that have already been supposed to become affected by the digitalization, municipalities should exclusively have recourse to AI when there is a strong and emergent need to find a specific correlation and conduct a comprehensive review, but on the condition of the retention of critical thinking and the decision being non-detriment to the rule of law. This way, in pursuit of so-called efficiency and mobility, the Municipal law would not forfeit its objectives.

Integrated infrastructures, sustainable and safe mobility, logistics – the basic components of the idea of so-called 'Smart cities' the primary focus thereof is directed on the citizens' needs. One of AI's significant aims for municipalities in the aforementioned concept is to provide the government with an accurate assessment of damage (e.g., its prediction, detection, classification and localization), maintain order on the roads

which comprises strengthened, revitalized and secure transport systems of connected and automated mobility, inter alia resulting in the reduction of overall environmental implications caused by traffic (for instance, decreasing GHG emissions by 90% by 2050) [5]. Hence, the technology would facilitate the level of local stability. Nevertheless, it is worth noting the fact that the relevant legal framework has to be adopted and enacted. Indisputably, some of the EU local communities have already gained benefit from the use of such innovations. For example, Stockholm Municipality deployed AI in order to be proactive in predictions of possible leaks in water and sewer systems, while in Helsinki the technology was tested on its precision on prognosticating the weather and guiding snow ploughs to certain areas with a high probability of snowfall; some similar practices were quite successful [4].

It is vital to highlight that by expanding the scale of such experiments, the situations, conditions and circumstances become more complex, especially when we have no general regulatory act. These mobility and connectivity in systems of transport prescribe the use of automated vehicles as well as their nexus with each other, establishing specific data-centers that would operate and control the traffic as well as the application of drones. However, since the taxonomy of the liability for the use of such machines with AI deployed has not been crystallized and stipulated on the level it has to be, the legal lacuna that arises may lead to such a turn of events when the government, including the municipal representatives, would not be in a position to preserve security and sustainability as the level of cybercrime is increasing and the perpetrators would have a higher possibility to intrude into the data centers and hence, cause mass disturbances, specifically on the cross-border corridors which intrinsically intertwine the novel vehicles. Thus, before implementing such global and promising projects, the mechanisms of security measures' realization should be developed, prescribed and brought into life. The status quo enlightened above would provide the municipalities in particular with certain strategies that would maintain the stability of the world order, guaranteeing the fundamental human rights.

Synthesizing the information enlightened in our scientific research above, it has to be emphasized that the list of aspects we touched upon

is not exhaustive. Moreover, various spheres would definitely undergo crucial changes and be altered taking into account the projects of ‘Smart cities’; and nowadays we may have already become the witnesses of challenges that arise in terms of establishing the liability, guaranteeing data protection, ensuring access to the Internet (hence, safeguarding the right to education, especially during the COVID-19 pandemic) etc. Therefore, for the purposes aforementioned it is necessary to reach an accord between the society and trailblazing technologies by establishing a flexible regulation the provisions thereof would not be declarative, but actual and efficient. In such a state of affairs, miscellaneous legal branches, including the Municipal law would serve the people, comply with modernity and reach a harmony with innovations in the long term.

References

1) Prianykova P., ‘Cybercrime as an obstruction for the deployment of AI into miscellaneous transport systems (the taxonomy of criminal liability for the use of AI is included)’ // Science foundations of modern science and practice. Abstracts of X International Scientific and Practical Conference. Athens, Greece. – 2021. – Pp. 186-193. – URL: <https://isg-konf.com/wp-content/uploads/2021/11/Science-foundations-of-modern-science-and-.pdf> – (Accessed on 27 November 2021).

2) ‘A definition of AI: Main capabilities and scientific disciplines’, High-Level Expert Group on Artificial Intelligence – URL: https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf – (Accessed on 27 November 2021).

3) Proposal for a Regulation of the European Parliament and of the Council (Artificial Intelligence Act) and amending certain Union legislative acts – URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206> – (Accessed on 27 November 2021).

4) ‘Nordic municipalities’ work with artificial intelligence’, Ulf Andreasson and Truls Stende – URL: <https://norden.diva-portal.org/smash/get/diva2:1375500/FULLTEXT01.pdf> – (Accessed on 27 November 2021).

5) Communication from the Commission to the European Parliament and the Council on the EU Strategy for a Sustainable and Smart Mobility – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=pi_com%3AAres%282020%293438177 – (Accessed on 27 November 2021).

ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ У СФЕРІ СОЦІАЛЬНИХ КОМУНІКАЦІЙ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Доронін І. М.

доктор юридичних наук, доцент,
завідувач наукової лабораторії права
національної та міжнародної безпеки
ДНУ «Інститут інформації, безпеки і
права НАПрН України»

ЗАГРОЗИ БЕЗПЕЦІ ТА ПРАВА ЛЮДИНИ В ІНТЕРНЕТІ: ПОШУК БАЛАНСУ

Сучасні дослідники у сфері інформаційного права приділяють суттєву увагу проблематиці інформаційної безпеки та пов'язаним із нею безпековим явищам. До числа зазначених явищ можливо віднести кібербезпеку, військову безпеку і кіберпросторі, «цифрову безпеку» та аналогічні за змістом поняття, з'ясування сутності яких є предметом наукових дискусій. Предметні напрями наукових досліджень у межах спеціальності «Право», визначені як рекомендаційні наказом Міністерства освіти і науки України від 28.12.2018 № 1477, визначають серед них правові основи інформаційної безпеки, організації та діяльності суб'єктів її забезпечення.

Більшість із сучасних дослідників зосередили свою увагу на проблематиці правової регламентації системи державного управління та відповідних державних органів у сфері інформаційної безпеки. Зазначене, зазвичай стосується і контексту забезпечення прав людини. Тобто мова йде про забезпечення або захист прав, що неодмінно досліджується в контексті з'ясування суті відносин «людина-держава». Слід додати, що розуміння прав людини, пов'язаних з інформаційною сферою (прав інформаційного

суспільства, прав у мережі, «цифрових прав» тощо), обов'язково включає до себе доволі широке коло прав, частина з яких поступово легітимізується на рівні міжнародно-правових документів.

Не вдаючись до надмірної деталізації системи прав, можливо зосередитись на доктринальній суті прав людини у сучасному світі. Варто погодитись із розумінням прав людини як доволі складного феномену, що не залишається власне юридичним концептом і потребує трактування як феномену між мораллю та правом [1, с. 59-60]. Водночас, варто визнати, що розуміння суті прав людини можливо тільки в юридичному контексті, в іншому є випадку можливо вести мову лише про передумови цих прав або про суспільну свідомість, яка генерує мораль і виробляє певні підходи до втілення таких проявів. В усякому разі без визнання на рівні права концепт «прав людини» може сприйматись лише як моральний орієнтир, релігійна догма або настанова.

У питанні визначенні цифрових прав можливо спостерігати аналогічний розвиток подій. Певний концепт «свободи» або «права», висловлений у суспільстві та у подальшому – у суспільній свідомості поступово легітимізується у міжнародно-правових документах. Цей процес не є достатньо впорядкованим або ж систематизованим. Мова йде про певні ідеї та погляди, що набувають виду правових приписів, трансформуючись у деяких випадках.

Наприклад, утопічні декларації свободи інтернету та іншої мережевої свободи у кінці 1990 – початку 2000 років були враховані на так званому «романтичному етапі» розвитку міжнародно-правового регулювання інформаційної сфери. Зокрема, Декларація про свободу спілкування в Інтернеті, ухвалена Комітетом міністрів Ради Європи на засіданні 28 травня 2003 року, багато в чому за змістом повторює маніфести анархістів Інтернету (на кшталт «Декларації незалежності кіберпростору» Дж.П. Барлоу 1996 року) [2. 3]. Хоча б тому, що перша і друга статті Декларації визначають, що «країни члени не будуть застосовувати до змісту (контенту) в Інтернет обмеження, що перевищуватимуть аналогічні обмеження по відношенню до інших засобів постачання змісту (контенту)», «країни члени повинні заохочувати саморе-

гуляцію або спільну регуляцію стосовно змісту (контенту) поширюваного в Інтернет». Також згадується, що «державні органи не повинні застосовувати загальне блокування чи засоби фільтрації для відмови у доступі громадськості до інформації та комунікацій в Інтернет, незважаючи на кордони». Теж саме по суті, але в гіперболізованому вигляді стверджував Дж.П. Барлоу.

Але останнім часом зазначені приписи поступово забуваються і країни, що брали участь в ухваленні зазначеної Декларації, змагаються у розробці тих чи інших механізмів обмежень в інтересах боротьби з дезінформацією або «мізінформацією» (неологізм, що означає надання інформації, яка не є неправдивою, але застосовується для «маніпулювання» суспільною свідомістю). Зараз важко чітко визначити хронологічні рамки для зміни підходів, оскільки до російської «гібридної війни» різноманітні обмеження вводились для протидії розповсюдженню ідеології тероризму, пропаганди, злочинів проти неповнолітніх, порнографії і т. ін.

На нашу думку зараз особливої ваги набувають питання пошуку балансу. А саме балансу між правами людини та інтересами, що зумовлюють встановлення певних обмежень. В широкому сенсі мова йде про розуміння «справедливого балансу» між правом та обставинами, що зумовлюють його обмеження (наприклад, інтереси) в термінології рішень Європейського суду з прав людини [4]. Варто зазначити, що в будь-якому разі такий баланс буде сприйматись аксіологічно. На цьому шляху досить важливим є дослідження суті та переліку суб'єктів, що створюють або можуть створювати загрози безпеці.

Так, для прикладу технічне та юридичне розуміння «великих даних» дозволяє зробити висновок про те, що значну їх частину складають «персональні дані» хоча і за умови існування механізмів технічної деперсоналізації при обробці інформації. Враховуючи зазначене, належне дотримання прав людини, у тому числі і захист персональних даних при роботі з «великими даними слід розуміти як сучасний виклик насамперед у сфері захисту персональних даних. Що стосується суб'єктного складу, тобто кола суб'єктів можливого порушення прав, то оскільки технологічно

зазначену інформацію збирають та зберігають в основному недержавні суб'єкти – спеціалізовані компанії в сфері високих технологій, неможливо стверджувати про традиційне сприйняття джерела загроз з боку іноземної держави (групи держав). У сучасному західному науковому дискурсі жваво обговорюються проблеми надмірного зростання приватних компаній у сфері високих технологій, що може створювати загрози соціуму у широкому розумінні. Основні висловлені з цього приводу точки зору стосуються випадків пошуку «загрози Китаю», яке зазвичай сприймається як надмірне розповсюдження могутності інформаційно-комунікаційних компаній КНР шляхом захоплення ринку персональних мобільних пристроїв, що створює передумови для їх використання в інтересах певної держави. На сьогодні фахівці не дійшли однозначного висновку про централізовані дії компаній або уряду КНР щодо несанкціонованого збирання інформації про користувачів мобільних засобів зв'язку та її можливого використання на шкоду іншим державам, але таке сприйняття є усталеним трендом у сучасній політиці [5, 6].

Іншим джерелом загрози є небезпека, яка виходить від новітніх світових економічних гігантів у сфері інформаційних технологій, що є власниками операційних систем, іншого програмного забезпечення, закладів електронної торгівлі, соціальних мереж, тощо [7, 8].

Зазначені джерела перебувають під певним (але обмеженим) впливом держав, водночас дискусії навколо їхньої ролі в обмеженні прав людини є доволі жвавими.

За таких умов потребує певного переосмислення та зміни і підхід до прав людини, оскільки в даному випадку обмежувачем для права буде не суспільний інтерес, виконання державних функцій або загальне явище на кшталт «національної безпеки», а право таких гігантів на вільне підприємництво, оскільки вони не є власне монополістами у розумінні сучасного конкурентного законодавства. Тому зміна підходу до розуміння джерела загроз вбачається як така, що настане неодмінно і спонукатиме до подальших правових наукових досліджень

Список використаних джерел

1. Ломанн Г. Права людини між мораллю і правом// Філософія прав людини. За ред. Ш. Госепата та Г. Ломанна. Київ: Вид-во «Ніка-Центр», 2016. С. 59-86.
2. Барлоу Дж. П. Декларация независимости киберпространства // Криптоанархия. Екатеринбург, УльтраКультура, 2005. С. 61-65.
3. Декларация про свободу комунікацій в Інтернет. Затверджена Комітетом міністрів на 804 засіданні. Страсбург, 23.05.2003. URL: <https://cedem.org.ua/library/deklaratsiya-pro-svobodu-komunikatsij-v-internet/>
4. Блажівська Н. Поняття «справедливий баланс» у практиці Європейського суду з прав людини// Актуальні проблеми правознавства. 2018. Вип. 1 (13). С. 55-62.
5. Tang M. Huawei Versus the United States? The Geopolitics of Exterritorial Internet Infrastructure// *International Journal of Communication*. 2020. 14. P 4556–4577
6. Lee J. The Connection of Everything: China and the Internet of Things// *MERICS*. June, 24. 2021. URL: <https://merics.org/en/report/connection-everything-china-and-internet-things>
7. Zuboff S. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*. 2015. Vol. 30. P. 75–89.
8. Degrippio S. Understanding the information TikTok gathers and stores// *Proofpoint*. 2020. Jan. 8. URL: <https://www.proofpoint.com/us/blog/threat-protection/understanding-information-tiktok-gathers-and-stores>

Фурашев В. М.

кандидат технічних наук, старший науковий співробітник, Перший заступник з наукової роботи ДНУ «Інститут інформації, безпеки і права Національної академії правових наук України НАПрН України»

ІНФОРМАЦІЯ, ІНФОРМАЦІЙНЕ ПРАВО, ЦИФРОВІ ТЕХНОЛОГІЇ: ЗВ'ЯЗОК ТА ВПЛИВ НА СОЦІАЛЬНУ ТРАНСФОРМАЦІЮ

Характерною рисою сучасного часу є намагання зміни організаційних, технічних, технологічних та інших акцентів у всіх складових системи життєзабезпечення людини, суспільства – сферах промислового та сільськогосподарського виробництва, державного управління та надання адміністративних і побутових послуг, охорони здоров'я, безпеки та оборони, освіти та науки, а також інших шляхом максимального використання цифрових технологій. Причому чітко проглядається бажання, зробити все це у максимально короткі терміни, у історичному вимірі часу.

Цілком зрозуміло, заміна, повна або часткова, людської праці автоматизованими, робототехнічними засобами з використанням елементів штучного інтелекту або без їх використання, максимального використання штучного інтелекту та інших досягнень науково-технічного прогресу, “потягне” за собою дуже суттєву, коли не докорінну, зміну суспільних відносин та кваліфікаційних потреб. Багато сучасних професій просто зникнуть, деякі – трансформуються. Лише окремі сучасні професії будуть інтенсивно розвиватися. З'явиться потреба у нових професіях, нових кваліфікаційних знаннях.

Також характерною рисою сучасного часу є всезростаюча роль інформації, інформаційної складової як одного з основних «двигунів» процесів які наразі відбуваються.

Саме інформація формує світогляд людини. Саме інформація формує суспільні відносини. Саме інформація, у сукупності з ін-

шими природними та штучними факторами, формує суспільство та визначає ступінь його єдності. За великим рахунком, саме інформація формує державність та суверенність.

Щодо мови та її зв'язку з інформацією. У людському розумінні, мова є комунікаційним засобом обміну інформацією між живими істотами, показником належності до визначеного кола общини. Це природне.

Але час минає, цивілізаційні процеси не зупиняються. Наука, техніка та технології розвиваються, вдосконалюються, з'являються нові.

Настав час коли виникла потреба встановлення комунікаційного зв'язку між людиною та штучними засобами – чіпами, найпростішими обчислювальними засобами. Людство вирішило цю проблему – виникли такі процеси, як алгоритмизація та програмування. Відповідно, з'явилося поняття «мова програмування» та наука «кібернетика».

Звернемо увагу на поняття «мова програмування», сутність завдання якої є встановлення двостороннього комунікаційно-комунікативного зв'язку «людина – штучний об'єкт («співбесідник», «виконавець»)), тобто обмін інформацією у режимі «завдання (команда) здійснення визначених дій – результати (виконання) здійснення «замовлених» дій та їх відображення», причому у форматі, що сприймається обома сторонами. Як ми бачимо, знов-таки маємо справу з інформацією та її обміном.

Зараз мова йде вже про розробку та впровадження роботів зі штучним інтелектом, які спроможні «спілкуватися» з людиною, тобто обмінюватися інформацією, напрямку, «без посередників» у вигляді зовнішніх комунікативно-комутаційних засобів.

Таким чином, коли ми говоримо про всезростаючу роль інформації, маємо на увазі всіх суб'єктів (природних та штучних) забезпечення життєдіяльності людини, суспільства та держави.

Повертаючись до характерних рис сучасного часу у частині трансформації, здавалося б «сталих», «прогнозуємих» суспільних відносин на всіх рівнях – побутових, міжособистісних, внутрішньодержавних та міждержавних, регіональних та глобальних, від-

носин, необхідно відмітити, що вже зараз спостерігаємо прискорення цих змін. Спробуємо, дуже коротко, окреслити деякі з них.

Глобалізований інформаційний простір разом з відносно простим та зрозумілим доступом до інформації у сукупності із різноманітними легкосприйнятними, навіть дітками віком від 4-5 років, засобами забезпечення цього доступу, привів до того, що значна частина людства, не тільки громадян України, а майже всього цивілізованого світу, вже не уявляє свого існування без цього.

Можливість використання сучасних комунікативних засобів робить зайвим «паперове» листування, за будь-якими приводами, з родинним колом, що не може не позначитися на родинних зв'язках.

Впровадження надання державних та інших управлінських електронних послуг, з одного боку, позитив, а з іншого – остаточно розмежовує державний та інший управлінський апарат та населення. Кожен живе своїм життям лише іноді перетинаючись.

Перелік реальних та майбутніх негативних наслідків від прискореної та всеохоплюючої цифровізації можна продовжувати досить довго. Ясно, на даний час, лише те, що процеси соціалізації людини, формування його світогляду, особливо первісного, все більше і більше переміщуються у кіберпростір. Це – по-перше.

По-друге, роль інформації, яка була окреслена вище, залишилася без змін, але більше відповідальна.

Від якості, спрямованості, об'єктивності та неупередженості, своєчасності та повноти інформації, яка циркулює у кіберпросторі залежить дуже й дуже багато, а саме – мир або війна, розвиток або занепад, стабільність або турбулентність та інше.

Саме тому необхідно більш уважно та прискіпливо відноситися до встановлення та забезпечення чіткого дотримання правил поведінки з інформацією, інформаційних правовідносин.

Зараз час настав, про що свідчать положення Доктрини інформаційної безпеки України (Указ Президента України від 25.02.2017 р. № 47/2017), Стратегії кібербезпеки України (Указ Президента України від 26.07.2021 р. № 447/2021) та Стратегії зовнішньополітичної діяльності України (Указ Президента України від 26.07.2021 р. № 448/2021)

При цьому необхідно згадати, що приблизно у 2007 – 2016 роках був досить активний науковий рух у нагальності та напрямів упорядкування законодавства в інформаційній сфері, інформаційного законодавства. Було проведено досить значна кількість наукових досліджень, захищено не одна докторська та кандидатська дисертація за різними науковими спеціальностями (більшою частиною – за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право). Тобто, фактично, була підготовлена визначена наукова база для розгортання безпосередньої практичної роботи. Але в силу об'єктивних та більше суб'єктивних причин та обставин, подальші дії так й не відбулися. Також необхідно згадати, що питання практичного упорядкування законодавства в інформаційній сфері «вирішується» з 1992 року, незважаючи на неодноразові доручення Президента України, Кабінету Міністрів України, Ради національної безпеки і оборони України.

Цілком зрозуміло що час, який минув з моменту «спаду» інтересу до «наведення законодавчого ладу» у інформаційній сфері, відбулося багато чого як з боку змін у сфері суспільних відносин, так і у сфері правовідносин. Але ці процеси продовжуються, нагромаджуються один на одного, причому зі зростаючим градієнтом.

Цілком зрозуміло, що сьогоденне відношення до законодавчого стану інформаційної сфери фактично зводить нанівець зусилля по підвищенню ефективності правозастосовної та правоохоронної діяльності у цій сфері, а також підготовки висококваліфікованих спеціалістів.

Цілком природно, що така ситуація не може не відобразитися, з урахуванням вищенаведеного, на процесах та ефективності забезпечення національної безпеки, державного суверенітету та їх невід'ємних складових – інформаційної безпеки, кібербезпеки, інформаційного суверенітету країни.

Підсумовуючи можна сказати, що існують необхідні компоненти вирішення піднятого питання – нагальна вимога часу та реальних обставин сучасного стану країни, наукова база та висококваліфіковані спеціалісти та цілі колективи (спеціалізовані наукові

установи), напрацьований та перевірений часом об'єкт упорядкування, окреслені шляхи вдосконалення та подальшого розвитку. Не вистачає лише державного замовлення з відповідними умовами та забезпеченням.

Радзієвська О. Г.

кандидат юридичних наук, старший дослідник, провідний науковий співробітник ДНУ «Інститут інформації, безпеки і права Національної академії правових наук України НАПрН України»

ПРАВА ТА БЕЗПЕКА ОСОБИ В УМОВАХ СОЦІАЛЬНИХ І ЦИФРОВИХ ТРАНСФОРМАЦІЙ

Інноваційний розвиток країни, впровадження нових технологій та активне застосування їх у виробничій, соціальній та управлінській сферах призводить до дедалі більшої цифровізації суспільства та суттєвих змін у суспільних відносинах.

Будь-яка діяльність сучасного суспільства нерозривно пов'язана з інформацією та інформаційними технологіями, відповідно складова інформаційної безпеки сьогодні є досить значимою у будь-якій сфері. Збільшення кількості та частоти інформаційних обмінів виробничого і невиробничого характеру неминуче призводить до підвищення рівня інформаційної небезпеки у суспільстві. Його підсиленню сприяє також підвищення інтенсивності спеціальних інформаційних операцій як складових економічної, політичної та соціальної політики на державному та міжнародному рівнях. При цьому загрози в інформаційному просторі стають дедалі масштабними та наскрізний. Тому система забезпечення інформаційної безпеки в державі вимушена постійно модернізуватися, трансформувати власні підходи і механізми протидії інформаційним небезпекам, пристосовуючись під нові виклики глобального інформаційного простору.

Останнім часом в Україні спостерігається розуміння важливості питань забезпечення інформаційної безпеки. Лише протягом цього року було прийнято низку нормативно-правових актів щодо забезпечення інформаційної безпеки. Однак багато питань все ще залишаються поза правовим полем нашої держави.

Особливо гостро сьогодні постають питання правового забезпечення захисту приватності особи та її персональних даних. Підвищення кількості та частоти цифрових комунікацій у суспільстві, а також збільшення електронних комунікацій між державою та громадянином, у тому числі і надання певних послуг через спеціалізовані додатки, підвищує ризики для інформаційної безпеки людини. Концентрація великої кількості персональних даних на незахищеному носії інформації, як то смартфон, підвищує ризик несанкціонованого доступу до них та неправомірного використання.

Актуальними залишаються питання використання даних користувачів соціальних мереж. Великі дані (BIG DATA), зібрані за допомогою файлів cookies, формують цифровий профіль суб'єкта комунікацій. Автоматично сформовані дані про користувача, його вподобання, інтереси, зібрані методом аналізу його діяльності в мережі, разом з поширеною ним же інформацією про себе, у тому числі фото, відео, становлять живий інтерес для бізнесу, політики, соціальних та комерційних проектів. Такий профіль стає надзвичайно цінним ресурсом для будь-якої компанії. Найбільш часто великі дані (BIG DATA) використовуються у сучасному маркетингу для створення персоналізованої (таргетованої) реклами та у політичних перегонах. Виникають суттєві запитання щодо правомірності процесів автоматичного збирання та використання даних про особу системою, а також щодо змісту самих даних.

З однієї сторони, жодним нормативно-правовим документом України така інформація про людину не ідентифікована як персональні дані. Тоді як в Європейському Союзі інформація, зібрана з допомогою файлів cookies, вважається персональними даними відповідно до Загального регламенту щодо захисту даних 2016/679 (GDPR) [1] та Директиви про обробку персональних да-

них та захист конфіденційності в секторі електронних комунікацій 2002/58/EC (ePrivacy Directive) [2]. Таке роз'яснення стосовно цього питання були надані European Data Protection Board за рішенням у справі Vidal-Hall v Google Inc. [3].

Також виникають сумніви у питаннях щодо дотримання правових норм та порядку дій при збиранні та використанні даних про користувача мережі Інтернет у відповідності до Закону України «Про захист персональних даних» [4]. Процедура отримання згоди користувача на обробку його персональних даних у мережі сьогодні є досить формальною, а інформування суб'єкта персональних даних про порядок обробки даних, володільця персональних даних, склад і зміст зібраних персональних даних, права, мету збору, а також про осіб, яким буде передано персональні дані є недостатньою. Повторне отримання згоди суб'єкта персональних даних на обробку його персональних даних при зміні мети обробки персональних даних, як правило, взагалі не здійснюється. Що є прямим порушенням Закону України «Про захист персональних даних» [4].

Сама технологія персоналізованої реклами є нічим іншим, як нав'язуванням окремого товару, послуги чи думки, і одним із видів інформаційно-психологічного впливу на свідомість людини. Такі дії порушують право особи на захист від маніпулювання свідомістю, право на захист від недостовірної інформації, а також ставить під загрозу повноцінність реалізації ним права вибору. Також відкритими залишаються питання правомірності використання персоналізованої (таргетованої) реклами в мережі в аспекті порушення права особи на приватність.

Надзвичайно популярним сьогодні є використання відеоспостереження в громадських місцях у різних містах України. Зокрема, на кінець 2020 року лише в місті Києві функціонували понад 6 тисяч камер відеоспостереження в громадських місцях, серед яких є ті, що мають функцію детектування обличчя. Доступ до матеріалів, зібраних камерами відеоспостереження, крім уповноважених органів місцевої влади мають також правоохоронні органи в межах своїх повноважень. Встановлення камер відеоспостереження

в громадських місцях на думку правоохоронців знижує рівень злочинності. У тестовому режимі перебуває система розпізнавання обличчя в режимі реального часу (LFR). Ця технологія обробки біометричних даних побудована на автоматичному розпізнаванні особи за цифровим зображенням її обличчя з подальшою ідентифікацією через профіль, який зберігається в базі даних у форматі фото та відео, у режимі реального часу.

У рамках контролю за додержанням законодавства про захист персональних даних Департаментом у сфері захисту персональних даних Уповноваженого Верховної Ради України з прав людини у першому півріччі минулого року було проведено низку перевірок дотримання вимог законодавства про захист персональних даних під час здійснення відеоспостереження в громадських місцях м. Києва та подальшої обробки отриманих таким чином персональних даних. За результатами перевірок комунальних підприємств «Інформатика», «Київський метрополітен», Департаменту інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації) виявлено низку порушень законодавства про захист персональних даних. Серед основних – неповідомлення суб'єкта персональних даних про його права, визначені частиною другою статті 8 Закону України «Про захист персональних даних» [4] під час здійснення відеоспостереження, а також відсутність або неналежне оформлення документів, якими визначаються процедури обробки та захисту персональних даних. Про це йдеться в оприлюднених результатах перевірок дотримання вимог законодавства у сфері захисту персональних даних в рамках здійснення відеоспостереження [5].

Тому питання використання відеоспостереження в громадських місцях у рамках забезпечення правопорядку в містах України також викликає суттєве занепокоєння у питаннях реалізації права особи на приватність та захисту її персональних даних.

Підсумовуючи, хочеться зазначити, що соціальні та цифрові трансформації, що відбуваюся нині, потребують оперативного реагування правової системи держави задля забезпечення ефективного правового регулювання суспільних відносин в усіх без ви-

ключення сферах. Питання забезпечення інформаційної безпеки є сьогодні вкрай актуальними. Водночас, грань між забезпеченням безпеки та правами і свободами в інформаційній сфері надзвичайно тонка. Потрібні дуже чіткі маркери та критерії для виявлення і нейтралізації інформаційних небезпек, здатних завдати суттєвої шкоди особі, суспільству та державі, при одночасному дотриманні демократичних принципів забезпечення реалізації основоположних прав та свобод людини і громадянина.

Література:

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

2. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) *Official Journal L 201, 31/07/2002 P. 0037 – 0047*. URL: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058>

3. Vidal-Hall v Google Inc. [2015] EWCA Civ 311. URL: <https://www.judiciary.uk/wp-content/uploads/2015/03/google-v-vidal-hall-judgment.pdf>

4. Про захист персональних даних: Закон України від 1 червня 2010 р. // База даних Законодавство України / ВР України. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

5. Результати перевірок дотримання вимог законодавства у сфері захисту персональних даних в рамках здійснення відеоспостереження, зокрема під час функціонування комплексної системи відеоспостереження міста Києва. URL: <https://ombudsman.gov.ua/ua/all-news/pr/rezultati-perev%D1%96rok-dotrimannya-vimog-zakonodavstva-u-sfer%D1%96-zaxistu-personalnix-danix-v-ramkax-zd%D1%96jsnennya-v%D1%96deosposterezhennya,-zokrema-p%D1%96d-chas-funkcz%D1%96onuvannya-kompleksno%D1%97-sistemi-v%D1%96deosposterezhennya-m%D1%96sta-ki%D1%94va/>

Заславська Л. В.

науковий співробітник ДНУ «Інститут
інформації, безпеки і права НАПрН
України»

ЦИФРОВА ЕРА: НОВІ МОЖЛИВОСТІ ТА НОВІ ВИКЛИКИ ДЛЯ ЛЮДИНИ І СУСПІЛЬСТВА

Немає сумніву у тому, що світ цифрових технологій, в який ми входимо, – це не лише новий логічний етап розвитку технологічної сфери людства, а й усієї існуючої правової та соціально-політичної реальності. Поки що не достатньо загальноприйнятих і гармонізованих визначень та правових дефініцій у цій сфері, однак цифрові технології стрімко розвиваються. Цифровізація (англ. digitalization) стає найважливішим фактором економічного зростання економіки будь-якої країни і взагалі є сучасним трендом розвитку.

Впровадження в життя будь-яких нових технологій, зокрема цифрових – процес, безумовно, тривалий і несе в собі масу невідомих ще викликів та небезпек для людства.

Із точки зору безпеки, будь-який вид електронної комунікації виключно вразливий, оскільки за допомогою технічних засобів з комп'ютерів можна зняти будь-яку інформацію. Існують, звичайно, способи захисту, але стовідсоткової гарантії, що вони спрацюють, немає. Загрозою є не тільки те, що спецслужби країн світу сьогодні здатні підключатися й «знімати» за допомогою технічних засобів інформацію навіть із оптоволоконних (цифрових) кабелів. Вільний ринок технічних засобів цифрової електроніки, на жаль, надає доступ до величезних обсягів даних через сучасні мережі комунікації іноземним розвідкам та кримінальним структурам, що постійно продукує все нові загрози і виклики. Добуваючи інформацію, державні і приватні спецслужби досягли такого рівня, що здатні «зламувати» не лише канали зв'язку, комп'ютерних мереж, але й людський мозок. Технічно їм для цього потрібні лише дві речі: велика обчислювальна потужність – певний обсяг персональних даних, зокрема, біометричних. До сьогоднішнього дня

ні в кого, крім спецслужб, не було такої мотивації, однак ситуація змінюється через поліпшення ефективності машинного навчання, штучного інтелекту, розвитку психології, біології, зокрема нейробіології, необхідних для розуміння, як працює людський мозок. За таких умов виникає необхідність забезпечення безпеки основних інструментів цифрової економіки – захист електронних підпису, платежів, токенів, sim-карт, online-сервісів, захис тінформації в електронних хмарах, базах даних, розвиток криптографії і технологій аутентифікації особи, захист системи електронного документообігу, каналів передачі інформації, захист серверів, безпека діяльності комерційних і державних електронних майданчиків, захист від загроз впливу через інформаційні канали на літальні апарати, зброю, транспорт, новітні технології тощо. [1]

Таким чином, у зв'язку із швидкими темпами цифрового розвитку перед людством постала проблема як технічного так і правового захисту інформації. Інша загроза, що виникла при переході на «цифру» – це швидкі темпи скорочення числа висококваліфікованих працівників, нестача працівників робочих спеціальностей, безробіття, низька здатність до навчання новітнім технологіям працівників більш старшого віку. Саме тому у зв'язку з роботизацією робочих місць, автоматизацією управлінських процесів, зростаючим застосуванням 3D принтерів суттєвою загрозою вважається зростання безробіття, що може призвести до порушення прав людини на працю (статті 43 Конституції України).

Україна є найбільшим у світі експортером агентів цифрової економіки. На Заході попит на таких фахівців величезний. Тільки в Європі щороку потрібно близько 100 000 інженерів. З 17000 інженерів, які сьогодні випускають українські ВУЗи – майже 10 000 – це потенційні емігранти. Вже зараз економіка стикається з гострою нестачею фахівців інженерного профілю. У випадку якщо державна політика у сфері інформаційних технологій не зміниться, і в її основі лежатиме імпорту техніки, технологій і програмного забезпечення, то ефект може виявитися негативним. Вивільнені «білі комірці» можуть не знайти собі нового фаху, як через відсутність належної кваліфікації, так і внаслідок заповнювання

зростаючих сегментів ринку імпоротною технікою та іноземними фахівцями. Проте для українського ринку праці наслідки економічної політики, що наразі здійснюється, ще довго будуть набагато більш значущими, ніж цифрова революція. Внаслідок різкої деградації економіки у зв'язку з її реформуванням за рецептами МВФ знищуються цілі галузі промисловості з мільйонами високотехнологічних робочих місць. При цьому всупереч загальносвітовим тенденціям найбільш різкого скорочення зазнають саме виробництва сучасного технологічного укладу, що забезпечують розширення зайнятості. Україна залишається єдиною країною в світі, де швидкими темпами скорочується число висококваліфікованих працівників. Більшість з них змушені перейти на низько кваліфіковану роботу або емігрувати.[2]

Зі спалахом коронавірусної хвороби COVID-19 набагато очевиднішими стали ризики посилення нерівності в Україні і проблема цифрового розриву серед населення.

Хоча завдяки сучасним технологіям, як-от застосунки для проведення відеоконференцій і швидкісному інтернету, віддалена робота – реальна і цілком прийнятна альтернатива для офісних працівників, але чимало професій доволі складно перевести в онлайн режим.

У режимі ізоляції багатьом українцям складно адаптуватися до нових викликів – чи то через брак цифрових навиків, чи просто через обмежений доступ до інтернету.

Пандемія коронавірусу змушує інституції, бізнеси і людей швидко опанувати цифрові технології. А ось ті, хто не встигають пристосуватися до нового способу ведення справ, ризикують залишитися в невигащному становищі.

За оцінками Торгово-промислової палати України, через введення карантину понад півмільйона людей втратили роботу. Скільки з них мають усе необхідне, щоб почати працювати з дому?

А як щодо тих, кому бракує цифрових навичок, щоб використовувати цифрові рішення, або тих, у кого немає базових інструментів, необхідних для застосування таких рішень? Чи в кожному домі є комп'ютер, планшет або смартфон? Чи кожен дім в Україні підключений до інтернету?

Перехід до роботи онлайн неминучий, і для більшості людей це вже відбувається. Проте доступ до технологій і зв'язку залишається перешкодою для багатьох спільнот в Україні. Наприклад, ми знаємо історії з невеличких сіл, де державні службовці працюють позмінно під час карантину, бо «ми не можемо забрати додому таку кількість документів».

У сільських школах навчальний процес зупинився – через поганий зв'язок і відсутність гаджетів серед найбільш вразливих і бідних груп населення або ж через те, що громада поблизу «лінії зіткнення» на сході України не може дозволити собі заплатити 5 тис. гривень за швидкісний інтернет, а отже – не може скористатися вищезгаданими ініціативами. Це все приклади цифрового розриву, і вони вимагатимуть скоординованої відповіді всього суспільства, щоб запобігти поглибленню нової – цифрової – нерівності в наших суспільствах.

Цікаве питання виникає і при запровадженні державою застосунку «Дія» – «Цифрова держава». А чи всім категоріям доступний цей застосунок? Чи кожен громадянин країни має смартфон, має необхідні знання та навички щоб користуватися цими державними послугами? Виходить так, що великій аудиторії громадян країни ця державна послуга не доступна.

Отже, запровадження цифровізації в сучасному суспільстві – це важливий крок вперед та нові можливості розвитку в усіх сферах життєдіяльності. Проте слід зважувати й на те, що перед людством можуть постати невідомі виклики та загрози внаслідок швидких темпів розвитку електронної ери.

Література

1. Цифровізація як нова реальність України. [Електронний ресурс] – Режим доступу: <https://lexinform.com.ua/dumka-eksperta/tsyfrovizatsiya-yak-nova-realnist-ukrayiny/>
2. Дві сторони цифрових технологій: «цифрова диктатура» або збереження стійкості [Електронний ресурс] – Режим доступу: <https://razumkov.org.ua/statti/dvi-storony-tsyfrovykh-tekhnologii-tsyfrova-dyktatura-abo-zberezhennia-stiikosti>

Еннан Р. Є.

кандидат юридичних наук, доцент,
магістр інтелектуальної власності,
доцент кафедри права інтелектуальної
власності та патентної юстиції
Національного університету «Одеська
юридична академія»

КУЛЬТУРНА СПАДЩИНА У ЦИФРОВОМУ СЕРЕДОВИЩІ: ОСОБЛИВОСТІ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ МУЗЕЙНОЇ ДІЯЛЬНОСТІ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Глобальна інформаційна мережа Інтернет і електронна комерція справляють величезний вплив на традиційні засоби охорона прав інтелектуальної власності, що використовуються в країнах, які розвиваються, а також на охорону та поширення об'єктів інтелектуальної власності, належних правовласникам, при їх виході на тепер відкритіші світові ринки. З огляду на це, Всесвітня організація інтелектуальної власності (ВОІВ) розробляє проекти, покликані надавати допомогу при використанні культурної та художньої спадщини країнам, які розвиваються, на основі застосування цифрових технологій у середовищі Інтернет.

Проект ВОІВ щодо музеїв і галерей є одним з прикладів роботи в цьому напрямі. Водночас деякі країни, що розвиваються, можуть не побажати розгортати повністю технологію електронної комерції для цих цілей, побоюючись, що їхні об'єкти інтелектуальної власності можуть зазнати ризику порушення через їх доступність у світовому цифровому середовищі. Розробка міцної правової основи для об'єктів інтелектуальної власності та сприяння обговоренню таких питань, як безпека, технологія шифрування (кодування), забезпечення конфіденційності, охорона прав споживачів і питання вирішення спорів покликані, зокрема, зняти ці побоювання та заохотити країни, що розвиваються, активніше використовувати можливості електронної комерції.

Музеї та галереї відіграють важливу роль у зборі, збереженні, експонуванні й поширенні культурної та художньої спадщини світу. Вони забезпечують збереження культурної цілісності й різноманітності, виконують свою місію, виставляючи свої колекції на огляд публіки як у межах країни, так і на міжнародному рівні. Дотепер музеї для виконання своїх функцій займалися веденням і утриманням «фізичних» об'єктів у своїх колекціях, використовуючи для цього традиційні засоби. З розвитком цифрових технологій культурна спадщина, що зберігається в музейних колекціях, які зазвичай складаються з манускриптів, фотографій, картин, скульптур і предметів культури, може бути представлена в цифровій формі (оцифрована) та поширюватися в цифровій формі з використанням нових носіїв і мережевих каналів. Оцифрування припускає створення цифрових зображень, відтворених з музейних колекцій. Як тільки з твору «знімають» цифрову копію, остання може передаватися каналами мережі Інтернет або безкоштовно, або за ліцензією з використанням технічних засобів захисту.

Оцифрування зображень музейних експонатів крок багатонадійний, особливо для країн, які розвиваються, – у сенсі сприяння економічному розвитку, проведенню академічних і наукових досліджень, а також підготовці кадрів. Воно дає музеям можливість вести та використовувати свої колекції культурних і художніх об'єктів, заохочуючи обмін знаннями та поширення знань про світову культуру. Створення цифрового архіву може допомогти зберегти національну культурну спадщину та надати стимул представникам мистецтва для подальшої творчості, забезпечуючи їм доступ до культурної спадщини попередніх поколінь. Інтернет пропонує музеям, зокрема й невеликим, регіональним і спеціалізованим, а також галереям, унікальну можливість, досі майже незвідану, експонувати культурні багатства будь-якому зі світової спільноти, в кого є доступ до комп'ютерної мережі.

Однак процес викладення оцифрованих зображень музейних експонатів в онлайн-доступ може бути пов'язаний з необхідністю значних інвестицій і ставить перед музеями, що є зберігачами культурної спадщини, певні ризики. Музеї, що побажали ви-

ставити свої колекції онлайн, мають спочатку здійснити обробку своїх творів для отримання електронних зображень. Оцифрування може виявитися дорогим і технічно складним процесом, до того ж, виникають супутні витрати, пов'язані з необхідністю вивантаження та підтримки цих зображень в онлайн-доступі для широкої громадськості. Представлення експонатів у цифровій формі також висуває на перший план клопоти щодо належного забезпеченню охорони прав інтелектуальної власності. Це часом відлякує тих, хто в інших випадках радо вітає використання нових технологій. Ситуація ускладнюється також тією обставиною, що нині в багатьох музеях діють адміністративні процедури, розроблені під використання та поширення друкованих форм публікації, вони не передбачають можливості використання цифрових зображень творів. Отож для проведення оцифрування експонатів музеї мають з'ясувати, чи досить їм наданих прав для виготовлення репродукцій у цифровій формі. Своєю чергою, таке виготовлення може привести до відмінностей в інтерпретації обсягу угод між музеями й авторами творів. Отож важливо, щоби музеї розуміли ці питання та, відповідно, могли здійснювати контроль за підтримкою і використанням своїх цифрових колекцій задля мінімізації пов'язаних з цим ризиків.

Розробку проектів цифрових музеїв гальмує і відсутність досвіду, міжнародних норм та стандартів у цій сфері. Крім цього, відсутні типові ліцензійно-договірні документи для надання об'єктів культури в онлайн-доступ. Здійснення проектів з оцифрування музейних об'єктів зачіпає низку політичних, технічних і фінансових питань, які необхідно вирішити до того, як зображення музейних об'єктів будуть надані для доступу в цифровому середовищі.

Зважаючи на такі труднощі, деякі установи, що мають справу з культурною спадщиною, розробили нові проекти для здійснення ліцензування своїх колекцій, що експонуються в режимі онлайн, за участю декількох музейних об'єднань. Наприклад, Консорціум художніх музеїв (AMICO) є неприбутковою організацією, що має базу даних із близько 100 000 оцифрованих творів мистецтва, отриманих від 30 музеїв Північної Америки. На більшість таких

творів є ліцензії на використання у навчальних закладах з дослідницькою чи навчальною метою. Музеї та архів Каліфорнійського проекту (МОАС), що працюють у режимі онлайн, надають безкоштовний доступ до понад 150 000 зображень, отриманих з 11 публічних і приватних музеїв, бібліотек, архівних колекцій Каліфорнії. Ще одним прикладом цифрового подання є онлайн-колекція Ермітажу в Санкт-Петербурзі. Музей Ермітаж експонує свою цифрову колекцію безкоштовно тільки для особистого користування. Щоб відстежувати, яким саме чином використовуються цифрові зображення, в останні інкорпоровані невидимі цифрові водяні знаки.

ВОІВ вивчає можливість реалізації проекту, присвяченого музеям, який має на меті допомоги музеям країн, які розвиваються, забезпечити доступ в режимі онлайн до зображень з їхніх колекцій культурної спадщини та супутньої інформації для комерційних, навчальних і соціальних цілей. Проект спрямований на дослідження питань охорони прав інтелектуальної власності, їхніх правових і адміністративних аспектів, що має допомогти виробити систему експонування цифрових зображень об'єктів культури в цифрових мережах. Проект також спрямований на виявлення та розробку необхідних технологій, покликаних забезпечувати й регулювати доступ до колекцій, ідеться, зокрема, про технічні заходи захисту зображень від незаконного копіювання й маніпулювання, що зазвичай вбудовані в загальну систему управління електронними зображеннями в цифровому середовищі. Такі нові системи мають бути інтегровані з уже наявними системами управління музейними колекціями. Необхідно виявити групи потенційних користувачів, для яких належить визначити відповідні умови та вимоги доступу, зокрема: університети, академічні й дослідницькі заклади, загальноосвітні школи, періодичні видання, індивідуальні користувачі.

На початковій стадії реалізації цього проекту ВОІВ надавала консультативну допомогу з питань інтелектуальної власності установам культурного призначення, розташованим у країнах-учасниках ВОІВ. Крім цього, в 2001 році був опублікований аналіз,

проведений Міжнародним інститутом інтелектуальної власності, «Управління фондом музейних об'єктів у цифровій формі: довідковий посібник з управління музейними ресурсами». Цей проект планується інтегрувати в глобальну інформаційну мережу інтелектуальної власності WIPOnet, яка дозволяє музеям, що беруть участь у цьому проекті, розташовувати свої онлайн-колекції на серверах, підтримуваних мережею WIPOnet. Отож у BOiB з'являється унікальна можливість надавати експертну допомогу таким музеям і покращувати мережевий доступ до їхніх колекцій, а також сприяти країнам, які розвиваються, в забезпеченні охорони та підтримці своїх культурних і художніх цінностей, застосовуючи систему інтелектуальної власності, реалізовану в цифровому середовищі.

Борисов О. Ю.

магістр права, аспірант ДНУ

«Інститут інформації, безпеки і права
Національної академії правових наук
України», адвокат

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БАЛАНСУ МІЖ ІНТЕРЕСАМИ ЛЮДИНИ, СУСПІЛЬСТВА ТА НАЦІОНАЛЬНОЇ БЕЗПЕКИ В УМОВАХ АКТИВНОГО РОЗВИТКУ І ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ

XXI століття стало добою безпрецедентного технологічного стрибка у сфері інформаційних технологій. Так, інтенсивність прогресу в цій сфері поступово наростала вже протягом минулого століття, і в наш час вже беззаперечно можна сказати, що найближче майбутнє людства, вирішення глобальних проблем і розвиток чи не всіх сфер життєдіяльності суспільства будуть нерозривно пов'язані із застосуванням інформаційних технологій, розвитком Інтернету речей, штучного інтелекту тощо.

Безумовно, одним з найбільш вагомих і, без перебільшення, доленосних досягнень науково-технічного прогресу в сфері ін-

формаційних технологій стала поява мережі Інтернет та стрімкий розвиток як самої мережі, так і її інфраструктури, супутніх ринків технологій та послуг.

Результатом такого процесу стало небачене раніше розширення можливостей доступу людини до інформації. Так, за даними Міжнародного союзу електрозв'язку, станом на кінець 2019 року доступ до мережі Інтернет мало трохи більше за 51% населення планети, що складає близько 4-х мільярдів осіб, і ці показники невинно зростають.

Разом з тим, невинно розширюються і можливості впливу на свідомість окремо взятої людини або групи людей, в тому числі і з метою соціальної дестабілізації певного регіону або держави. Іншими словами, сучасні цілком звичні, побутові інформаційні технології можуть бути використані для організованої інформаційної агресії як всередині окремої держави, так і на міждержавному рівні.

Єдиним абсолютним захистом від використання інформаційних технологій в цілях інформаційної агресії сьогодні є повна ізоляція інформаційного простору, що захищається, від зовнішніх контактів, а також тотальний контроль за ним. Саме такий шлях забезпечення інформаційної безпеки було обрано Північною Кореєю, значною мірою він реалізується Російською Федерацією, окрім цього, в якості тимчасового безпекового заходу відключення інформаційних мереж було використано Азербайджаном в початковий період загострення воєнного конфлікту із Вірменією в районі Нагорного Карабаху в 2020 році.

Водночас, подібний спосіб захисту не може бути застосовано на постійній основі сучасною правовою, демократичною, соціальною державою, адже як міжнародне, так і національне законодавство сучасних розвинутих держав закріплює за людиною і широко регламентує ряд прав і свобод, пов'язаних з доступом до інформації.

Так, у ст. 19 Загальної декларації прав людини сказано: *«Кожна людина має право на свободу переконань і на вільне вираження їх; це право включає свободу безперешкодно дотримуватися своїх*

переконань та свободу шукати, отримувати та поширювати інформацію та ідеї будь-якими засобами та незалежно від державних кордонів» [2].

У ч. 1 ст. 10 Конвенції про захист прав людини і основоположних свобод сказано: *«Кожен має право на свободу вираження поглядів. Це право включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів. Ця стаття не перешкоджає державам вимагати ліцензування діяльності радіомовних, телевізійних або кінематографічних підприємств» [3].*

Водночас, тут же ч. 2 ст. 10 Конвенції про захист прав людини і основоположних вказує на можливість обмеження права на свободу вираження поглядів: *«Здійснення цих свобод, оскільки воно пов'язане з обов'язками і відповідальністю, може підлягати таким формальностям, умовам, обмеженням або санкціям, що встановлені законом і є необхідними в демократичному суспільстві в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров'я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і безсторонності суду».*

Національним законодавством України також закріплюється право кожного на свободу думки і слова, на вільне вираження своїх поглядів і переконань.

Так, зокрема, ст. 34 Конституції України передбачає таке: *«Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір...»*

При цьому тут же в статті зазначено: *«Здійснення цих прав може бути обмежене **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 запобіган-*

ня розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя» [1].

Частина ж 1 ст. 17 Конституції України встановлює, що: «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу».

Відтак, з положень Конституції України слідує, що інформаційна безпека держави має вищий пріоритет, ніж права та інтереси окремої людини чи групи людей.

Україна дійсно має досвід застосовування правових механізмів, зокрема, для блокування доступу населення до веб-ресурсів і припинення діяльності телевізійних каналів, що можуть нести загрозу національній безпеці України.

Так, наприклад:

1) 15 травня 2017 року Указом Президента України від 15.05.2017 № 133 було уведене в дію рішення РНБО України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)», згідно з яким на території України було заблоковано роботу ряду російських веб-ресурсів, зокрема соціальної мережі «ВКонтакте». 14 травня 2020 року Указом Президента України Володимира Зеленського №184 ці санкції було продовжено [4].

2) Указом Президента України від 02.02.2021 № 43/2021 було уведене в дію рішення РНБО України від 2 лютого 2021 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)», яким було обмежено діяльність ряду національних телеканалів [5].

У наведених прикладах право на свободу слова було обмежено, серед іншого, в інтересах інформаційної безпеки України.

Разом з тим, слід пам'ятати, що пріоритетність інтересів інформаційної безпеки держави не скасовує необхідність додержання решти вимог Конституції України й забезпечення гарантованих нею прав і свобод завжди і всюди, коли це тільки можливо.

Більше того, як видно із положень ст. 34, Конституція України на разі допускає обмеження свободи слова винятково законом. Від-

так, обмеження указами Президента України функціонування на території України ряду веб-сайтів і телевізійних каналів було здійснено в порушення порядку, встановленого Конституцією України.

І якщо практика обмеження прав і свобод людини в інтересах національної безпеки може бути розумно обґрунтована і виправдана, то практика порушення вимог Конституції України є неприпустимою за жодних обставин, оскільки підриває основи державності та правопорядку.

Більше того, здійснення правового регулювання в інформаційній сфері переважно за допомогою заборони як способу правового регулювання може дестабілізувати соціальну обстановку в державі, знизити авторитет державної влади.

За таких обставин неабиякої актуальності набуває питання забезпечення балансу між інтересами держави у сфері забезпечення її національної, в тому числі інформаційної, безпеки і правами та інтересами людини в інформаційній сфері.

З огляду на викладене, можемо дійти висновку, що для забезпечення ефективного правового регулювання у сферах обігу інформації та забезпечення інформаційної безпеки України необхідним є розумне і збалансоване поєднання різних способів правового регулювання: дозволу, заборони і зобов'язання.

При цьому додержання законності має бути непорушною аксіомою правового регулювання в цій сфері, оскільки безпосередньо впливає на соціальну стабільність, на єдність і цілісність суспільства і держави.

Окрім зазначеного, для забезпечення ефективного і збалансованого правового регулювання у сфері обігу інформації та забезпечення інформаційної безпеки України доцільними є такі заходи:

- 1) здійснення інвентаризації, впорядкування і послідовного вдосконалення національного законодавства обігу інформації та забезпечення інформаційної безпеки України; вдосконалення відповідних правових режимів;

- 2) розробка базового нормативно-правового акту (типу Стратегії) у сфері інформаційної безпеки, яким би закріплювалась загальна концепція забезпечення інформаційної безпеки України з

урахуванням необхідності збалансованого правового регулювання в інформаційній сфері;

3) розробка і запровадження правових механізмів обмеження свободи слова в інтересах інформаційної безпеки України, які б дозволили одночасно забезпечити оперативність, обґрунтованість і законність відповідного правового втручання держави;

4) розробка і включення до навчальних програм як загальної середньої, так і вищої освіти навчальних дисциплін, які б передбачали навчання поводженню з інформацією в сучасних умовах;

5) активне залучення національних наукових спроможностей для роботи над вдосконаленням правового регулювання в інформаційній сфері.

Список використаної літератури:

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

2. Загальна декларація прав людини. Режим доступу: https://zakon.rada.gov.ua/laws/show/995_015#Text

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

4. Указ Президента України від 15.05.2017 № 133. Режим доступу: <https://www.president.gov.ua/documents/1332017-21850>

5. Указ Президента України від 02.02.2021 № 43/2021. Режим доступу: <https://www.president.gov.ua/documents/432021-36441>

Нагнибіда А. В.

студент Хмельницького університету
управління та права імені Леоніда
Юзькова

ПОНЯТТЯ І ЗМІСТ ЦИФРОВОГО СУВЕРЕНІТЕТУ ДЕРЖАВИ В СУЧАСНОМУ ПРАВІ

В сучасному світі, в період цифровізації, де технології все більше набувають популярності та розвиваються з космічною швидкі-

стю, державі дуже важливо забезпечити незалежність та самостійність інформаційного поля. Вільний обмін цифровими даними, їх вільний обіг та поширення з допомогою мережі Інтернет зумовлює потребу в конфіденційності та захисті такої інформації. Надто важливим з точки зору національної безпеки є захист інформаційного поля. Для України, як країни на території якої тривають активні військові дії, це питання набуває особливого значення. Саме тому сьогодні все більш вагомою та актуальною стає концепція інформаційного (цифрового) суверенітету держави.

Серед великої кількості літератури та різних джерел, зокрема зарубіжних, найбільш загальне визначення цифрового суверенітету наступне: «цифровий суверенітет є ключовою ідеєю епохи Інтернету – ідея, що сторони повинні мати суверенітет над своїми цифровими даними» [1]. Як бачимо при цьому не розкривається сутність цього поняття та його властивості. Тому для його розуміння, розглянемо перш за все поняття суверенітету держави. Як відомо, поняття суверенітету досить широке і існує досить багато визначень цього поняття. Суть їх загалом полягає в незалежності та самостійності держави у прийнятті будь-яких рішень, без стороннього впливу, натиску та примусу. Згідно поширеного академічного визначення **«суверенітет держави – її незалежність і самостійність у здійсненні внутрішньої та зовнішньої політики»** [2]. Наведене типове визначення суверенітету, пов'язане швидше з окресленням меж суверенітету, як правило, кордонами держав, певними географічними параметрами та владою. Однак, розгляду якщо говорити про суверенітет інформаційний, то слід зазначити, що сучасні технології поширення інформації, потужні інформаційні обміни в рамках уже сформованого глобального інформаційного простору сьогодні значною мірою нівелюють територіально-географічні особливості суверенітету як такого [3].

В електронних західних джерелах визначення цифрового суверенітету розглядається як здатність контролювати свою власну цифрову долю – дані, апаратне та програмне забезпечення, на які ви покладаетесь і які створюєте.» [4], На перший погляд, термін «суверенітет» над частинами Інтернету може здатися абсолютно

недоречним. Адже однією з передумов визнання суверенітету держави в міжнародному праві є здійснення влади над територією. Ендрю Вудс обґрунтовує своє визначення «суверенітету даних» на трьох основних елементах державного суверенітету: «має верховний контроль над всією територією країни та незалежний від інших суверенів». Протиріччя між поняттям «цифровий суверенітет» та територіальною основою суверенітету зникає, коли ми усвідомлюємо, що для здійснення контролю над будь-якою територією все більше необхідно здійснювати контроль за онлайн-діяльністю, доступною на цій території. Це розуміння поєднує місце і кіберпростір [5].

Таким чином, співвідношення «традиційного» поняття суверенітету та цифрового суверенітету уже на перший погляд містить певне протиріччя. Якщо суверенітет держави має справу з географічними кордонами країни, її територією, то інформаційний суверенітет, який за своїм змістом є складовою поняття суверенітету є у цьому розумінні більш широким поняттям, яке не обмежене межами території країни. Адже цифровий суверенітет передусім пов'язаний зі здатністю держави та її правом визначати зміст інформації, передусім в кіберпросторі, незалежно від місця знаходження такої інформації – в межах країни чи поза її межами.

Слід відмітити, що у законодавстві України існує легальне нормативне визначення інформаційного суверенітету. Відповідно до Закону України «Національну програму інформатизації», інформаційний суверенітет держави – *здатність* держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави» [6]. Інших визначень в чинному законодавстві даного поняття немає як і більш детальних норм щодо засобів та способів контролю держави за вказаними інформаційними потоками.

Разом з тим у свій час у Верховній Раді України було зареєстровано законопроект «Про інформаційний суверенітет та інформаційну безпеку України» відповідно до якого інформаційний суверенітет визначався як «*право* держави на формування і здійснення

національної інформаційної політики відповідно до Конституції і законодавства України, міжнародного права в національному інформаційному просторі України» [7]. Перш ніж продовжити, варто сказати, що Державна інформаційна політика України визначається як сукупність основних напрямів і способів діяльності держави по одержанню, використанню, поширенню та зберіганню інформації.

Порівняння цих двох дефініцій дозволяє визначити відмінності між ними. Отже, як бачимо в першому визначенні вжита конструкція «котролювати і регулювати потоки інформації з-поза меж держави», тобто це означає, що держава пов'язує інформаційний суверенітет з виключним правом здійснювати контроль та правове регулювання за інформаційним простором загалом та інформацією, яка поступає в країну з-поза її меж. В той час як визначення із законопроекту показує нам, що інформаційний суверенітет це *«право держави на формування і здійснення національної інформаційної політики»*. У цьому визначенні не вказано якої саме інформації, а тому можна зробити припущення, що всієї: як тієї, що надходить в країну з-поза меж, так і «внутрішньої». На наш погляд, друга дефініція у цьому контексті є більш сучасно-орієнтованою, тому що кожного дня через державу проходить неймовірно велика кількість інформації, а особливо всередині держави для якої потрібен захист та конфіденційне збереження. Крім того, сучасні реалії свідчать, що з точки зору національної безпеки, надзвичайно важливо контролювати обидва напрями руху інформації і з-поза меж країни, і в середині країни. Адже факти існування та викриття ботоферм в середині країни, з допомогою яких держави агресори дезінформують український народ є непоодинокими. Так, нещодавно Служба безпеки України викрила чергову ботоферму, яка діяла на користь російських спецслужб. Під час обшуків за адресами перебування організаторів протиправної діяльності в Херсонській області правоохоронці виявили понад 3 тисячі сім-карток, а також комп'ютерну техніку з підтвердженнями незаконних дій [8]. Як бачимо, у цьому випадку дезінформування здійснюва-

лось в середині країни і таким чином підривались основи державної політики у сфері безпеки громадян та громадського порядку.

Слід також додати, що на відміну від чинного закону, зазначеним проектом Закону передбачалися напрями здійснення інформаційного суверенітету, які включають:

- законодавче визначення та забезпечення державною стратегічних напрямів розвитку і захисту національного інформаційного простору, цілісної державної інформаційної політики;
- визначення норм, засад і меж діяльності зарубіжних та міжнародних суб'єктів в національному інформаційному просторі України;
- формування та захист інтересів України в світовому інформаційному просторі, міжнародних інформаційних відносинах; гарантування інформаційної безпеки України.

Як бачимо проект Закону більш детально підходив до питання регулювання та здійснення інформаційного суверенітету.

Як підсумок зазначимо, що на сьогодні на наш погляд концепція цифрового (інформаційного) суверенітету набуває надзвичайно важливого значення. З невідомих причин, наразі це питання не регулюється належними чином на рівні нормативно-правових актів. Разом з тим, видається, що таке регулювання в умовах збройної агресії на території України потрібне та держава повинна визначати легальні напрями і форми контролю інформації, аж до обмеження окремих інформаційних прав, з метою забезпечення суспільної безпеки та стабільності країни та східноєвропейського регіону загалом.

Список використаних джерел

1. Digital Sovereignty. URL: <https://www.techopedia.com/definition/33887/digital-sovereignty>
2. Теорія держави і права: підручник ; за заг. ред. д-ра юрид. наук, проф., акад. НАПрН України О. М. Бандурки ; МВС України, Харків. нац. ун-т внутр. справ. Харків, 2018. 416 с.

URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/6689/Teoriia%20derzhavy%20i%20prava_pidruchnyk_KhNUVS_2018.pdf?sequence=4&isAllowed=y

3. Національний інформаційний суверенітет у контексті розвитку новітніх інформаційних технологій ; НАН України, Нац. б-ка України ім. В. І. Вернадського. К. : НБУВ, 2011. С. 8. URL: <http://nbuviap.gov.ua/images/nauk-mon/monograf-suverenitet.pdf>

4. What is digital sovereignty and why is Europe so interested in it? \ «Digital sovereignty refers to the ability to have control over your own digital destiny – the data, hardware and soft ware that you rely on and create.» URL: <https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/>

5. Sovereignty 2.0, Anupam Chander, Haochen Sun «At first glance, the term «sovereignty» over parts of the internet may seem entirely out of place. Afterall, one of the prerequisites for the recognition of the sovereignty of a state in international law is the exercise of power over a territory.³³ Andrew Woods grounds his definition of “data sovereignty” in three core elements of state sovereignty: “(1) supreme control; (2) over a territory; (3) independent from other sovereigns.”³⁴ The tension between the notion of “digital sovereignty” and the territorial foundation for sovereignty disappears when we recognize that in order to exercise control over any territory, it is increasingly necessary to exercise control over the online activities available in that territory. This in sight connects place and cyberspace».

URL: <https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3422&context=facpub>

6. Про Національну програму інформатизації: Закон України від 4 лютого 1998 року № 74/98-ВР. URL: <https://zakon.rada.gov.ua/laws/show/74/98-вр#Text>

7. Про інформаційний суверенітет та інформаційну безпеку України : проект Закону України. URL: <http://uacm.kharkov.ua/ukr/index.shtml?ulaws/usuvetr.htm>

8. СБУ знешкодила у Херсонській області велику ботоферму спецслужб РФ. Інтерфакс-Україна. URL: <https://ua.interfax.com.ua/news/general/781995.html>

Андрусенко А. О.

студентка НТУУ «КПІ ім. Ігоря
Сікорського»

Науковий керівник: Дубняк М. В.

кандидат юридичних наук старший
викладач, НТУУ «КПІ імені Ігоря
Сікорського»

МІСЦЕ ПРАВА НА КІБЕРБЕЗПЕКУ В СИСТЕМІ ІНФОРМАЦІЙНИХ ПРАВ

Масове використання в останні десятиріччя у найрізноманітніших сферах суспільного життя комп'ютерних і телекомунікаційних технологій, включаючи інтернет-технології, поряд із наданням значної кількості переваг сприяло виникненню великої кількості загроз. Реалізація цих загроз завдає значної шкоди як на національному рівні, так і на міжнародній арені. Це спонукало до розуміння необхідності вирішення нагальної проблеми з метою мінімізації, ліквідації та попередження кіберзагроз. [2, с.109].

Метою дослідження є розмежування понять кібербезпека та інформаційна безпека, та визначення місця права на кібербезпеку серед інформаційних прав.

Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України [1].

На думку Харитоненко І. О., кібербезпека – захист прав і свобод людини під час використання кіберпростору. Забезпечення кібербезпеки має ґрунтуватися на принципах відкритості, доступ-

ності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі [4, с. 164].

В широкому сенсі під системою забезпечення кібербезпеки варто розуміти сукупність організаційно об'єднаних органів управління, а саме: державних органів, громадських організацій, посадових осіб та окремих громадян, які спрямовують свою діяльність на створення умов для реалізації національних інтересів у кіберпросторі, а також сил, засобів і методів, які використовуються для досягнення даної цілі відповідно до законодавства України. Також можна додати, що система забезпечення кібербезпеки є єдиним державно-правовим механізмом, та всі його суб'єкти діють чітко в межах, визначених законодавством [2, с.110].

Часто кібербезпеку та інформаційну безпеку ототожнюють, але це різні поняття. Відповідно до ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» кібербезпека розуміється як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання й нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі.

Інформаційна безпека розуміється як стан захищеності життєво важливих інтересів людини, суспільства й держави, за якого запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, котра використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання й порушення цілісності, конфіденційності та доступності інформації.

Проаналізувавши ці два визначення, Хоббі Ю., робить висновок, що інформаційна безпека здебільшого стосується захисту саме інформації та доступу до неї, а кібербезпека – захисту прав і свобод людини під час використання кіберпростору [3, с.38]

З огляду на вищевикладене, Хоббі Ю., пропонує розглядати право на кібербезпеку як право на такий правопорядок, за умов

якого забезпечуються, охороняються й захищаються права і свободи людини під час використання кіберпростору.

Висновки: з урахуванням проаналізованого дослідження Хоббі Ю. [3, с.41], відзначимо, що право на кібербезпеку можна розглядати як невід’ємне, невідчужуване право особи на захищеність її важливих інтересів, зокрема й інформаційних прав, під час використання кіберпростору. Право на кібербезпеку можна віднести до інформаційних прав людини, оскільки кіберпростір розглядається як окрема сфера протиборства і складається з інформації.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року No 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 30.11.2021)
2. Діордіца І. В. Система забезпечення кібербезпеки: сутність та призначення. *Підприємництво, господарство і право*, 2017. С. 109-116.
3. Хоббі Ю. С. Право людини на кібербезпеку: проблеми визначення та гарантування. *Юридичний вісник*, 2020, С. 37-43.
4. Харитоненко І. О. Право на кібербезпеку: проблеми визначення: збірник тез круглого столу, присвяченого 72-й річниці прийняття Загальної декларації прав людини. Київ, 2020, С. 163 – 164.

Моргун А. М.

студентка Чернівецького
національного університету
ім. Ю. Федьковича

Науковий керівник: Заморська Л. І.

доктор юридичних наук, доцент
кафедри теорії права та прав людини
Чернівецького національного
університету ім. Ю. Федьковича

ПРАВА ЛЮДИНИ І ГРОМАДЯНИНА В ІНФОРМАЦІЙНІЙ СФЕРІ

У ХХІ столітті суттєвий вплив на розвиток суспільства здійснили інформаційні технології, змінили їх правове регулювання та певні цінності. Інформаційне суспільство породжує все нові очікування та кидає виклики сучасним реаліям. Але використання технологічних інструментів може не тільки вирішити проблеми, а й з легкістю створити їх. Підтримка та розвиток демократії, утвердження справедливості та рівності, забезпечення відкритості та прозорості у відносинах між індивідами та владою створюють ілюзію тільки позитивного впливу, але послаблення держави, глобалізація та появлення авторитетних недержавних політичних акторів створюють нові загрози для прав людини. Варто зазначити, що концепція прав людини, як і концепція інформаційного суспільства починали свій розвиток суто з гіпотез, але все ж завдяки міжнародно-правовій легалізації вони виведені на політичному рівні правової дійсності.

Оскільки Інтернет являється головним каталізатором для здійснення всіх прав людини, є важливим фактором культурного, освітнього, соціального розвитку та основним джерелом інформації в сучасному суспільстві, то ми розглянемо права людини, пов'язані з використанням Інтернету, тобто “Цифрові права” або “Інформаційні права”.

Інформаційними правами називають певні можливості, які гарантовані державою, задовольняти потреби в поширенні, охороні, використанні, отриманні, захисті необхідного для життєді-

яльності обсягу інформації [1, ст. 117]. Вони становлять цілісний екзистенціальний феномен, який можливо розпізнати тільки крізь призму їхніх системних властивостей, що якраз таки проявляється через наявність прав і свобод, які мають інформаційний характер у різноманітних сферах життєдіяльності суспільства. Досить часто права людини онлайн окреслюють науково необґрунтованим поняттям “цифрові права”. Візьмемо до прикладу право на свободу слова, яке давно включене до каталогу основоположних прав людини в міжнародних актах- Міжнародному пакті про громадянські та політичні права, Загальній декларації прав людини- і в будь-якому випадку буде захищене, не залежно від сфери в якій воно реалізується. А виникнення такого “цифрового права” як бути забутим є досить нещодавнім. На нашу думку, цифрові права слід розглядати як окрему категорію, яка систематизовано містила б у собі весь порядок захисту таких прав та їх реалізації, так як деякі гарантії на них даліше розпорошені по резолюціях, рекомендаціях та інших актах.[4, ст. 6]

Основним цифровим правом людини є право на доступ до Інтернету. Це невід’ємна умова для реалізації прав і свобод людини та можливість прийняття участі в процесах, які пов’язані з державними справами. Воно охоплює цілих два аспекти:

1. Заборона безпідставного обмеження в користуванні Інтернетом державою, а особливо відключати його в цілому регіоні або в усій країні.

2. Зобов’язання держави вживати всіх заходів щодо максимального доступу своїх громадян до Інтернету.

Право доступу до Інтернету має базуватись на кількох важливих принципах:

- недискримінація та інклюзивність – сам доступ має забезпечуватись за адекватну ціну, а взаємодія в мережі повинна бути вільна від дискримінації за будь-якими ознаками;
- безпека Інтернету – держава повинна гарантувати безпеку;
- мережева нейтральність – особи, які користуються послугами повинні могли самі обирати систему та програмне забезпечення[2].

На сьогодні це право не закріплене на міжнародному та національному рівнях.

Наступне право, на яке варто звернути увагу, це право на свободу вираження поглядів онлайн. Базою демократичного суспільства та основною умовою його розвитку та самореалізації людини є свобода вираження поглядів. Вона включає в себе право поширювати інформацію, суть якої відповідає праву вираження в реальному житті, вільно шукати її та отримувати[6]. Держава, як відомо, повинна забезпечувати певні умови для такої реалізації та не перешкоджати їй, але

зважаючи на все, це право не є абсолютним та може бути обмежене згідно таких критеріїв:

- законність – обмеження повинно чітко відповідати закону та здійснене уповноваженими органами;
- легітимна ціль обмеження – порушення територіальної цілісності, захист прав інших людей, підтримка національної безпеки, запобігання розголошенню інформації, отриманої конфіденційно;
- необхідність у демократичному суспільстві – органи повинні обґрунтувати підстави обмеження та вжити мінімальних заходів[4, ст. 16-17].

Персональні дані є однією з найбільш конвертованих валют у сучасному світі. Можна висловитись, що користуючись соціальними мережами ми платимо за це своїми даними. Право на захист персональних даних регулюється Законом України “Про захист персональних даних”[5], який встановлює чіткий перелік умов обробки особистих даних. Основною з таких підстав є згода суб’єкта даних на обробку та збір. Окремо слід зазначити, що в багатьох випадках у користувачів взагалі не має вибору: особа змушена передати свої дані, бо в іншому разі вона взагалі не зможе користуватись тим чи іншим сервісом. Така згода є умовно-добровільною. Водночас, якщо щодо захисту персональної інформації, що міститься в державних базах даних, існує певна нормативна база, то питання збирання, зберігання та обробки інформації системами відеоспостереження залишаються поза увагою законодавця, поз-

бавляючи громадян можливостей ефективно захистити свої права. Так, лише в Києві на сьогодні встановлено понад 7 тисяч камер відеоспостереження, і, за даними Київської міської державної адміністрації, ця кількість буде зростати.[3]

Зважаючи на карантинні обмеження, особа має право мирно зібратись з іншими громадянами в Інтернеті. На практиці це означає, що людина може обрати собі будь-який сайт чи додаток та приєднатись до зустрічі для обговорення якогось питання. Це право передбачає можливість створення певних профспілок, проведення мітингу та бути присутнім на політичних дебатах.

Так само як в Інтернеті людина має бути убезпечена від посягань на її права. Кожна особа має право на ефективний засіб правового захисту в разі порушення та обмеження прав і свобод. На початку не обов'язково звертатися зразу до судових органів, так як захист можна отримати від Інтернет-провайдера, органів державної влади та працівників поліції. Засобами такого захисту може бути вибачення, виправлення, роз'яснення, компенсація або ж поновлення контенту. Механізмами захисту прав людини в Інтернеті є:

1. Звернення до суду.
2. Звернення до Уповноваженого ВРУ з прав людини
3. Звернення до міжнародних судів чи організацій
4. Звернення до Управління боротьби з кіберзлочинністю Міністерства внутрішніх справ України.

Підсумовуючи все вищесказане, ми можемо зробити висновок, що Інтернет є одним з найпотужніших резервуарів знань і всі мають мати можливість бути активним учасником. Цифровий вимір прав людини з подальшим розвитком буде тільки збільшуватись та потреба захисту і правового регулювання буде завжди актуальною, як і механізм міжнародного унормування.

Список використаної літератури:

1. Беланюк М. В. // Права людини в Інтернеті // Захист прав, свобод і безпеки людини в інформаційній сфері в сучасних умовах: Матеріали другої науково-практичної конференції. 21 травня 2020 р., м. Київ.

2. Володовська В. Заборони та свободи в інтернеті: як виглядати-ме Декларація цифрових прав людини: URL: https://zmina.info/articles/zaboroni_ta_svobodi_v_interneti_jiak_vigljiadati_me_deklaracija_cifrovih_prav_ljudini/ (дата звернення: 18.05.2020)

3. Права людини онлайн: Порядок денний для України / Віта Володовська, Максим Дворовий – Київ: ГО «Лабораторія цифрової безпеки», 2019.

4. Про захист персональних даних: Закон України від 20.11.2012р. №5491-VI. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

5. Персональні дані онлайн: проблеми регулювання та перспективи захисту [Електронний ресурс] // Реанімаційний пакет реформ. – 2019. – Режим доступу до ресурсу: <https://rpr.org.ua/news/personal-ni-dani-onlayn-problemy-rehuliuвання-ta-perspektyvy-zakhystu/>.

6. Конституція України [Електронний ресурс] : від 28.06.1996. – Режим доступу: <http://zakon4.rada.gov.ua/laws/show/254-к/96-вр>

Дядюша В. В.

студентка НТУУ «Київського
політехнічного інституту ім. Ігоря
Сікорського»

СОЦІАЛЬНІ МЕРЕЖІ ЯК НОВИЙ ВИМІР ВЕДЕННЯ ІНФОРМАЦІЙНИХ ВІЙН

Бурхливий розвиток соціальних мереж є рушійним механізмом для розширення населення, так як розвивається система інформаційної комунікації (соціальні мережі), які не завжди є контрольованими. Держава у свою чергу повинна реагувати та контролювати дані процеси.

Збільшення виробництва нової інформації в національному інформаційному просторі є, з одного боку, позитивним явищем, оскільки зміцнює національний інформаційний потенціал, що є важливим чинником розвитку інформаційного суспільства в міжнародних відносинах сьогодення. З іншого боку, через участь переважної більшості некваліфікованих чи малокваліфікованих

зацікавлених сторін у створенні інформації, національний інформаційний простір рясніє інформацією яку досить важко відокремити, достовірну інформацію від дезінформації.

Дезінформування та маніпулювання інформацією, на думку В. Петрика, досягається через: тенденційне викладення фактів (інформування, яка полягає в упередженому висвітленні фактів або іншої інформації щодо подій за допомогою спеціально підібраних правдивих даних; як правило, за допомогою цього методу спеціально сформована інформація подається дозовано, до постійно зростаючого напруження); дезінформування «від зворотного» (відбувається шляхом надання правдивих відомостей у перекрученому вигляді чи в такій ситуації, коли вони сприймаються об'єктом спрямувань як неправдиві; в результаті виникає ситуація, коли об'єкт фактично знає правдиву інформацію про наміри чи конкретні дії протилежної сторони, але сприймає її неадекватно, не готовий протистояти негативному впливу); термінологічне «мінування» (полягає у викривленні первинної правильної суті принципово важливих, базових термінів і тлумачень загальносвітоглядного та оперативного-прикладного характеру); «сіре» дезінформування (передбачає використання синтезу правдивої інформації з дезінформацією); «чорне» дезінформування (використання переважно неправдивої інформації) [2].

Донедавна Інтернет мав переважно інформаційну складову, але зараз в ньому посилюється агітаційно-пропагандистський сектор, який характеризується вираженою агресією. Традиційні засоби масової інформації все частіше працюють з інтернет-ресурсами, такими як джерела інформації та інструменти впливу на поінформованість громадян.

Поняття інформаційної війни – можна розглядати, як інформаційно-орієнтовану атаку, незалежно від використовуваних засобів. Це певна зброя, що використовується у стратегічних інформаційних війнах. Ця зброя не завдає фізичних ушкоджень, але може призвести до справжньої війни.

Цікаво зазначити, що засоби масової інформації від початку створювались із потреби впливати на якомога більшу кількість населення.

ІВ розглядає інформацію як окремий об'єкт або як потенційну зброю і прибуткову мішень. Інформаційну війну можна розглядати, як якісно нову форму ворожості, активних контрзаходів в інформаційному просторі [1].

Варто взяти до уваги висновки, зроблені Н. Ф. Семен, досліджуючи проблеми інформаційної війни проти України. Дослідниця наголошує на тому, що ефективність боротьби з військовою агресією настане лише за умови створення в Україні необхідної правової бази для боротьби з пропагандою. «Для того щоб ефективно протистояти в інформаційній війни та адекватно відповідати російській стороні, слід чітко усвідомити, що формат інформаційної війни вже давно вийшов за рамки насильства» [3, с. 18].

Отже, можна зробити висновок, що недостатня увага до питань, пов'язаних із запобіганням інформаційним загрозам може завдати значної шкоди політичній системі будь-якої держави, аж до знищення.

На сьогодні з боку нашої держави, ще не розроблені кардинальні заходи з протидії інформаційним атакам. Це означає те, що в інформаційній війні успіх держави буде забезпечуватися за рахунок вдосконалення інформаційних технологій.

Список використаних джерел:

1. Наливайко Л. Р. Інформаційна безпека та інформаційна політика в Україні: конституційно-правовий аспект. Вісник Запорізького державного університету. 2003. – № 1. С. 60–65.
2. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи URI: <http://justinian.com.ua/article.php?id=3222>
3. Семен Н. Ф. Російські інтернет-ресурси як чинник інформаційної війни проти України (на прикладі сайтів «Правда.Ру» та «Российский диалог») : ареш. дис. к. н. соц. комун; спеціальність 27.00.01. Дніпро : Дніпровський національний університет імені Олеся Гончара, 2018. 23 с.

Скулинець І. В.

студентка НТУУ «КПІ ім. Ігоря
Сікорського»

Науковий керівник: Дубняк М. В.

кандидат юридичних наук старший
викладач, НТУУ «КПІ імені Ігоря
Сікорського»

ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ПРАВ ЛЮДИНИ В СОЦІАЛЬНИХ МЕРЕЖАХ

У сучасному світі все більше людей стають залучені до інформаційного світу. Особливо стрімко сьогодні розвиваються соціальні мережі, деякі навіть набирають великих обертів на світовому ринку. Так, уже багато років найпопулярнішою соціальною мережею світу є Facebook. Станом на січень 2021-го там було понад 2,7 мільярда користувачів. На другому місці YouTube – більш ніж 2 мільярди користувачів. Далі – месенджери WhatsApp та Facebook Messenger, а також Instagram. TikTok має сьому позицію, а Twitter – шістнадцяту [1]. Тому варто з'ясувати, чи здійснюється правове забезпечення наших прав, як користувачів різноманітних соціальних мереж.

Метою даного дослідження є порівняльно-правовий аналіз значення поняття «соціальні мережі» та узагальнення різносторонності проблематики інформаційних прав користувачів соціальних мереж.

З'ясуємо поняття «соціальна мережа» і виділимо її основні ознаки.

Відомий дослідник Д. Бойд зазначає, що сайти соціальних мереж як веб-сервіси, дозволяють людям: 1) створювати загальнодоступний або напіввідкритий профіль в обмеженій системі, 2) формулювати список інших користувачів, з якими вони мають спільне з'єднання і діляться інформацією, 3) переглядати та перемішувати їхній список з'єднань з іншими, створених користувачами в системі [2, с. 211].

Івашнюва С. В. в своїй роботі дотримується загального визначення поняття «соціальна мережа» як віртуального майданчика, що забезпечує своїми засобами спілкування, підтримку, створення, розбудову, відображення та організацію соціальних контактів, у тому числі й обмін даними між користувачами, який передбачає попереднє створення облікового запису [3, с. 15].

Дослідниця Спасова К. І. визначає цю категорію як відокремлену платформу, онлайн-сервіс або сайт, що передбачає можливість для користувачів здійснювати комунікацію та обмін інформацією в межах певної категорії відносин [4, с. 12].

На основі вище наведених даних дослідників, можемо визначити, що для соціальних мереж характерні такі ознаки: створення загальнодоступного або напіввідкритого профілю в обмеженій системі, здійснення комунікації та обміну інформацією між користувачами. Проаналізувавши такі терміни, як веб-сервіс, віртуальний майданчик, відокремлена платформа і веб-сайт, доцільно вважати, що найбільш повно відображає суть визначення «соціальної мережі» поняття веб-сайт. Згідно із ст.1 Закону України «Про авторське право і суміжні права», веб-сайт – це сукупність даних, електронної інформації, інших об'єктів авторського права і суміжних прав тощо, пов'язаних між собою і структурованих у межах адреси веб-сайту і облікового запису власника цього веб-сайту, доступ до яких здійснюється через адресу мережі Інтернет [5].

Законодавство України досить об'ємно описує наші права на доступ до інформації, її поширення і захист. Зокрема, ст.34 Конституції України гарантує кожному 1) право на свободу думки і слова, на вільне вираження своїх поглядів і переконань, 2) право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір [6]. Ст.5 Закону України «Про інформацію» передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів, а також те, що реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси ін-

ших громадян, права та інтереси юридичних осіб [7]. Відповідно до ст.1 Закону України «Про захист персональних даних» регулюються правові відносини, пов'язані із захистом і обробкою персональних даних, що спрямовано на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних [8]. Це лише деякі положення щодо забезпечення прав, як онлайн, так і офлайн.

Відзначимо, які існують проблеми правового регулювання інформаційних прав в соціальних мережах:

1. Право приватності і захисту персональних даних.

Хоча в соціальних мережах, наприклад у Facebook, визначено в Умовах і правилах сайту – здійснення мережею “зберігання, оброблення і поширення інформації користувачів”, однак у зв'язку з тим, що існує ризик не ознайомлення осіб з даними правилами – це часто призводить до таких негативних наслідків, як неусвідомлення особою того, що будь-які викладені нею дані, фото і відео можуть бути скопійовані та використовуватися іншими програмами, пов'язаними з даною мережею, тому що Facebook звільняється від відповідальності за порушення конфіденційності сторонніми програмами [9].

2. Неконтрольованість щодо вікового обмеження.

У соціальних мережах для яких є вікове обмеження, так чи інакше зареєстровано дуже багато підлітків, які часто можуть побачити ту інформацію, яка може ним нашкодити, особливо в психологічному плані.

3. Надання надмірного та непропорційного доступу до інформації у зв'язку зі збором інформації про діяльність користувача.

Наприклад у Tik Tok, відразу при реєстрації пропонується вибрати декілька категорій, які б ви хотіли переглядати у себе в стрічці. З однієї сторони це правильно, тому що мережа враховує вподобання користувачів. Проте також пропонуються й інші відео з рекламою чи неякісним контентом, таким як: порнографія, пропаганда наркотиків чи алкоголю, і якщо людина все більше дивитиметься такі відео, то вони частіше з'являтимуться у стрічці. Такі

судження підтверджуються останніми дослідженнями американського видання Wall Street Journal [10].

Отже, під соціальною мережею ми розуміємо веб-сайт, який дозволяє користувачам створювати загальнодоступний або напіввідкритий профіль, за допомогою якого вони мають зв'язок з іншими користувачами цієї системи і обмінюються з ними інформацією. Не дивлячись на існуюче правове поле в Україні, продовжують існувати ризики, що пов'язані з використанням і обробленням персональних даних, неконтрольованим процесом щодо вікового обмеження та наданням надмірного і непропорційного доступу до інформації у соціальній мережі. Це далеко не повний перелік загроз, які виникають, однак доповнення правових актів новими поняттями, які б стосувалися цифрових прав користувачів соціальних мереж, не усуне вказаних проблем. Що свідчить про необхідність більш комплексного підходу до правового регулювання, яке забезпечить співмірні способи охорони прав та інтересів громадян під час користування соціальними мережами.

Список використаної літератури:

1. Соцмережі-2021. URL: <https://hromadske.ua/posts/socmerezhi-2021-tiktok-starshaye-facebook-perevazhno-zhinochij-a-strichku-mi-gortayemo-400-miljoniv-rokiv>

2. Boyd D. M., Ellison N. B. Social Network Sites: Definition, History, and Scholarship. Journal of Computer Mediated Communication. 2008. №13. P. 211-230 URL: <https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1083-6101.2007.00393.x>

3. Івашнюва С. Використання соціальних сервісів та соціальних мереж в освіті / Наукові записки НДУ ім. М. Гоголя. Психолого-педагогічні науки. 2012. №2. С.15 – 17 с. URL: http://nbuv.gov.ua/UJRN/Nzspp_2012_2_5.

4. Спасова, К. І., Відшкодування моральної шкоди при порушенні немайнових прав у соціальних мережах. Автореф. На здобуття наук. ступеня канд.юрид.наук. 12.00.03 С. 23 с. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/14644/%d0%90%d0%b2%d1%82%d0%be%d1%80%d0%b5%d1%84%d0%b5%d1%80%d0%b0%d1%82_%d0%a1%d

0%bf%d0%b0%d1%81%d0%be%d0%b2%d0%b0%20%d0%9a.%d0%86.
.pdf?sequence=3&isAllowed=y

5. Закон України «Про авторське право і суміжні права» // Відомості Верховної Ради України (ВВР). 1994. №13. ст.64 URL: <https://zakon.rada.gov.ua/laws/show/3792-12#Text> (дата звернення: 19.11.2021)

6. Конституція України // Відомості Верховної Ради України (ВВР). 1996. №30. ст. 141 URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80/paran4269#n4269> (дата звернення: 19.11.2021)

7. Закон України «Про інформацію» // Відомості Верховної Ради України (ВВР). 1992. №48. ст.650 URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (дата звернення: 19.11.2021)

8. Закон України «Про захист персональних даних» // Відомості Верховної Ради України (ВВР). 2010. № 34. ст.481 URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 19.11.2021)

9. Політика використання даних Facebook. URL: <https://uk-ua.facebook.com/about/privacy>

10. Як TikTok підсаджує дітей на відео з сексом і наркотиками/ Розслідування Wall Street Journal URL: <https://texty.org.ua/articles/104690/yak-platforma-tiktok-pidsadzhuye-ditej-na-video-z-seksom-i-narkotykamyr-zsliduvannya-wall-street-journal/?fbclid=IwAR0MEG7c-ZtdC-3imXw1jhbT7msgiuHlb5vvvg98VXu1D7-veQlF6bHXJu3g>. (дата звернення: 19.11.2021)

Супрунович М. Ю.

студент НТУУ «КПІ ім. Ігоря
Сікорського»

Науковий керівник: Дубняк М. В.

кандидат юридичних наук старший
викладач, НТУУ «КПІ імені Ігоря
Сікорського»

ПРАВО НА ДОСТУП ДО ІНТЕРНЕТУ

У наш час мережа Інтернет має широкий спектр економічного, соціального, політичного та культурного використання і є частиною життя кожного з нас. Багато продуктів, сервісів та послуг

зараз реалізуються онлайн – починаючи від державних послуг і закінчуючи інтернет-банкінгом. Проте, як і в будь-якій іншій сфері людської діяльності важливим є обговорення правового регулювання, адже на даний час ці відносини практично не регулюються, на законодавчому рівні в Україні не гарантується доступ до Інтернету.

Метою дослідження є характеристика та аналіз права на доступ до мережі Інтернет, а також міжнародного досвіду його правового закріплення.

Право на доступ до Інтернету у літературі визначається як право людини мати змогу користуватися віртуальним простором мережі Інтернет, що реалізується за допомогою апаратного та програмного забезпечення комп'ютерів та цифрових пристроїв, зокрема, смартфонів [1, с. 3]. Варто зазначити, що в науковій спільноті вказане питання є дискусійним. На сьогоднішній день не існує єдиного підходу до визначення самого поняття та складових права на доступ до мережі Інтернет. Науковці визначають його як право на доступ безпосередньо до мережі Інтернет, а іноді розуміють це право виключно як інструмент для здійснення низки інших прав.

Цікавим є погляди різних організацій на цей правовий аспект. Зокрема, Організація Об'єднаних Націй (далі – «ООН») висловлює певну позицію і зазначає, що мережа Інтернет є важливим інструментом для забезпечення низки прав людини і тому гарантування доступу до Інтернету має бути пріоритетом для усіх держав [2]. В 2016 р. ООН опублікувала резолюцію рекомендаційного характеру, в якій зазначила, що в онлайн режимі люди мають ті ж права, що і в офлайн. Також в ній засуджується будь-яке обмеження та блокування доступу до Інтернету [3, с. 2]. Як зазначав сам Винахідник Всесвітньої Мережі Тім Бернес-Лі, “мережа була створена для досягнення суспільних благ людства, вона має допомагати людям працювати разом” [4, с. 78].

В 2015 р. Парламент Італії опублікував проект «Білль про права людини в Інтернеті» [5]., в якому говорилося про право на доступ до Інтернету. Франція, Іспанія, Фінляндія, Естонія, Греція законо-

давчо закріпили дане право на початку поточного століття. Великобританія пішла шляхом фактичного визнання даного права – на даний момент державою взято на себе зобов'язання забезпечити повсюдний доступ в Інтернет не нижче певної швидкості. Конституційне право на доступ до інформації з розвитком сфери високих технологій безсумнівно підлягає подальшому детальному вивченню. Тому у наш час немає єдиної точки зору на те, чи можливо віднести право на доступ до мережі Інтернет до прав людини, чи це лиш засіб реалізації інших прав.

Проблемним є також питання сутності права на доступ до мережі Інтернет, зокрема, немає згоди щодо того, чи є воно негативним або позитивним. Джон Квін в своїй статті «Доступ до Інтернету як фундаментальне право» зазначає, що дане право за своєю природою є скоріш негативним, тобто таким, що характеризується як право не бути позбавленим доступу до Інтернету. Однак, деякі держави, серед яких Франція та Фінляндія, пішли навіть далі та визнали право на доступ до мережі позитивним [6, с. 1, 3].

У сфері регулювання права на Інтернет в Україні існує правовий парадокс. З одного боку, низка державних послуг та документів «оцифровуються» і стають доступними онлайн (наприклад, додаток «Дія»). З іншого боку, в національному законодавстві досі нема загальної норми щодо права на доступ до мережі Інтернет.

16 квітня 2014 р. було зареєстровано (а у вересні 2014 р. – внесено до порядку денного п'ятої сесії Верховної Ради України сьомого скликання) Проект Закону «Про внесення доповнень до Цивільного кодексу України (щодо гарантування права фізичної особи на доступ до інтернету)» № 4715 [7]. Цей законопроект передбачав можливість доповнити ЦК України ст. 302-1 такого змісту: «фізична особа має право на доступ до інтернету»; «право фізичної особи на доступ до інтернету не може бути обмежене»; «обмеження доступу до певних даних, що містяться в інтернеті, можливо лише на підставі рішення суду про незаконність таких даних». Проте, проект не було схвалено.

Підсумовуючи, слід зазначити, що протягом останніх 10 років ООН неодноразово наголошувала на важливості забезпечення

громадян правом на доступ до Інтернету. Варто визнати, що від можливості реалізації права на доступ до Інтернету залежить реалізація багатьох інших прав та свобод громадянина, тому є необхідною умовою для забезпечення повноти здійснення інших прав та свобод людини і громадянина в сучасному суспільстві.

Список використаних джерел

1. Huang Z. St Andrews Research Repository // Why There Can Be a Human Right to Internet Access. St Andrews, 2019. Режим доступу: <https://research-repository.st-andrews.ac.uk/handle/10023/17802>
2. Internet Access Is Not a Human Right // Vinton G. Cerf // The New York Times. 2012. № 2812.
3. The promotion, protection and enjoyment of human rights on the Internet // Human Rights Council. 2016. Режим доступу: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf
4. Мукомела І. В., Право на доступ до Інтернету: проблеми визначення та забезпечення // Вісник Національної академії правових наук України № 4 (87) 2016.
5. Declaration of Internet Rights. 2015. Режим доступу: https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/testo_definitivo_inglese.pdf
6. Kwan. J. Internet access as a fundamental right / J. Kwan – TWS Policy Paper. – 2011. – N3. – P. 1,3
7. Про внесення змін до Закону України «Про внесення доповнень до Цивільного кодексу України (щодо гарантування права фізичної особи на доступ до Інтернету) : Закон України від 16 квітня 2014 р. № . 4715

ОСОБЛИВОСТІ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ РОЗВИТКУ СУЧАСНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ СУСПІЛЬСТВА

Пархоменко Н. М.

доктор юридичних наук, професор,
вчений секретар Інституту держави
і права імені В. М. Корецького НАН
України

ЗАБЕЗПЕЧЕННЯ ПРАВ І СВОБОД ГРОМАДЯН З ОГЛЯДУ НА ФУНКЦІОНУВАННЯ СУЧАСНИХ КОМУНІКАТИВНИХ ПРАКТИК

Багатофункціональність, зручність, швидкість передавання інформації, насиченість, інтернаціоналізм – властивості, що характеризують сутність сучасних комунікаційних платформ, зростання попиту серед населення та вплив на розвиток суспільних відносин. Саме у ХХІ столітті Інтернет та соціальні мережі стали однією із невід’ємних складових соціального середовища: від особистого спілкування та задоволення особистих потреб до потреб політики, права, бізнесу, культури, екології та ін. Адже активна і потужна робота різного роду комунікативних практик, з огляду на їх властивість всепоширення та доступності, оперативності подання та обміну інформацією, відносної контрольованості, має або може мати як позитивні так і негативні ефекти. До позитивних слід віднести можливість отримання публічної інформації, он-лайн консультацій та різного роду послуг, в т.ч. адміністративних, організації відносин між державою та громадянським суспільством тощо.

Відповідно з’являються та функціонують комунікативні відносини, окремі складові яких потребують правового врегулювання. За таких обставин, функція держави полягає у необхідності зако-

нодавчого закріплення державної інформаційної політики, визначенні ступеня, форм та способів участі органів державної влади у процесі інформатизації як на державному, так і міжнародному рівнях[2; 9]. У зв'язку із цим наразі в Україні сформована відносно нова галузь права – інформаційне, норми якої урегульовують відносини у сфері створення та поширення інформації. Йдеться насамперед про організацію, упровадження, функціонування комунікативних проектів (платформ, практик), результати роботи яких можуть мати як позитивний, так і негативний ефект, зокрема спричинити наслідки, пов'язані із порушенням прав і свобод громадян, їх законних інтересів. Зокрема, йдеться про негативний вплив інноваційних комунікативних практик на окремі сфери суспільних відносин, що зумовлює: десоціалізацію особистості, розрив соціальних зв'язків, доступ до персональних даних, порушення таємниці листування та поширення конфіденційної інформації, злам державних серверів та оприлюднення таємної інформації або інформації з обмеженим доступом, що може спричинити загрози національній безпеці і шкоду окремим особам, але й викликати та ін.

Зазначені проблеми дедалі частіше стають об'єктом дослідження юридичної науки. Наразі найбільш широко проаналізовані основні аспекти формування та розвитку комунікативних практик в аспекті інформаційного суспільства, а саме організація та діяльність апарату держави, механізму держави в умовах інформаційного суспільства, організаційно-правове та наукове забезпечення інформатизації в Україні та ін. З-поміж іншого запропоновано виокремити правничу інформаціологію, як міжгалузевий напрям науки про інформаційно-комунікативні процеси та соціально-правові відносини, які виникають при цьому, роль та місце юридичної науки, практики та соціального управління у процесах інформатизації суспільства, інноваційні зміни у правових явищах, породжених ними суспільних наслідках, процесах, тенденціях та відносинах, удосконалення засобів і методів адміністративної діяльності та юридичної практики за допомогою інформаційних технологій та ресурсів[2; 9]. Втім, майже недослідженими зали-

шаються проблеми правового врегулювання відновлення порушених в наслідок функціонування комунікативних практик прав і свобод громадян та їх відновлення, що насамперед вимагає осмислення сутнісних характеристик комунікативної діяльності, комунікативних практик в правовому аспекті.

Сучасні соціально-поведінкові науки визначають комунікативні практики як різновид соціальних практик, сутністю яких є представлення та передавання певним суб'єктом власного або суспільного досвіду, знань, переконань, норм, цінностей, здобутків тощо певному зацікавленому середовищу, в результаті чого змінюється уявлення про об'єкт комунікації та формується нова суб'єктивна модель знань та цінностей.

Важливо при цьому зазначити, що результатом комунікацій є формування відповідних цінностей у суб'єктів комунікації. Зокрема, комунікативні практики базуються на колективному досвіді та спрямовані на підтримання і розвиток комунікації задля забезпечення відчуття «спільності» суб'єктів комунікації при збереженні їх індивідуальності, що дає змогу досягати власних інструментальних цілей[7] (приміром, щодо віднайдення способів вирішення актуальних повсякденних задач і проблем, що турбують громадян, а також способів задоволення власних цілей, потреб та інтересів, комунікації з іншими членами громади, спільноти).

Щодо комунікативних платформ, то сутність кожної з них полягає в об'єднанні людей відповідно до їх інтересів, а також надання їм можливості підтримувати віртуальне спілкування[3]. У загальному вигляді та за різними критеріями комунікативні платформи поділяють на такі *різновиди*: 1) залежно від призначення: для побуту, роботи; 2) мережі відео спрямованості; мережі аудіо спрямованості; мережі з акцентом на фото; 3) залежно від змісту інформаційного наповнення: тематичні (за віком, статтю, інтересами, освітою, родом діяльності, та ін.); 4) за рівнем доступу: закриті та відкриті тощо.

Таким чином, різні комунікативні платформи мають різне спрямування та виключне призначення, що знаходить застосування у різних сферах суспільних відносин. Варто зазначити, що історично перши-

ми виникли платформи, які пропонували спілкування між людьми за особистими інтересами. Але, з прискоренням розвитку ІТ сфери, почали активно створюватися та функціонувати комунікативні платформи, метою яких стало надання інформації та консультацій органами влади, політичними партіями, громадськими організаціями та ін. До прикладу, «Форум прогресивних підприємців», «Український освітній всесвіт», Форум організацій громадянського суспільства, Національна платформа «Діалог про мир та безпечну реінтеграцію» та ін.

Комунікативну платформу в політичній сфері можна визначити, як он-лайн сервіс, що використовується для побудови і відображення соціальних мереж та соціальних зв'язків між людьми. Такі ресурси дозволяють своїм користувачам обмінюватися ідеями, повідомляти про цікаві посилання, ділитися новинами, у сфері політики – працювати зі своїми виборцями, доносити передвиборчі лозунги та програму, проводити консультації, надавати допомогу, в т.ч. правову і т.ін. До прикладу, за ініціативою Президента України МЗС України розроблено та впроваджено концепцію «Кримська платформа» як міжнародну комунікативну платформу обговорення та координації зусиль міжнародного співтовариства щодо окупації Криму, об'єднання зусиль для розуміння та відповіді на загрози та виклики, які із цим пов'язані.

Комунікативні практики в сфері права відбуваються в контексті правової інформатизації, «як сукупності організаційних, соціально-економічних і науково-технічного процесів забезпечення потреб державних органів, юридичної та управлінської практики та фізичних осіб відомостями на основі інформаційно-телекомунікаційних систем, які формують, накопичують, обробляють, організовують і надають користувачам масиви соціально-правових інформаційних ресурсів для удосконалення правової системи держави і світового правопорядку[2; 9]». Внаслідок запровадження комунікативних практик інформаційний простір в Україні постійно наповнюється правовим контентом, завдяки чому зміст права доводиться до широких верств населення, впливаючи на суспільну правову культуру, правову свідомість та, відповідно, правопорядок. Не залишається без змін правотворча та правореалізаційна сфера, набуваючи

інноваційних рис, виходячи за національні межі, набуваючи відповідність міжнародним стандартам та європейським принципам, особливо в сфері забезпечення прав і свобод людини. Відповідно нових рис поступово набуває правова система України загалом.

В сучасному світі палітра комунікативних платформ та їх потенціал значний, що передбачає створення відповідних механізмів забезпечення загалом та організаційно-правових зокрема, особливо в контексті реалізації прав і свобод громадян, їх захисту. Йдеться про постійне удосконалення: системи органів державного управління в сфері інформатизації, їх структури, повноважень, зв'язків з іншими суб'єктами інформатизації; нормативно-правових засад та механізмів функціонування інформаційного суспільства, реалізації інформаційної функції держави та інформаційної політики; розвиток недержавного сектору інформатизації. Ефективність зазначених процесів безпосередньо залежить від якості відповідного законодавства, дієвості правових механізмів. Завдання законодавця насамперед полягає у забезпеченні правомірної поведінки учасників інформаційних відносин; безпеки надання та отримання інформаційних послуг; визначенні стандартів якості інформаційного продукту; механізми відповідальності за правопорушення в інформаційній сфері.

Використана література:

1. Беляков К. І. Організаційно-правове та наукове забезпечення інформатизації в Україні: проблеми теорії та практики. Дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. – Ін-т держави і права ім. В. М. Корецького НАН України. – Київ, 2009. С. 9.

2. Волошин Максим. Комунікативні платформи соціальних інтернет-мереж. *Історико-політичні проблеми сучасного світу*. С. 274, 275. file:///C:/Users/%D0%9F%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C/Downloads/Ippss_2015_29-30_41.pdf

3. Сергодеев В. П. Коммуникативные практики в интернет сообщениях. *Вестник АГУ*. 1 (135). 2014. С. 133-138.

Некіт К. Г.

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

ДО ПИТАННЯ ПРО ПРАВА НА МАШИННО ГЕНЕРОВАНІ ДАНІ

Бурхливий розвиток промислового Інтернету речей (ІоТ) з високою вірогідністю може привести до нової промислової революції. На думку аналітиків, до 2030 року ІоТ може додати до глобальної економіки 14,2 трильйона доларів. Потенційний прибуток завдяки промислому Інтернету речей може скласти 7,1 трильйона доларів для Сполучених Штатів, 1,8 трильйона доларів для Китаю, 700 мільярдів доларів для Німеччини та 531 мільярд доларів для Великобританії [1].

Підключені до Інтернету пристрої щоденно створюють величезні обсяги інформації. Наприклад, смарт-годинники відстежують фізичну активність людини, вимірюють серцевий ритм, кількість кроків, тиск тощо. Смарт-автомобілі щоденно збирають найрізноманітнішу інформацію – стосовно трафіку, заторів на дорогах, стану доріг, улюблених маршрутах та звичках власника машини. Частина з таких даних є очевидно персональними, навіть особливо чутливими даними, однак інша частина, яка може бути відділена від конкретної фізичної особи та деперсоніфікована, очевидно, має складати окрему категорію інформації. Така інформація може використовуватись як іншими особами (для розуміння оптимальних маршрутів), виробниками розумних пристроїв (для вдосконалення продуктів свого виробництва), для державних структур (для поліпшення стану доріг та ситуацій на дорогах) тощо. Саме тому останнім часом все частіше говорять про необхідність розробки особливого правового режиму для даних, згенерованих машинами.

Обираючи правовий режим для машинно генерованих даних, перш за все, необхідно здійснити категоризацію величезного ма-

сиву даних, які створюються кожного дня. З цією метою необхідно, перш за все, виділити дві категорії даних – власні (персональні) та спільні дані (ті, які можуть передаватись третім особам і використання яких представляє певну цінність). Останні можуть бути поділені на три групи: 1) дані, якими можна ділитись з довіреними партнерами, зокрема, конфіденційні дані; 2) дані, якими можна ділитись із зацікавленими третіми особами, або індустріальні дані; 3) дані, якими можна ділитись із будь-ким, або відкриті дані [2]. Очевидно, найбільший інтерес з точки зору заснованої на даних економіки та розвитку бізнесу представляють індустріальні дані, щодо яких ведеться дискусія про можливість їх комерційного використання. При цьому постають два найважливіші питання – кому належать права на такі дані і які саме права тут виникають.

Структура Інтернету речей обумовлює наявність численних зв'язків між різноманітними суб'єктами, зокрема, виробниками пристроїв, постачальників комплектуючих частин, розробниками програмного забезпечення та компаніями, які аналізують масу зібраних даних. Тому важко визначити, хто з них у кінцевому підсумку може вважатися володільцем згенерованих машинами даних. Станом на сьогодні, володільцем даних вважається той, хто сам створив дані або має право власності на механізм, який створив дані [1].

Однак відповідно до положень чинного законодавства, дані не можуть належати суб'єктам на праві власності. Власники механізмів, що створюють дані, фактично лише контролюють доступ до даних, на якому праві їм належать такі дані станом на сьогодні законодавством не визначено. Тим не менш, будь-який представник бізнесу, як-от власник пристроїв, підключених до Інтернету, виробники комплектуючих, постачальники сировини тощо можуть мати зацікавленість у доступі до згенерованих машинами даних. Однак власники об'єктів, які генерують дані, досить часто не дають доступ іншим суб'єктам до даних протягом функціонування пристроїв, які їх генерують. Це дає підставу дослідникам стверджувати, що власники активів, які генерують дані, фактично мають подібну до права власності можливість адміністрування да-

них та право відмови у доступі до даних усім іншим зацікавленим особам, навіть незважаючи на те, що в них немає справжнього права власності на такі дані [2].

Станом на сьогодні права на машинно генеровані дані розглядаються також крізь призму права інтелектуальної власності. Об'єкт, який генерує дані, може збирати та використовувати дані датчиків для моніторингу продуктивності та власного стану, а також прогнозування та планування його технічного обслуговування. Такі дані можуть бути відправлені в центр обробки даних для хмарного зберігання та/або обробки. Внаслідок обробки та аналізу згенеровані машинами дані перетворюються на бази даних, які сьогодні визнаються об'єктами права інтелектуальної власності. Отже, організація, яка виконує роботу з обробки та аналізу даних на законних підставах отримує права інтелектуальної власності на такі оброблені дані. Вони можуть передавати права використовувати такі дані третім особам, до яких при цьому не переходять права інтелектуальної власності.

Сервіси обробки даних збирають дані для отримання додаткової цінності, що може принести комерційну вигоду іншим об'єктам. Коли виробник збирає дані щодо значної кількості об'єктів, можна виявити певні тенденції. Інформація, отримана в результаті аналізу активів одного виробника, може бути використана на користь інших, які стикаються з аналогічними проблемами. Цей зворотний зв'язок дозволяє іншим учасникам екосистеми отримати вигоду із взаємного досвіду та сприяє підвищенню ефективності всіх підприємств [1].

Отже, права інтелектуальної власності виникають на етапі, коли дані використовуються для конкретних цілей, наприклад, як частина нових досліджень і розробок. Наразі суб'єкти намагаються керувати згенерованими машинами даними через інститут прав інтелектуальної власності [2]. Однак це не дає відповіді на питання щодо прав не необроблені дані, згенеровані машинами.

На рівні Європейського Союзу (ЄС) на вирішення проблеми прав на машинно генеровані дані спрямований новий Закон про дані, який знаходиться на етапі обговорення. Закон про дані має

доповнити інші заходи ЄС для створення міцної основи для цифрової довіри, відкриття даних державного сектору, видалення цифрових кордонів, заохочення торгівлі даними, відкриття конкуренції та сприяння кращій безпеці на єдиному ринку ЄС. Закон спрямований на заохочення обміну даними між представниками бізнесу для полегшення доступу та використання даних для реалізації повного потенціалу економіки даних ЄС.

Одним із завдань в процесі розробки Закону про дані є надання відповіді на питання, чи можуть права на базу даних охоплювати машинно згенеровані дані та за яких обставин [4]. Отже, можливість реалізації прав на машинно згенеровані дані за допомогою права інтелектуальної власності на бази даних дискутується на рівні європейського законодавства.

Тим не менш, питання про необроблені дані, які генеруються пристроями, підключеними до Інтернету речей, поки що залишається відкритим. Видається, що правовий режим таких даних слід визначати виходячи з розуміння їх сутності. Нами вже підіймалися питання про те, що на сучасному етапі розвитку суспільства постає питання про необхідність розрізнення двох відмінних категорій – інформації та цифрових даних, які співвідносяться як загальне та конкретне [5]. Основна відмінність цифрових даних полягає в тому, що вони не призначені для обробки з метою перетворення на знання. Тому спробуємо відшукати відповідь, чи не слід вважати машинно генеровані дані цифровими даними, що дозволило б поширити на них правовий режим права власності.

Машинно генеровані дані мають цінність, оскільки містять остаточний запис у реальному часі про всі дії та дії користувачів, а також транзакції, програми, сервери, мережі та мобільні пристрої [6]. Дані, згенеровані машинами, мають значний потенціал для навчання та вирішення проблем. Використання таких даних може сприяти покращенню виробництва, удосконаленню налаштування бізнес-процесів, пришвидшення вирішення проблем та у цілому розвитку економіки. Однак все це можливо завдяки тому, що вони обробляються і перетворюються на знання щодо певної галузі, проблеми тощо. Отже, цінність згенерованих машинами

даних виникає саме завдяки їх обробці, самі по собі необроблені дані навряд чи мають економічну цінність. Тому такі дані є інформацією за своєю правовою природою та особливості їх використання, розпорядження ними та їх охорони мають визначатись правилами про інформацію як особливий об'єкт цивільних прав.

Література:

1. Hitchin P. The Industrial Internet of Things: Who Really Owns Your Data? URL: <https://www.ge.com/power/transform/article.transform.articles.2017.may.the-industrial-internet-of-thi#>
2. Seppala T. First considerations towards industrial data sharing practices. URL: <https://www.raute.com/blog/industry-insights/first-considerations-towards-industrial-data-sharing-practices/>
3. Sidaka S., Modral J. EU's possible Data Act: What can we anticipate from the Inception Impact Assessment and the Consultation? URL: <https://www.dataprotectionreport.com/2021/07/eus-possible-data-act-what-can-we-anticipate-from-the-inception-impact-assessment-and-the-consultation/>
4. Некіт К. Г. Цифрові дані та інформація як об'єкти права власності. *Часопис цивільного права*. 2021. № 42. С. 38-44.
5. What Is Machine Generated Data? URL: <https://www.indicative.com/resource/machine-generated-data/>

Кігай В. А., Заблоцька А. О.

курсанти факультету підготовки
фахівців для підрозділів стратегічних
розслідувань Дніпропетровського
державного університету внутрішніх
справ

Науковий керівник: Мітусова К. С

викладач кафедри цивільного права
та процесу Дніпропетровського
державного університету внутрішніх
справ

ВИКОРИСТАННЯ МУЛЬТИМЕДІЙНИХ ТЕХНОЛОГІЙ ПІД ЧАС ЗАНЯТЬ З ТРУДОВОГО ПРАВА

В останні роки увагу викладачів та науковців привертають мультимедійні технології. Під мультимедійною технологією ми розуміємо технологію, яка описує послідовність розробки, роботи та застосування інструментів обробки інформації. Щодо різних аспектів використання мультимедійних технологій в освіті, то автори обмежуються використанням технічних засобів навчання або комп'ютерних засобів навчання «нового» покоління, які мають характерні особливості: здатність переводити в різні форми (текст, звук, графіка, відео, анімація) та інтерактивна обробка інформації.

Мультимедійне заняття з трудового права дозволяє об'єднати неймовірну кількість цікавих завдань в одному занятті та залучає дедалі більше прихильників. Щоб створити на екрані динамічні моделі процесів, викладач має організувати цільове спостереження за змінами та пропорціями.

Зазначимо, що мультимедійні технології – одна з областей інформаційних технологій, яка найшвидше розвивається в освітньому процесі [1, с.65].

Варто виділити три основні завдання когнітивної комп'ютерної графіки в процесі викладання трудового права. Перше завдання – створити такі моделі уявлення знань, у яких можна було б

одними й тими самими засобами уявити як характерні об'єкти логічного мислення, і образи, із якими оперує образне мислення. Друге завдання – візуалізація людських знань, для яких поки що немає текстових описів. Третій – це пошук способів перейти від зображень до гіпотези про механізми і процеси, які ховаються за динамікою зображень, що спостерігаються.

Перегляд теоретичного матеріалу служить для ознайомлення студента та курсанта зі сторінками інформації у вигляді текстових та графічних слайдів, мультимедійних вставок, відеокліпів, демонстраційних та наочних програм. Студенти мають можливість перегортати інформаційні сторінки вперед або назад, дивитися на теорію, знаходити потрібний розділ у змісті.

Таким чином, переваги використання мультимедійних технологій (оперативне використання інформації, підключення аудіовізуального матеріалу та ін.) в організації навчального процесу не підлягають сумніву. Використання таких технологій в трудовому праві значно активізує навчальну інформацію, робить її більш зрозумілою та легкою для засвоєння.

Використання мультимедійних технологій під час викладання трудового права пов'язані з рішенням низки дидактичних завдань, вкладених у підвищення освітнього рівня під час викладання цієї дисципліни.

Більшість мультимедійних уроків побудовано за такою схемою:

1. Мотивація до навчання – невеликий вступний матеріал. Мотивація часто охоплює проблемні теми.

2. Оголошення теми та очікуваних результатів заняття.

3. Теоретична частина заняття – засвоєння навчального матеріалу: робота з концепціями, невеликими фрагментами тексту з педагогічною інформацією. Можливе згрупування студентів та курсантів у невеликі творчі групи для вирішення практичних завдань.

4. Практична частина заняття – після ознайомлення зі змістом мультимедійної програми практична робота продовжується.

5. Короткий зміст завдання – включає міркування про проведення заняття.

Сучасний стан застосування мультимедійних технологій характеризується не спорадичним, а систематичним використанням комп'ютерів. Основна проблема, що виникає, – це розробка методів комп'ютеризації навчання [2, с.90].

Можлива або повна реструктуризація та орієнтація на створення нових комп'ютеризованих курсів чи впровадження методики з частковою комп'ютерною допомогою. Однак перехід на мультимедійні технології та системи необхідний. Відомо, що можливості використання мультимедійних технологій у навчальному процесі є дуже різноманітними. Це пов'язано зі здатністю комп'ютера відображати, зберігати, обробляти і передавати великі обсяги різного роду інформації, а також ефективно управляти інформаційними ресурсами.

Таким чином, широке використання мультимедійних інструментів у навчальних класах не лише надасть учням інформацію та позитивно вплине на їхню обізнаність та загальну освіту, але також сприятиме кращому навчанню.

Список використаних джерел

1. Трудове право України [текст] підручник / За загальною редакцією М. І. Іншина, В. Л. Костюка, В. П. Мельника. Вид. 2-ге, перероб. і доп. Київ: Центр учбової літератури, 2016. 472 с.
2. Трудове право України: навчальний посібник / кол. авторів; за ред. В. О. Кучера. – Львів: ЛьвДУВС, 2017. 564 с.

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ СУСПІЛЬНИХ ВІДНОСИН В СФЕРІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ІНТЕРНЕТУ РЕЧЕЙ

Мисливий В. А.

доктор юридичних наук, професор,
професор кафедри інформаційного,
господарського та адміністративного
права КПІ імені Ігоря Сікорського.

ФОРМИ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ У ЦИФРОВОМУ ВИМІРІ

Можливість застосування інформаційних технологій (далі – ІТ) у кримінальному праві, у першу чергу, ставить питання щодо практичних реалій їх використання у правовому середовищі, що значною мірою залежать від ступеня розвитку таких систем, а також панівної системи права, в якій судовий прецедент не відіграє суттєвої ролі, що саме притаманно вітчизняній системі права.

Позитивний результат застосування ІТ, а в подальшому – елементів штучного інтелекту (далі – ШІ), значною мірою буде залежати від належного рівня прорахунків ризиків та специфічних аспектів, пов'язаних з ресурсними, технічними, організаційними та іншими можливостями їх впровадження, а також складністю кримінально-правової матерії. Важливим фактором у цій сфері також буде рівень правової освіти, професійного досвіду, правової культури та правосвідомості правників, що впливатиме на їх довіру до інновацій у правозастосовній діяльності.

У правовій сфері ІТ та елементи ШІ потенційно можуть використовуватися на різних рівнях, проте ці досягнення цифрового суспільства у вітчизняному кримінальному праві поки не отримали належного застосування, що не сприяє ефективній реалізації

наявного арсеналу кримінально-правових засобів у протидії та запобіганні злочинності.

У зв'язку з цим доцільно розглянути можливості застосування ІТ при вирішенні сутнісних питань кримінального права, що інтегруються в рамках реалізації форм кримінальної відповідальності в процесі кримінального судочинства.

Можливість і доцільність такого підходу вдається прийнятною, виходячи з того, що зіставлення певних стандартів і шаблонів, моделювання відповідних правових висновків вже сьогодні є цілком доступним для певних програмних продуктів ІТ, у тому числі з елементами ШІ. Звичайно, що чимало прибічників традиційного підходу у правозастосуванні вважають, що існуючі інтелектуальні системи не спроможні повністю взяти на себе функції слідчого або судді, оскільки прийняття ними таких рішень – це сфера високої складності, а, як відомо, правова діяльність тісно поєднується з когнітивною та емоційною компетентностями. З цим важко не погодитись, адже, дійсно, такі категорії, як «кримінальна відповідальність», «зворотна дія закону», «суворий вид покарання» і багато інших вимагають поєднання різних когнітивних рівнів при оцінці певних фактів, правових приписів, їх тлумаченні і розмежуванні, пошуку та обранні обґрунтованих правових позицій при застосуванні кримінально-правових інститутів та їх норм. Разом з цим, звернення до питань застосування ІТ показує, що кримінальне право є однією із галузей права, в якій цифрові технології заслуговують на їх впровадження. Розглянемо це на прикладі такої теоретично-прикладної проблеми, як форми реалізації кримінальної відповідальності.

У теорії кримінального права загальноновизнано, що кримінальна відповідальність може бути реалізована в трьох формах: 1) в осуді особи, яка вчинила кримінальне правопорушення, без призначення їй покарання (зокрема, ч. 4 ст. 74 КК України); 2) в засудженні особи з призначенням їй покарання, від реального відбування якого вона звільняється з можливістю застосування інших заходів кримінально-правового впливу (ч. 1 ст. 75 КК України); 3) в засудженні особи з призначенням їй покарання з його реальним відбуванням.

Будь-яка з названих форм реалізації кримінальної відповідальності вимагає точної кримінально-правової кваліфікації вчиненого діяння, а отже визначення відповідних статей Кримінального кодексу України (далі – КК), які передбачають вчинене діяння. При цьому кожне з діянь підлягає самостійній кваліфікації, а її результатом виступає формула кваліфікації, яка передбачає вчинене діяння як кримінальне правопорушення. Водночас, визначення формули кваліфікації потребує здійснення диференціації та формалізації окремих кримінально-правових інститутів, значної кількості норм, категорій, елементів та ознак, що становлять зміст того чи іншого посягання, його ступінь тяжкості, стадії вчинення, ознаки співучасті, розмір заподіяної шкоди та багато інших. Формула кваліфікації також має враховувати законодавчі та/або підзаконні нормативно-правові акти (стаття, частина, пункт, параграф, абзац), що слугують встановленню детального змісту ознак складу кримінального правопорушення. У подальшому системне інтегрування вказаного комплексу ознак та їх аналіз за допомогою ІТ дозволяє визначити відповідну формулу кваліфікації діяння.

Таким чином, формула кваліфікації – це виражене буквами, числами та окремими розділовими знаками умовне позначення співвідношення відповідних елементів в системі кримінального права. І хоча поняття «формула» в цьому контексті не є аналогом її математичного синоніму, його вживання в понятійному апараті кримінального права цілком виправдане. Адже формула кваліфікації як кримінально-правова категорія є стислим і точним визначенням співвідношення між ознаками вчиненого діяння та ознаками кримінального права, яку можна застосовувати до відповідного конкретного випадку вчинення кримінального правопорушення.

Яким би ускладненим не був перебіг подій та обставин при вчиненні одного чи множини посягань, тяжкість спричинених злочинною поведінкою наслідків та інші кількісно-якісні характеристики діяння, всі вони вимагають відповідної конкретної кримінально-правової оцінки з огляду на формалізовані в законі про кримінальну відповідальність ознаки, що у подальшому зна-

ходять своє місце у формулі кваліфікації кримінального правопорушення.

Крім того, слід враховувати, що, незважаючи на певну кримінально-процесуальну перманентність формули кваліфікації кримінального правопорушення під час кримінального судочинства, її остаточне визначення при притягненні особи до кримінальної відповідальності залишається обов'язковим кримінально-правовим компонентом.

Іншою важливою складовою форм реалізації кримінальної відповідальності є призначення особі, визнаної винною у вчиненні кримінального правопорушення, кримінального покарання. Визначення покарання, як і кваліфікація діяння, також вимагає його окреслення через відповідну формулу, оскільки в кримінальному праві покарання характеризується багатьма ознаками, які на підставі їх формалізації дозволяють визначати його за допомогою формули – як вираженого буквами, числами та окремими знаками пунктуації умовного позначення співвідношення відповідних елементів цього інституту кримінального права. У першу чергу це стосується врахування видів і розмірів покарання та їх особливостей застосування: загальних засад призначення покарання, обставин, що пом'якшують або обтяжують покарання, особливостей та правил призначення покарання тощо. У цьому ж контексті можливо розглядати підстави та умови звільнення від покарання та його відбування.

Таким чином, досягнення за допомогою ІТ точного визначення формул кваліфікації та покарання кримінального правопорушення, їх повне та всебічне обґрунтування з урахуванням вимог кримінального законодавства є ефективним інструментом визначення форми реалізації кримінальної відповідальності.

Аналіз багаторічної судової практики з огляду на вивчення вироків в Єдиному державному судовому реєстрі показує, що у багатьох випадках судді при визначенні кваліфікації кримінальних правопорушень не враховують міжнародні документи та національне галузеве законодавство, яке регламентує порядок та правила безпеки в окремих сферах, довільно або помилково тлумачать

певні ознаки складів кримінальних правопорушень, не враховують або не мотивують наявність певних пом'якшуючих чи обтяжуючих покарання обставин і т. ін. Ці та інші недоліки викликають порушення законності, винесення необґрунтованих судових рішень, що негативно впливає на авторитет судової влади та стан правосуддя в цілому.

Звичайно, що порушення, які припускаються при застосуванні кримінального законодавства, можуть бути різноманітними, але їх неприпустимість є беззастережною, адже кримінальне право є однією з найгостріших за впливом зброєю держави. У цьому сенсі ми переконані, що використання ІТ в якості інтелектуального помічника детектива, дізнавача, слідчого, прокурора, судді, захисника аналогічно тому інструменту, що допомагає лікарям точно діагностувати захворювання та рекомендувати обґрунтований протокол лікування.

Безумовною перевагою ІІІ є його здатність вивчати величезні обсяги інформації, визначати закономірності, які навіть кваліфікована людина може не помітити або пропустити, надавати необхідні висновки при прийнятті відповідних правових рішень, зокрема при кваліфікації кримінальних правопорушень та призначенні покарань за їх вчинення.

Адже важко уявити ситуацію, за якої ІТ чи ІІІ з якоїсь причини «пропустить» у змісті вироку при кваліфікації чи призначенні покарання певну конститутивну ознаку складу злочину або обставину, що обтяжує покарання, чи не відзначить необхідність обґрунтувати те чи інше положення вироку, яке суд зобов'язаний мотивувати у вироку, але цього не зробив. У таких випадках відповідна програма за результатами аналізу судового вироку чи іншого процесуального документа повинна «заблокувати» можливість його винесення, запропонувавши судді (суддям) усунути відповідні прогалини, помилки чи інші недоліки. При цьому поки що не має підстав для застережень, що на сучасному етапі цифровізації впровадження ІТ чи елементів ІІІ замінить собою або принизить роль судді у кримінальному судочинстві, адже вони будуть лише надійним допоміжним технологічним засобом в його діяльності.

Ми не випадково звернулись до питань обґрунтованості «формули кваліфікації» і «формули покарання» як кримінально-правових категорій, адже вони є важливими складовими кримінального судочинства, оскільки саме ці формули обов'язково постановляються судом в резолютивній частині обвинувального вироку, який для підсудного визначає не лише кару за вчинене кримінальне правопорушення, а й має бути вердиктом справедливості кримінальної відповідальності.

Розгляд вказаних питань обумовлюється необхідністю перформатування чинного кримінального права, спроба якого здійснюється в рамках його реформування шляхом розробки нової моделі кримінального законодавства. Сьогодні одним із напрямків законотворчої роботи є спроба здійснення цифровізації закону про кримінальну відповідальність, що, зокрема, означає впровадження ІТ в діяльність, пов'язану із застосуванням норм кримінального права. Звернення до цифрових технологій є не лише вимогою часу, але й цілком перспективним напрямом поєднання зусиль технічних та правових наук, а тому, безумовно, заслуговує на підтримку [1].

Список використаних джерел

1. Кримінальний кодекс України (проект). URL: <https://newcriminalcode.org.ua/upload/media/2021/11/15/1-kontrolnyj-tekst-proektu-kk-14-11-2021-oznaky.pdf> (дата звернення: 19.11.2021 р.)

Капліна О. В.

доктор юридичних наук, професор,
завідувач кафедри кримінального
процесу Національного юридичного
університету імені Ярослава Мудрого

ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ ПРОБЛЕМИ КРИМІНАЛЬНОГО ПРОЦЕСУ УКРАЇНИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СУСПІЛЬСТВА

Однієї з тенденцій розвитку сучасного світу є всеохоплюючі процеси цифровізації, яка пронизує всі сфери людської діяльності та здійснює істотний та різноплановий вплив на локальному, регіональному та глобальному рівнях. Без перебільшення можна казати, що цифрові технології значно модернізували світ та соціальну дійсність. Разом з тим очевидним є амбівалентний вплив цифровізації. З одного боку – вона створює невідані раніше можливості у всіх галузях людської життєдіяльності, вплітає інформаційні технології у побут, робить світ прозорим, несе в себе можливості для значного покращення життя, перетворення економіки, управління, медицини, сфери послуг, спрощує та прискорює процеси комунікації, з'єднує, долаючи тисячокілометрові відстані, тощо. З іншого боку, цифрові технології породжують негативні наслідки у вигляді нових форм злочинності у сфері високих технологій, так звані кіберзлочини.

За допомогою комп'ютерних технологій вчиняються самі різні кримінальні правопорушення. Переважна більшість їх складів міститься у розділі XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України. Втім, переліком цих правопорушень взагалі не вичерпуються всі суспільно небезпечні діяння, які можуть бути вчинені за допомогою комп'ютерних мереж. Не є сталою термінологія, адже у науковому та правозастосовному дискурсі використовуються такі поняття, як «комп'ютерні злочини», «кіберзлочини», «злочини у сфері інформаційних відносин»,

«злочини в сфері комп'ютерних технологій», «у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» тощо. Чинне законодавство не дає визначення відповідних понять, що не дозволяє класифікувати всі можливі кримінальні правопорушення що вчиняються за допомогою сучасних комп'ютерних та цифрових технологій. Вони гіпотетично можуть бути вчинені різними способами, зокрема, за допомогою викрадення комп'ютерної інформації, здійснення кібератак, розповсюдження шкідливих програм, так званих вірусів, створення несправжніх інтернет-аукціонів тощо, що викликає складності під час їх кваліфікації. Найчастіше такі кримінальні правопорушення кваліфікуються як загальнокримінальні злочини. Наприклад, за ч. 3 ст. 190 КК України «Шахрайство», як шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки. При використанні підроблених електронних засобів доступу до банківських рахунків, слідчі кваліфікують дії винної особи за ст. ст. 200 КК України «Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення». Збут і розповсюдження порнографічних предметів з використанням електронно-обчислювальної техніки кваліфікується за ст. ст. 301 КК України. Вилучення посадовою особою фінансової установи з банківських рахунків клієнтів електронних коштів, які перебували у правомірному володінні потерпілого, кваліфікується за ч. 2 ст. 191 КК України.

Крім того, само узагальнююче поняття, яке зараз використовується, вже є звичним для пересічних громадян та правників – «кіберзлочини» – не відображає суті суспільно небезпечних діянь, що вчиняються, адже КК України всі кримінально карані суспільно небезпечні винні діяння поділяє на злочини та кримінальні проступки (ст. 12 КК України).

Ми є свідками поступового опанування правниками нової термінології, яка є по суті технічною, втім без усвідомлення її змісту слідчими, прокурорами, суддями неможливо здійснювати досудо-

ве розслідування, призначити експертизу, оцінювати докази, ухвалювати рішення. Серед неологізмів, якими повинні оперувати правники такі нові поняття, як «кібергруммінг», «дефейс», «кардинг» (англ. carding), «кард-треппінг»; «кеш-треппінг»; «програмний скімінг»; «проксі-сервер»; «прямий діспенс»; «кіберсквотінг» тощо.

Сьогодні жертвою комп'ютерних технологій стають не лише особи, а й держави стосовно яких можуть вестися кібервійни, кібертероризм, кібершпигунство, що призводить до суттєвих загроз національній безпеці або безпеці національної економіки.

Особливість «кіберзлочинів» полягає в тому, що вони: 1) мають дистанційний або транснаціональний характер; 2) часто є латентними (в тому числі прихованими від потенційної жертви); 3) є інтелектуально продуманими, «нетрадиційними» з точки зору об'єктивної сторони їх вчинення; 4) є триваючими, багатоепізодичними, або такими, що вчиняються одночасно в значних просторових межах; 5) пов'язані з можливістю легкого знищення їх слідів; 6) в силу специфіки ускладнюють запобігання їм, припинення або розкриття; 7) потребують залучення до їх розкриття відповідних фахівців та засобів, без яких неможливо уявити збирання «цифрових доказів».

Крім того, говорячи про другий негативний аспект впливу цифровізації на суспільство слід згадати про особливості розкриття злочинів, які вчиняється за допомогою комп'ютерних технологій, або про розкриття злочинів, що є «традиційними» для системи кримінальної юстиції, але здійснення досудового розслідування по них стикається з відсутністю належного правового регулювання, прогалиністю унормування особливостей збирання та перевірки «цифрових доказів», їх оцінки у судовому розгляді.

Обидва напрями впливу цифровізації на кримінальне провадження, у свою чергу, пов'язані із необхідністю відповідного законодавчого забезпечення, яке очевидно відстає від стрімкого розвитку цифрових технологій, а також головне – забезпечення прав людини у новій цифровій реальності. Аналогічні проблеми виникають майже у всіх країнах світу.

Новий «цифровий світ», який стрімко змінюється під впливом сучасних цифрових технологій та перетворює науково-фантастичні сюжети у реальність, є мейнстримом серед представників кібернетики, інформатики, політології, соціології, філософії тощо. До осмислення необхідності юридифікації цифрової реальності звертаються також представники різних галузей права. Що стосується кримінального процесуального права, то науковий доробок лише за останні роки поповнений низкою досліджень стосовно «цифровізації» кримінального провадження. Втім слід констатувати, що вітчизняні науковці переважно спрямовують свої інтелектуальні зусилля на окремі сегменти використання досягнень цифрового прогресу в певній галузі права, або стосовного окремого інституту права (речових доказів; документів; вчинення злочинів за допомогою цифрових технологій, електронних валют, шкідливого програмного забезпечення тощо). Кримінальному процесуальному праву бракує комплексного наукового дослідження, в якому би системно були розглянуті «цифрові проблеми» сучасного кримінального судочинства.

Всі ці фактори вказують на необхідність наукового осмислення проблем, що виникають зв'язку з цифровізацією суспільства та у кардинальній зміні підходів до національної цифрової безпеки, кібербезпеки та трансформації кримінального судочинства з їх урахуванням. Тобто масштаб цифрових трансформацій та викликів, які стоять перед нами, повинен дорівнюватися масштабу перетворень у кримінальному процесуальному законодавстві, інакше проблеми залишаться без свого законодавчого вирішення, а правозастосовна практика без належного правового інструментарію.

Уявляється, що процеси цифровізації здійснюють в основному потрібний вплив на трансформації, які повинні здійснюватися в кримінальному процесуальному праві.

По-перше, мова йде про оптимізацію кримінальної процесуальної форми, використання цифрових технологій під час досудового розслідування чи судового розгляду кримінальних проваджень.

По-друге, на своє вирішення чекають питання стосовно трансформації відповідно до вимог цифровізації засобів доказування

та їх законодавчого «оформлення». Особливості кримінальних правопорушень, що вчиняються за допомогою технічних засобів вимагають від органів досудового розслідування неортодоксальних, інноваційних способів їх розкриття.

По-третє, обговоренню та вирішенню підлягає ключова проблема доказового права – доцільності розширення переліку видів доказів, передбачених ч. 2 ст. 84 КПК за рахунок запровадження окремого виду – цифрового доказу.

Крім того, окремим напрямом є вирішення проблеми дотримання прав людини під час кримінального провадження, забезпечення так званого права на цифрову прайвесі, що повинно пронизувати всі названі вище аспекти правових та доктринальних трансформацій.

Звичайно, що процеси вдосконалення нормативного регулювання повинні йти паралельно з вивченням досвіду зарубіжних партнерів, врахуванням підходів інституцій ООН, досвіду міжнародних інституцій.

Каткова Т. Г.

кандидат юридичних наук, доцент,
доцент кафедри земельного та
аграрного права Державного
біотехнологічного університету

ПРАВОВЕ РЕГУЛЮВАННЯ NFT

У сучасному світі досить популярними стають цифрові активи та формується їх ринок. Одним з елементів такого ринку, який стрімко набирає капіталізації, є NFT. NFT (non-fungible tokens) – це сучасний цифровий актив, який існує на блокчейні та є невзаємозамінним по своїй суті [1]. Оскільки NFT працює на блокчейні, потрібно пару слів зазначити про цей реєстр.

У дослівному перекладі з англійської блокчейн – це ланцюжок блоків (block – блок, chain – ланцюжок). Механізм функціонування блокчейну та протокол біткойну були вперше описані у статті

С. Накамото. На сьогоднішній день, у літературі, а також у міжнародних стандартах пропонується досить велика кількість визначень блокчейна, які враховують ті чи інші його характеристики. Так, наприклад, О. В. Билінкіна відмічає, що блокчейн – це різновид розподіленого реєстру, призначеного тільки для додавання інформації, дані до якої записуються блоками з використанням криптографічних алгоритмів таким чином, що кожен новий блок включає інформацію про попередній блок. Безпека даних у блокчейні забезпечується за рахунок децентралізованого зберігання інформації та застосування криптографічних алгоритмів. Децентралізація є ключовою характеристикою блокчейну. Якщо облік транзакцій ведуть конкретні організації та записи про транзакції зберігаються тільки в одному місці, то неминучі ризики, пов'язані із внесенням змін до раніше проведених транзакцій. Технологія блокчейн знижує такі ризики, тому що пропонує систему обліку на основі розподілених реєстрів. У блокчейні дані зберігаються не на сервері якогось одного суб'єкта, але в безлічі незалежних комп'ютерів користувачів, об'єднаних через Інтернет. Блокчейн є новий підхід до створення баз даних, ключовою особливістю якого є відсутність єдиного центру управління [2].

Слід відмітити, концепція NFT продовжила «справу, розпочату блокчейном» і по суті запропонувала реалізацію ідеї створення програмованого цифрового дефіциту, який дозволив запустити процес формування крипто-предметів колекціонування. На відміну від криптовалюти, де всі токени ідентичні і мають родові ознаки, а значить взаємозамінні, NFT токени обмежені в своїй кількості і кожен з них є унікальним [3].

Згідно з умовами більшості платформ, предметом купівлі-продажу є токени, сертифікати або акції, які, як зазначено на сайтах платформ, подібні до купівлі частки у творі мистецтва. Мінімальна сума інвестицій у середньому становить від \$500 до \$5000. Суть ідеї полягає в тому, що власник реального предмета мистецтва, який бажає його продати, створює на блокчейн-платформі якийсь віртуальний аналог свого права власності на твір. Це віртуальне право власності, виходячи із вартості предмета мистецтва, дро-

битися на рівні частини (токени, акції, атоми тощо, найменування відрізняються залежно від платформи). Ці частини пропонуються для купівлі на ринку платформи іншим користувачам, вони можуть надалі відчуватися покупцями на цій же платформі, приносячи прибуток за умови зростання загальної вартості твору (або збитки при падінні вартості).

Сам оригінал твору в його матеріальному сенсі, як запевняють платформи, зберігається в захищених сховищах, музеях або в самого продавця, якщо він зберігає за собою якусь частку в праві власності. Власник та платформа отримують від покупців кошти. У цьому покупці віртуальних часток (токенів, акцій) що неспроможні ні розпорядитися самим предметом мистецтва, ні користуватися чи інакше мати їх у матеріальному сенсі. Вони набувають лише певного посвідчення (сертифікат чи свідоцтво), яке саме собою є активом, може бути продано (поступлено) у межах цієї ж блокчейн-платформи.

Блокчейн безперечно важливий для мистецтва. Насамперед для відстеження справжності творів, щоб у колекціонерів перед очима була історія покупок і продажу твору мистецтва. І аукціонні будинки це цінують, вони можуть ще сильніше тоді нарощувати ціну конкретному автору, знаючи що і за скільки продалося. Але інколи продаж «на хайпі» роздмухує ціну на твори мистецтва і це викликає ризик перетворення вартості на мильну бульбашку.

Запропонована форма інвестицій далека від набуття права власності на частку у предметі мистецтва у загальноприйнятому значенні. До придбання пропонуються цифрові права, що регулюються особливим чином. На даний момент в жодній країні світу не існує повноцінного та несуперечливого законодавства у галузі цифрових прав. У більшості країн до подібних операцій безпосередньо або за аналогією застосовується регулювання цінних паперів чи інших фінансових інструментів [4].

Аналіз NFT дозволяє виділити низку питань щодо правового регулювання:

1. Невизначеність правового статусу цифрових токенів.

У правилах більшості платформ, що продають цифрові права (токени) частку власності в предметах мистецтва, нечітко і техно-

логічно заплутано прописано зміст конкретних прав, укладених у запропонованих токенах. Правовий статус цифрових токенів необхідно визначати окремо у кожному конкретному випадку, виходячи з умов інвестиційної платформи та країни її регулювання. Якщо в країні приймається закон про цифрові активи, існує ризик закриття платформи з усіма активами і сервісами.

2. Неврегульованість оподаткування угод із токенами.

Ймовірно, при прийнятті закону цифрові токени будуть розглядатися як цінні папери у разі отримання інвесторами прибутку.

3. Відсутність гарантій захисту інвестицій.

Власник токена не має грошових прав, не бере участі в прибутку, а значить його актив не може бути використаний як інструмент інвестування.

4. Блокчейн не перевіряє справжність робіт і не верифікує автора на вході.

Іншими словами будь-яка особа може завантажити чужі цифрові зображення, видавши їх за свої. І при цьому не обов'язково вона здійснить правопорушення з юридичної точки зору. Особливо така можливість є очевидною для оцифрованого традиційного мистецтва, термін авторських прав на яке закінчився. Це означає, що під загрозою знаходяться раритетні предмети, що становлять музейні фонди, але при цьому популярні і дорогі, які можуть легко перейти в приватні цифрові активи [3].

5. Відсутність відповідальності блокчейн-платформ.

На сайтах більшості платформ заявлено, що вони самі відбирають предмети мистецтва для подальшого продажу, гарантують їхню справжність, проводять експертизу, готують доступні покупцям звіти про провенанс та стан твору. Однак якщо відкрити користувацькі угоди платформ, то в більшості випадків можна побачити умови, що жорстко обмежують будь-яку відповідальність платформ перед потенційними покупцями. Найчастіше вказується, що платформи, а також особи, що володіють ними, директори та співробітники не несуть жодної відповідальності за будь-які збитки користувача, що виникли в результаті використання платформи, продажу та зберігання токенів, інших послуг та розміще-

ної інформації, а також за технічні збої та недоступність сайтів та сервісів. Найчастіше вказується, що користувачі використовують платформу на власний ризик.

Сьогодні в Україні триває процес правового регулювання цифрових активів. Так, Президент України В. Зеленський повернув до Верховної Ради зі своїми пропозиціями Закон «Про віртуальні активи» (законопроект № 3637), який народні депутати ухвалили 8 вересня 2021 року. Цей документ визначає засади державного регулювання обігу віртуальних активів. Так, згідно із законом, регулювання ринку віртуальних активів здійснюється різними державними органами залежно від виду таких активів, зокрема й шляхом створення нового органу центральної виконавчої влади. Створення нового органу, як передбачено цим законом, потребуватиме значних видатків з державного бюджету. Президент України пропонує віднести регулювання обігу віртуальних активів до компетенції Національної комісії з цінних паперів та фондового ринку.

Література:

1. Меше О. NFT: майбутнє мистецтва вже сьогодні. URL: <https://legalhub.online/blog/nft-majbutnye-mystetstva-vzhe-sogodni>
2. Былинкина Е. В. Блокчейн: правовое регулирование и стандартизация. URL: <https://cyberleninka.ru/article/n/blokcheyn-pravovoe-regulirovanie-i-standartizatsiya/viewer>
3. Сімсон О. Цифрове мистецтво, блокчейнізація та NFT: юридичний розбір. URL: <https://ilti.com.ua/czifrove-misteczstvo,-blokcheyn%D1%96zac%D1%96ya-ta-nft-yuridichnij-rozb%D1%96r>
4. Куликова К. Блокчейн-платформи в искусстве: юристы предупреждают. URL: <https://www.pgplaw.ru/analytics-and-brochures/articles-comments-interviews/blockchain-platform-in-art-lawyers-warn/>

Костенко О. В.

доктор філософії (Ph.D.) з юридичних наук, завідувач наукової лабораторії теорії цифрової трансформації і права наукового центру цифрової трансформації і права ДНУ «Інституту інформації, безпеки і права НАПрН України»

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЗАСТОСУВАННЯ ЦИФРОВИХ ОСОБИСТОСТЕЙ ТА АВАТАРІВ

Поняття крадіжка особистих даних, як термін вперше сформульовано у Великій Британії та США у 1964 році, і характеризує навмисні дії, спрямовані на незаконне заволодіння та використання чужих особистих даних, з метою отримання фінансової вигоди, матеріальних благ або привілеїв. Протягом 50 років крадіжки особистих даних в основному здійснювалися стосовно таких відомостей як номер паспорту, посвідчення водія, номер банківського рахунку або кредитної картки, PIN-кодів, електронних підписів, відбитків пальців, паролів або будь-якої іншої інформації, яка може бути використана для доступу до фінансових або матеріальних ресурсів людини.

Розвиток інформаційно-комунікаційних технологій [1.с.264] досягнення науково-технічної революції 4.0, соціальні мережі створили нові напрями консолідації даних про людину, а саме: її цифрових двійників – цифрову особистість та цифровий аватар (далі – аватар).

Згідно первинної моделі соціальні мережі мали на меті стати платформою для спілкування та обміну ідеями між користувачами, висвітлювання подій та життя конкретної людини. Однак, на сьогодні мета соціальних мереж значно змінилася, а інформація про громадянина набула ваги цифрової особистості, яка нині є найбільш актуальною. Так, тепер соціальні мережі формують певний стереотип цифрової особистості, так званий «happy man» (щаслива людина). З сторінок «глянцевих» журналів в цифрове

середовище переноситься концепція успішної людини та її ідеальне життя. Проте цифрова особистість «happy man» у соціальних мережах і реальна людина – це дві різні сутності.

Наступним етапом технологічного розвитку цифрової особистості стає аватар. Ще недавно аватарами вважалися 2D іконки в інтернет-середовищі або 3D моделі у віртуальних реальностях [2. с.224] та світах комп'ютерних чи он-лайн ігор. Наразі технологічно аватари мають більш розширену структуру та призначення, а їх створення стало більш доступним. Процес створення аватара проходить чотири етапи: за допомогою автоматизованих програм формують реалістичну 3D-модель; комп'ютерною анімацією CGI захоплюють та синтезують рухи тіла та міміку прототипу; із застосуванням нейромереж та програм зі штучним інтелектом [3.с.19] шляхом машинного навчання аналізують всі дії прототипу, синтезують модель поведінки, формують мовлення, наділяють здатністю сприймати мову людини та розвивати власний емоційний інтелект; програмують ігровий двигун управління аватором. На даному етапі розвитку суспільних відносин масове застосування таких технологій має незначні потреби.

Аватари наповнюються різноманітною інформацією про реальну людину-прототип використовуючи при цьому різні джерела інформації, які поки що не сконцентровані в одному інформаційному банку аватарів.

Так до даних, які традиційно надходять з вищевказаних архаїчних носіїв ідентифікаційних даних [4. с.201] додається інформація із: електронних медичних карток про біологічні параметри та стан здоров'я; банківських систем і систем типу «ДІЯ» про голос, риси обличчя та рухи, дані документів; пристроїв IoT, які у реальному часі фіксують різні фізичні параметри людини або підтримують життєво важливі функції організму; нейромереж і програм зі штучним інтелектом, які аналізують дії прототипу в цифровій екосистемі (від політичних поглядів до інтимних проблем) прототипу в цифрових мережах; даних з державних реєстрів; окремих програм на кшталт «віртуальна примірювальна», які швидко створюють 3D копію людини тощо.

У 2019-2020 роках у соцмережах з'явилося понад 50 нових віртуальних людей-аватарів. Відносини між людиною та технологіями зі штучним інтелектом все більше персоналізуються. Фактично цифрова особистість та аватари стають найціннішими державними інформаційними ресурсами і потребують захисту не тільки в галузі інформаційної безпеки, а й визнання їх в законодавчому полі та їх регулювання правового забезпечення.

Перш за все, держава повинна виявляти найбільшу зацікавленість в технологічному, етичному і правовому регулюванні застосування технологій цифрової особистості та аватарів. Оскільки це дає змогу державі більш раціонально та ефективно використовувати людські ресурси, спрямовувати людей на навчання або роботу, до яких людина більше пристосована, формувати галузеві науково-технічні кадри та кадрові резерви, поліпшити загальний стан здоров'я населення, оптимізувати багато процесів в яких приймає участь людина тощо. Але застосування державою технологій цифрової особистості та аватарів може нести ризики формування авторитарної держави під гаслом «забезпечити кібербезпеку людини та його аватара в середині формуючихся метавсесвітів», що може суттєво обмежувати права і свободи громадян. Наприклад, деякий час через технічні особливості системи «ДІЯ» неможливо було отримати електронний витяг із медичних реєстрів про вакцинацію від COVID-19, а механізм ідентифікації користувача із задіянням «3D-ідентифікації» суттєво ускладнював користувачу отримання такого витягу за наявності щеплення.

На нашу думку тезис «забезпечити кібербезпеку людини та його аватара в середині формуючихся метавсесвітів» крім позитивних тенденцій несе приховану загрозу можливості гібридних кібервійн в кіберпросторі, за аналогією військового втручання з метою «захисту населення іншої держави за мовними або національними ознаками».

Крім цього, залишається відкритим проблема «автономного» функціонування аватара. Тобто якщо дані, які формують аватар, знаходяться на єдиному ресурсі, то виникає спокуса або гіпотетична можливість застосування цифрового двійника людини без

згоди та відома людини-володільця аватара – вчинити електронний кіднепінг.

Електронний кіднепінг може мати мету доступу до фінансових та матеріальних ресурсів людини-володільця, а може використовуватися для скоєння терористичних дій не тільки в кіберпросторі але й проти фізичних об'єктів, людей та суспільства.

Саме тому, мусимо констатувати, що на сьогодні законодавство не здатне здійснити правову регуляцію суспільних процесів, які складаються з використанням технологій цифрової особистості та аватарів. Тож потрібно детальніше проаналізувати ризики використання технологій цифрової особистості та аватарів, які можуть обмежувати права і свободи людини. На нашу думку ці процеси розвиваються стрімко і розповсюдження їх у всі сфери суспільного життя неминуче.

Доцільно розпочати дослідження у сфері інформаційного права в напрямі розробки основних доктринальних та нормативно-правових понять, шляхом створення сучасного понятійно-категоріального апарату, розробки наукових підходів регулювання суспільних відносин із застосуванням цифрових особистостей та аватарів, формування пропозицій модернізації Кодексів, в тому числі Кримінального, визначення правопорушень стосовно крадіжки та незаконного використання цифрових особистостей та аватарів, формування пропозицій із державного примусу за скоєння таких злочинів тощо.

Для формування понятійно-категоріального апарату пропонуємо авторське визначення аватара та цифрової особистості та електронний кіднепінг:

Аватар – дані в цифровій формі, достатні для відтворення прототипу людини-володільця аватара в цифровій екосистемі (метавсесвіті) із максимальною достовірністю та правами, встановленими законодавством.

Цифрова особистість – визначені законодавством необхідні та достатні дані в цифровій формі, за якими здійснюється ідентифікація людини-володільця в цифровій екосистемі (метавсесвіті).

Кіднепінг аватара або цифрової особистості – незаконний доступ, заволодіння, використання, модифікація та знищення аватара/або цифрової особистості.

Література

1. Беляков К. І. Енциклопедія соціогуманітарної інформології / корд. проекту та заг. ред. проф. К. І. Беляков. – Київ: Видавничий дім «Гельветика», 2020. – Т. 1. – С.263-267.
2. Дзьобань О. П. Енциклопедія соціогуманітарної інформології / корд. проекту та заг. ред. проф. К. І. Беляков. – Одеса: Видавничий дім «Гельветика», 2021. – Т. 2. – С.224-228.
3. Баранов О. А. Інтернет речей і штучний інтелект: витoki проблеми правового регулювання. ІТ-право: проблеми та перспективи розвитку в Україні : зб. матеріалів II Міжнар. наук.-практ. конф. (м. Львів, 17 лист. 2017 р.). Львів, НУ «Львівська політехніка». 2017. С. 18–42.
4. Kostenko, O. V. Identification data management: legal regulation and classification. Науковий журнал «PNAP. Scientific Journal of Polonia University Periodyk Naukowy Akademii Polonijnej». 2020. Т. 43. № 6. Р. 198-204. DOI <https://doi.org/10.23856/4325>

Тихомиров О. О.

кандидат юридичних наук, доцент,
доцент кафедри цивільно-правових
дисциплін Національної академії
Служби безпеки України

ДО ПРОБЛЕМИ ПРАВ ЛЮДИНИ В УМОВАХ СТАНОВЛЕННЯ «ПРАВОВОГО СТАТУСУ» ШТУЧНОГО ІНТЕЛЕКТУ

Наукова дискусія навколо актуальних питань штучного інтелекту (далі – ШІ), Інтернету речей, правового статусу робототехніки на фоні домінування технократичного підходу, навіть у правовій науці, поєднаного з суто інструментальним розумінням права як регулятивного чи забезпечувального засобу викликає деяке занепокоєння, особливо з позицій гуманістичних засад у праві, передусім прав людини.

Для пояснення наведемо кілька тез, доволі поширених і популярних у наукових юридичних публікаціях із зазначеної тематики.

Теза перша – розвиток ІІІ зумовлює появу в суспільних відносинах нових «дійових осіб», які вимагають від людства наділення їх певними правами.

Навряд сьогодні подібні твердження можна розуміти буквально. То на чому ж вони ґрунтуються? Дійсно, ІТ настільки «вживилися» у наше життя, що дедалі більше сприймаються його невід’ємною частиною. Потенційна здатність ІІІ оптимізувати взаємодію, зокрема й у деяких правових відносинах, є безперечною. Напевно, що саме через цю можливість, а також через наділення ІІІ окремими когнітивними функціями, притаманними людині, народжуються своєрідні асоціації між особою (зокрема людиною) та ІІІ як учасниками правовідносин. Утім, учасникам правовідносин властива не тільки певна дієвість як здатність до визначення послідовності та вчинення тих чи інших дій для досягнення мети, в яких формально виражається взаємозв’язок між ними. Вибір варіантів поведінки людиною серед іншого зумовлюється: мотивацією – внутрішньою (власні переконання) і зовнішньою (можливість суспільного впливу); власними потребами, культурним фактором, правовими традиціями і, навіть, нерідко емоціями та звичками. Видається, що стверджувати про повсюдне поширення ІІІ саме з такими чи хоча б аналогічними можливостями, що могло б створити реальну потребу в його певній соціалізації, і, як наслідок, формування його правового статусу ще зарано.

Теза друга – можливість визнання роботів з ІІІ суб’єктом права за аналогією з традиційними суб’єктами права – фізичною чи юридичною особою. В цьому разі підтримується й обґрунтовується також ідея аналогії щодо правосуб’єктності ІІІ.

Якщо спроби порівняння ІІІ з юридичною особою лежать здебільшого в площині цивільного права, то аналогія з фізичною особою, тобто людиною, та її правами – питання засадничого рівня.

Сучасна юриспруденція ґрунтується на людиноцентризмі та визнанні прав людини фундаментальною цінністю, благом, умовами, а не тільки сукупністю певних визнаних можливостей, які формально називають правами. Ця ідея розвивалася поступово, протягом тисячоліть, разом із розвитком самого людства та уяв-

лень про гідне життя. Її корінням є доктрина природного права, в якій джерелом права є розум людини, а фундаментальні невідчужувані права належать людині від природи.

Визнання суб'єктом права за аналогією з людиною якогось іншого «створіння» буде суперечити самій суті природно-правових ідей та становитиме загрозу правам людини. Утім варто згадати, що деякі представники юснатуралізму вважали, що природні права можуть належати й іншим істотам – тваринам, що можна було б використати як аргумент при осмисленні ІІІ. Проте, в будь-якому разі, у природно-правовій доктрині розглядаються живі істоти природного походження, які природним шляхом самостійно відтворюються, розвиваються, живуть певний строк і помирають. Це відбувається за законами природи – під впливом старіння, хвороб, кліматичних умов, екосистемних зміни, природного відбору тощо.

Крім того, про права тварин йдеться переважно в контексті їх захисту саме від людини, в контексті обов'язків людини щодо них, а не з позицій альтернативності чи аналогічності людині як суб'єкту права і, тим більше не у зв'язку з взаємодією тварин між собою, як це прослідковується у пропозиціях щодо правового статусу ІІІ.

Очевидно, що ІІІ чи роботи з ІІІ не є природними біологічними створіннями та існують за іншими законами, тому пряме перенесення на них поняття прав, у тому значенні, яке надається правам людини чи фізичної особи, буде порушенням засадничих ідей сучасної юриспруденції.

Але когнітивні можливості ІІІ, здатності до формування і вибору варіантів власних дій, нехай навіть з певного програмно встановленого переліку, формують своєрідні соціально важливі комунікації між ними та людиною, що попадає в предметну сферу права з різних позицій та потребує належного осмислення.

Якщо ж таки торкатися ідей щодо правосуб'єктності ІІІ, зокрема так званої «електронної особи», а вони очевидно будуть розвиватися, то потрібно чітко усвідомлювати, що подібні ідеї у праві мають революційний характер. Тому ставлення до них має бути вкрай виваженим, від правильності вектору таких новацій залежатимуть подальші правові зміни.

Проведення хоча б якихось аналогій між ІІІ і людиною як суб'єктом права на рівні практичної юриспруденції видається доволі небезпечним, оскільки закладає підвалини розширення цих аналогій та, як наслідок, в майбутньому спричинення певної статусної конкуренції, в якій правам людини може бути завдана неоправдана шкода.

Теза третя – визнання ІІІ суб'єктом права дає можливість вирішувати проблеми відповідальності за дії ІІІ.

Тут важливо враховувати, що інститут юридичної відповідальності у праві здійснює комплекс функцій, які в певних комбінаціях притаманні кожному галузевому виду юридичної відповідальності. Ними є відновлення порушених прав (компенсація), превенція (загальна і спеціальна), виховання (перевиховання), покарання. Говорити про притягнення до юридичної відповідальності в контексті виконання тільки якоїсь окремої її функції, наприклад відшкодування завданої шкоди, як мінімум, некоректно.

Що ж до самостійної відповідальності ІІІ у випадку визнання його суб'єктом права, то викликає великі сумніви можливість для нього негативних наслідків особистого характеру, або ж виховного чи перевиховного впливу, оскільки ІІІ не є ні живою істотою, ні членом суспільства. З іншого боку виконання правовідновлювальної (компенсаційної) функції, зокрема щодо відшкодування шкоди, вимагатиме й наділенням ІІІ правом власності, тобто власним майном, що теж буде істотною проблемою. Наразі відповідальність ІІІ убачається можливою тільки в площині своєрідних організаційних заходів щодо нього.

Тому, потрібно також усвідомлювати, що «відповідальність» так званої «електронної особи» не може розглядатися в контексті традиційного розуміння юридичної відповідальності, тобто за аналогією з відповідальністю людини. Як осмислення статусу «електронної особи», так і сприйняття її відповідальності має відбуватися на інших засадах, які забезпечуватимуть непорушність фундаментальних правових цінностей і ідеалів, повагу до прав людини, і, водночас, гармонійне вирішення потреб у правовому вирішенні проблем ІІІ.

На підставі зазначеного, на противагу наявним у вітчизняних наукових публікаціях гіпотезам, пропонується інша – з урахуванням сучасного розуміння права як багатогранного феномену, блага, цінності, перенесення на ІІІ окремих елементів статусу людини (фізичної особи) можливе лише на рівні теоретизування.

Проте ця гіпотеза, звісно, не вирішує проблеми удосконалення правового регулювання відносин, в яких своєрідно присутній ІІІ. Дослідження і дискусії з цього питання мають продовжуватися. На сьогодні ж у вітчизняній правовій науці можна констатувати лише передумови певних парадигмальних змін:

- із революційним шляхом – зміна ціннісних орієнтирів у праві передусім на розуміння його суто як засобу, який можна штучно змінити й адаптувати (прогностичними методами чи моделюванням), навіть на рівні загальновизнаних історично сформованих засад (принципів і постулатів), під потреби впровадження у юридичну практику такого нового, хоча і своєрідного, але суб'єкта права як ІІІ;
- і традиційним – широкого сприйняття права як цінності, блага, як культурного і цивілізаційного надбання людства, а ІІІ – як новітнього елемента суспільних відносин, виникнення і поширення якого органічним шляхом створює потреби у незвично швидкій, і можливо дещо нетрадиційній, правовій рефлексії.

Грушева М. А.

студентка НТУУ «КПІ ім. Ігоря
Сікорського»

Науковий керівник: Дубняк М. В.

кандидат юридичних наук старший
викладач, НТУУ «КПІ імені Ігоря
Сікорського»

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ: ШТУЧНИЙ ІНТЕЛЕКТ І ТВОРЧІСТЬ

Сучасний світ можна охарактеризувати стрімким розвитком технологій. Такий розвиток зумовив появу штучного інтелекту, який нині використовується у багатьох сферах людської діяльності. За останні роки ми можемо спостерігати появу великої кількості арт-об'єктів, створених штучним інтелектом, що стало своєрідним викликом для правової системи.

Метою дослідження є з'ясування сутності проблеми охороноздатності арт-об'єктів, створених штучним інтелектом, а також підходів до визначення їх правового статусу.

Історія штучного інтелекту бере свій початок з середини ХХ ст. Саме у 1956р. американський інформатик Джон Маккарті офіційно запропонував термін «artificial intelligence»(штучний інтелект). За його версією, «це програма, яка опрацьовує і реагує на інформацію таким чином, що результат є подібним до реакції розумної людини на аналогічну ситуацію» [1, 84].

У Оксфордському словнику запропоноване визначення штучного інтелекту як теорії і розробки комп'ютерних систем, що здатні виконувати завдання, які зазвичай вимагають людського інтелекту, такі як візуальне сприйняття, розпізнавання мови, прийняття рішень і переклад з однієї мови на іншу [2]. Співставивши це визначення з попереднім, на нашу думку, штучний інтелект можна охарактеризувати як програму, яка здатна самостійно приймати рішення і робити висновки, сприймати інформацію, опрацьовувати її та створювати на її основі власні твори,

іншими словами, відтворювати функції людини, що вимагають розумової праці.

За допомогою технологій штучного інтелекту можуть створюватись потенційні об'єкти права інтелектуальної власності, тому виникає необхідність визначення того, чи потрібно охороняти продукти такої творчої діяльності.

Відомі випадки, коли штучний інтелект справді досягнув великих успіхів у мистецтві. Так, у 2018 році портрет Едмонд де Баламі, створений французькою арт-групою Obvious з використанням технології Generative Adversarial Network (GAN), був проданий на аукціоні Christie's за 432,5 тис. дол. Поруч з оприлюдненим зображенням вказувалось Image ©Obvious.

Група Obvious розробила алгоритм відбору згенерованих зображень, який полягав у тому, що зображення не мали відрізнятись від тих, які б могла створити людина. Але кінцевий результат залежав тільки від штучного інтелекту, який самостійно відбирав зображення [3, с. 48].

Щоб створити таке зображення довелося прикласти чимало зусиль і коштів. Тому не можна заперечувати, що для таких об'єктів, які представляють собою художню і комерційну цінність, потрібні спеціальні засоби правової охорони.

На жаль, питання надання штучному інтелекту авторського права на створені ним об'єкти все ще залишається досить суперечливим. Варто зазначити, що наразі у багатьох країнах на законодавчому рівні не врегульовано захист авторських прав на результати самостійної діяльності штучного інтелекту. У США існує підхід, згідно з яким автором визначається людина, що використовує штучний інтелект для створення твору, крім того допускається співавторство розробника(власника) і користувача штучного інтелекту [4, с.18]. Проте проблема полягає у тому, що не завжди людина спрямовано використовує штучний інтелект для досягнення визначеного результату, адже він може створювати твори й без її участі.

Щодо українського законодавства, у ст.1 закону України «Про авторське право та суміжні права» зазначається, що автором є фі-

зична особа, яка своєю творчою працею створила твір [5]. Тобто у чинному законодавстві України нормативно не врегульовано питання належності творів, створених штучним інтелектом.

На основі аналізу наукових публікацій Єврокомісії, USPTO, GBIPO, AIPPI, Капіца Ю. у своєму дослідженні, визначає кілька підходів щодо правової охорони об'єктів, які створені штучним інтелектом:

Підхід 1 полягає у тому, що окремі об'єкти мають охоронятись суміжними правами. Зокрема, у документі GBIPO вказується, що від таких об'єктів як звукозаписи, фільми, передачі мовлення не вимагається оригінальність, тому права на них у будь-якому випадку належатимуть виробникам. Такий підхід може застосовуватись і до результатів діяльності штучного інтелекту.

Підхід 2. Об'єкти, створені штучним інтелектом, мають охоронятись авторським правом. У ст. 9 Закону Великої Британії про авторське право, промислові зразки та патенти 1987 р. зазначається, що: "у випадку літературного, драматичного, музичного чи художнього твору, який створений комп'ютером, автором вважається особа, якою здійснюються заходи, необхідні для створення твору". Важливим критерієм при визнанні авторського права є оригінальність. Візьмемо до уваги судову практику і законодавство ЄС, згідно з якими охороноздатними об'єктами визнаються тільки оригінальні твори, які є результатом самостійної інтелектуальної діяльності автора. Звідси випливає, що автором творів, які підлягають охороні відповідно до чинного законодавства ЄС про авторське право, може визнаватися тільки людина. Крім того, у більшості юрисдикцій штучний інтелект не визнається автором створених ним об'єктів, адже він не має правосуб'єктності. [6, с. 62] Тому, на нашу думку, на даний момент не є можливим визнання штучного інтелекту автором створених ним об'єктів мистецтва. Він скоріше виступає лише інструментом для створення твору у руках розробника.

Згідно з третім підходом у дослідженні Капіца Ю., потрібно запровадити нове право з розширенням меж застосування права *sui generis* стосовно баз даних. Правом *sui generis* охороняють-

ся бази даних, які не відповідають критеріям оригінальності. Але наводяться пропозиції щодо застосування цього права для творів, створених штучним інтелектом. Зокрема, Британська група AIPI пропонує застосовувати нове суміжне право, що діє 25 років і має відшкодувати інвестиції, вкладені в розробку штучного інтелекту. Охороноздатними можуть бути художні, літературні, музичні твори, але твори не підпадають під охорону, якщо відсутня фізична особа, що брала участь у їх створенні.

Підхід 4 полягає у тому, що об'єкти, створені ШІ, не потребують правової охорони й ними можуть користуватись без жодних обмежень. Але цей підхід не є обґрунтованим, так як інвестиції у штучний інтелект мають окупатись і твори, створені штучним інтелектом мають бути захищені від недозволеного використання [3, с. 48-50].

Висновки. У результаті проведеного дослідження, можна зробити висновок, що охорона авторським правом об'єктів, створених штучним інтелектом – це лише питання нормативно-правового закріплення.

Проаналізувавши джерела, ми виявили багато підходів до вирішення проблеми авторства, проте, на нашу думку, не є доцільним вважати штучний інтелект автором, адже він постає лише інструментом для створення того чи іншого твору. Потенційним автором може бути людина – розробник або користувач штучного інтелекту, до чого схиляються у розвинених країнах, зокрема у США, Великій Британії. Але у більшості країнах, у тому числі і в Україні, невизначеним залишається питання, хто має авторське право на такі об'єкти і чи взагалі вони можуть бути охороноздатними. Тому не тільки у майбутньому, але й вже зараз, ми стикаємось з потребою вдосконалення чинного законодавства.

Список використаної літератури:

1. Tripathi, S., & Ghatak, C. (2021). Artificial Intelligence and Intellectual Property Law. *Christ University Law Journal*, 7(1), P.83-98.
URL: <https://doi.org/10.12728/culj.12.5>

2. Blackburn, Simon. The Oxford Dictionary of Philosophy., 3rd edition., Oxford., 2016. – 551 p. URL: https://en.oxforddictionaries.com/definition/artificial_intelligence.

3. Капіца, Ю. (2021). Тексти, музика, зображення, що створюються штучним інтелектом: до визначення моделі правової охорони. *Інформація і право*, (1 (36)), 45-54. URL: http://ippi.org.ua/sites/default/files/7_19.pdf

4. Прилипко, Д. (2021). Штучний інтелект та авторське право. *Теорія і практика інтелектуальної власності*, (2), 15-22.

URL: <http://uran.inprojournal.org/article/view/236526/235043>

5. Про авторське право та суміжні права : Закон України від 23.12.1993 р.№ 3792-ХІІ.

URL: <https://zakon.rada.gov.ua/laws/card/3792-12>

6. Павлюк. О. (2021). Критерії охороноздатності об'єктів авторського права, створених із використанням технологій штучного інтелекту: міжнародно-правовий досвід. *Цивільне право і процес*, С. 59 – 64 URL: <http://pgp-journal.kiev.ua/archive/2021/6/9.pdf>

Мельник А. Я.

студентка НТУУ «КПІ ім. Ігоря
Сікорського»

Науковий керівник: Дубняк М. В.

кандидат юридичних наук старший
викладач, НТУУ «КПІ імені Ігоря
Сікорського»

ПРОБЛЕМИ ВИКОРИСТАННЯ СИСТЕМИ БЛОКЧЕЙН В ЕЛЕКТРОННОМУ ГОЛОСУВАННІ

Електронне голосування новинка для українців, хоча для деяких держав світу це звичайна практика. Естонія впровадила цей тип голосування понад десяток років тому, а Швейцарія проводить його на блокчейні декілька років [1].

Метою даного дослідження є окреслення поняття системи блокчейн, аналіз переваг та недоліків її використання в електронному голосуванні.

При дослідженні різних підходів до визначення поняття «блокчейн», ми відзначимо думку Мелані Свон, згідно з якою, блок-

чейн – це ланцюжок блоків даних, обсяг якого постійно зростає в міру додавання майнерами нових блоків з записами останніх транзакцій. Блоки записуються в блокчейн в лінійному послідовно-хронологічному порядку [2, с. 7-8].

Своєю чергою Махер Альхарбі визначає блокчейн як розподілений реєстр, який зберігає історію всіх транзакцій які коли-небудь траплялися в мережі блокчейн [3, с.25].

Отже, блокчейн – це спільна база даних, яка записує операції між двома сторонами, а інформація про ці операції формується у ланцюги, які складаються з блоків, в яких і зберігається інформація.

Для подальшого дослідження необхідно визначити, що таке електронне голосування. Ольга Стогова визначає електронне голосування як можливість залучення громади за допомогою сучасних інформаційних технологій до вирішення різноманітних суспільно-політичних завдань [4, с. 39].

Онлайн-голосування або Інтернет-голосування – це версії електронного голосування, де виборці мають можливість віддати свій голос, не відвідуючи саму виборчу дільницю, використовуючи комп'ютер, планшет або смартфон. Як і інші підходи до електронного голосування, ці системи також полегшують підрахунок голосів [5].

Електронне голосування має дозволити швидше рахувати виборчі бюлетені, шляхом електронного обчислення знизиться ризик помилки через людський фактор, а також зменшиться кількість необхідного персоналу, який мав би обраховувати кількість бюлетенів. Також передбачається, що електронне голосування підвищить доступність до голосування для виборців, в особливості для населення сільських місцевостей; осіб, які тимчасово перебувають за кордоном, а також для людей, які мають фізичні обмеження. [6, с. 8]

Для того, щоб електронне голосування проходило безпечно та без втручань третіх осіб, необхідно забезпечити захищеність інформації. Відтак, враховуючи, що блокчейн містить записи про усі транзакції, припустимо, що він може бути надійною системою для здійснення е-голосування. [7, с. 7]

Можна окреслити такі переваги використання системи блокчейн у сфері електронного голосування: прозорість операцій, високий рівень захисту персональних даних, доступність до інформації учасникам голосування, неможливість змінити інформацію, уникнення можливих фальсифікацій документів. [8, с. 209]

Блокчейн характеризується високим рівнем захисту. Це головна перевага цієї системи, що дозволяє використовувати її й у сфері державного управління. До того ж блокчейн – прозора система, кожен учасник може відкрито переглядати інформацію стосовно кожної операції. В електронному голосуванні це важливо, адже це забезпечує доступ до інформації для кожного учасника голосування. [8, с. 208]

Оскільки інформація зберігається на пристроях кожного голосувальника, то будь-які зміни документів на одному пристрої не зможуть завдати шкоди загальній інформації. Масові фальсифікації можливі за умови, якщо половина виборців надасть доступ до інформації, а цей випадок неможливий [9].

Кожну ситуацію варто розглядати під декількома кутами, тому необхідно виділити й негативні сторони використання блокчейну в системі електронного голосування: вразливість до кібератак, неповна конфіденційність виборців, велика фінансова затратність, підвищені вимоги до користувачів [6, с. 9].

Так, як і будь-які нові технологічні системи, блокчейн вразливий для кібератак. Розробники системи запевняють користувачів, що і на такий випадок є захист: так, як інформація записана не на одному пристрої, будь-які маніпуляції із документами марні. Також зміна вихідного файлу приводить до деформації всього ланцюга, що не може бути непоміченим. Проте, кібератака може бути причиною серйозного збою в роботі системи, а це приведе до виборчого хаосу. [10]

Системи голосування на основі блокчейну можуть спричинити проблеми з конфіденційністю. Емануель Франціоні вважає, що повна відкритість даних призводить до юридичних обмежень, а повна анонімність – до застою в розвитку блокчейну [11]. Тобто, повної конфіденційності досягнути неможливо, відповідно, певна

інформація залишиться відкритою, наприклад, ім'я голосувальника, поштова адреса.

Наступною проблемою стає те, що дані зберігаються на комп'ютерах всіх учасників голосування і для реєстрації необхідна обробка великих обсягів даних. Це викликає підвищені вимоги до комп'ютерів і до швидкості Інтернету, що може бути недоступним для жителів сільської місцевості. Такі вимоги сприяють великим енерговитратам на обслуговування операцій в системі, наприклад, за розрахунками економістів у 2020 році витрати електроенергії на обслуговування біткоїну у світі будуть порівнянні з річним енергоспоживанням невеликої країни, наприклад, Данії [12].

Отже, система блокчейн має переваги над іншими платформами, що дозволяє її використання у сфері державного управління. Переважна більшість негативних сторін систем або вже має альтернативні шляхи вирішення, або розробляє їх. Для впровадження цієї системи в електронне голосування для України можна використати досвід Швейцарії, яка використовувала блокчейн. Однак серйозною проблемою залишається низьке правове забезпечення України та незмога фінансування пробних проєктів.

Список використаної літератури:

1. Полякова А. Вибори-2019 на блокчейні: як це працює і чому нам це потрібно 2018. URL: <https://www.epravda.com.ua/publications/2018/07/19/638824/>.
2. Мелані С. Блокчейн. Схема нової економіки, 2015. – 52 с
3. Alharby M. Models and Simulation of Blockchain Systems. A thesis submitted for the degree of Doctor of Philosophy 2020. P.173 – URL: <https://theses.ncl.ac.uk/jspui/bitstream/10443/5053/1/Alharby%20Maher%20E-Copy.pdf>.
4. Стогова О. «Електронне голосування: проблеми та перспективи» Юридичний науковий електронний журнал. №3, 2021, С. 38 – 40. URL: <https://doi.org/10.32782/2524-0374/2021-3/8>.
5. Ліллестрьом М. Переваги та ризики електронного голосування та онлайн-голосування. 2020. URL: <https://decentralization.gov.ua/news/12905>.

6. Впровадження електронного голосування. // International Institute for Democracy and Electoral Assistance, 2011, С. 43.

7. Park S. Going from bad to worse: from Internet voting to blockchain voting / Journal of Cybersecurity, 2021, №7, С. 1- 19.

8. Яровенко Г. М. Перспективи застосування технології блокчейн у системах забезпечення кібербезпеки банків. Підприємство та інновації. 2020, №12, С. 206–214.

9. Как блокчейн меняет мир? Применение, плюсы и минусы блокчейн. Портал о современных технологиях мобильной и беспроводной связи. 2021: URL: <http://1234g.ru/novosti/blokchejn-menyaet-mir>.

10. Iredale G. Top Disadvantages Of Blockchain Technology [Електронний ресурс] / Gwyneth Iredale // 101 Blockchains. – 2020. – Режим доступу до ресурсу: <https://101blockchains.com/disadvantages-of-blockchain/>.

11. Франціоні Е. Головоломка децентралізованої конфіденційності: як узгодити приватність і прозорість. 2018. URL: <https://blockchainconf.com.ua/uk/article/dannie-v-blokcheyne-anonimnost-ili-otkritost-doklad-vedushchego-razrabotchika-dusk-foundation-emanuele-francioni-91851>.

12. Простобанк Консалтинг. Що таке блокчейн? 2021. URL: https://bankchart.com.ua/finansoviy_gid/investitsiyi/statti/scho_take_blokcheyn_.

Саградян А. Г.

студентка НТУУ «КПІ ім. Ігоря
Сікорського»

Науковий керівник: Дубняк М. В.

кандидат юридичних наук старший
викладач, НТУУ «КПІ імені Ігоря
Сікорського»

ПОНЯТТЯ ТА СУТНІСТЬ СМАРТ-КОНТРАКТІВ

Все більшого значення набуває впровадження прогресивних інформаційних технологій та інноваційних проектів у всіх сферах людської діяльності. Не виключенням стали популярні протягом останніх років технологія Blockchain, та смарт-контрак. Звичайно ж, інвестування нових проектів, зазвичай є прибутковим, але попри популярність цих термінів виникає необхідність уточнення їх

значень, встановлення реальних можливостей їх застосування та функціонування.

Мета дослідження полягає у визначенні поняття смарт-контрактів, аналізі їх значення, співставленні переваг та недоліків та визначення проблем правового регулювання.

Створення системи публічних блокчейнів відкрило можливість для появи нової технології – «Смарт-контракти» або розумний контракт. Сам по собі смарт-контракт є децентралізованою системою, яка забезпечує всім сторонам, які беруть участь в переговорах, безпечне проведення угоди, перевірку та дотримання всіх умов, мінімізує виникнення конфліктних ситуацій, значно економить час, позбавляє від необхідності наймати посередників [1, с. 175]. Виконання розумного контракту відбувається на комп'ютері, а для опису контракту та його результату використовується програмування і криптографічні інструменти. Смарт-контракти представляють підвищений інтерес з боку банків і державних структур, завдяки тому, що розумні контракти значно перевершують стандартні системи в швидкості та безпеці. Завдяки децентралізованій системі та криптографії, виключається можливість шахрайства. Програмний код підтверджує здійснення угоди та далі автоматично визначає, що робити із зазначеним активом: послати учаснику угоди, повернути хазяїну або щось складніше. Під час проведення операції, в реєстрі знаходиться копія цього контракту, що надає достовірність і захищеність і не дає жодній зі сторін поміняти вже обумовлені умови.

Поняття «смарт-контракт» з'явився в 1996 р.: Нік Сабо, фахівець з інформаційних технологій, в той час аспірант Вашингтонського університету, визначив смарт-контракт як «набір обіцянок, виражених в цифровому вигляді, включаючи протоколи виконання сторонами цих обіцянок». Як «примітивного предка смарт-контрактів» він навів в приклад вендингові автомати, які без участі людини з боку продавця могли укласти та виконувати операції з купівлі–продажу товарів, які в них містяться. Таким чином, термін «смартконтракт» з'явився задовго до появи технології

блокчейн, але з розвитком саме цієї технології пов'язаний інтерес до практики використання «розумних контрактів» [2, с. 26].

Призначення смарт-контракту – передача інформації та забезпечення виконання усіма учасниками завданих у коді умов. Якщо дати більш «юридичне» визначення смарт-контракту, то воно звучатиме таким чином: це комп'ютерна програма, пов'язана з виконанням зобов'язань сторонами, які її використовують. В юридичному сенсі смарт-контракт може виконувати одну з двох функцій: безпосередньо виконувати закладені у код умови зобов'язання або відстежувати виконання чи порушення волі сторін, узгодженої у правочині, який сторони заклали у коді контракту. Смарт-контракти надають можливість безпечно обмінюватися грішми, частками у власності на нерухоме майно, цінними паперами та іншими активами напряду, тобто без участі посередників. [3]

Ключовий ефект та головна цінність смарт-контрактів у тому, що вони дозволяють зробити зобов'язання «самовиконуваним», тобто автоматизувати виконання обумовлених сторонами зобов'язань. Завдяки такій властивості, смарт-контракт виводить виконання зобов'язання поза межі волі сторін, яка може бути спрямована на не виконання або неналежне виконання. Такий функціонал забезпечує впевненість контрагентів одне в одному, а також високу прогнозованість виконання зобов'язань. Смарт-контракт є вираженням умов зобов'язання у вигляді програмного (машинного) коду, який не допускає вільних тлумачень чи інтерпретацій. Така реалізація гарантує, що після того як смарт-контракт погоджений і підписаний сторонами, будуть виключені подвійні трактування або спори щодо тлумачення умов виконання зобов'язання. Для виконання смарт-контракту не потрібна участь людини, оскільки він виконується автоматично. Це дозволяє, з одного боку, вивільнити час, який був би необхідний для вчинення дій, спрямованих на виконання, а з іншого – уникнути помилок та зловживань, тобто виключити «людський фактор». Таким чином, смарт-контракт є інструментом, який автоматизує правовідносини. Звісно, така автоматизація має певні технологічні та юридичні обмеження. Тому ви-

рішуючи питання про застосування смарт-контракту, потрібно перевірити свого роду «критерії прийнятності».

Першим таким критерієм є практичний ефект – відчутний і зрозумілий. З цієї позиції має сенс автоматизувати правочини, які передбачають періодичні повторювані платежі або вчинення дій, а також правочини зі значними сумами, в яких присутній дефіцит довіри між сторонами та існує ризик невиконання умов щодо оплати.

Другим критерієм є технічна можливість впровадження, тобто можливість закласти умови правочину в програмний код смарт-контракту. Для того щоб правочин відповідав цьому критерію, його умови мають бути пов'язані з об'єктивними та вимірюваними параметрами. Найбільш прийнятна модель використання смарт-контрактів у юриспруденції має назву «рікардіанський контракт» (Ricardian contract) – це такий метод запису договору, за умовами якого він викладається в матеріальній формі у вигляді класичного юридичного контракту з одночасним вираженням його умов в інших системах. Іншою системою можуть бути розподілені реєстри, різновидом яких є блокчейн. Ключова особливість рікардіанського контракту в тому, що умови правочину викладаються у форматах, які будуть зрозумілими обчислювальній машині для забезпечення функцій автоматичного виконання і контролю виконання та інших машинних дій, а також у вигляді звичного текстового документа, який є джерелом умов договору і може бути сприйнятий сторонами та їхніми юристами. Іншими словами, рікардіанський контракт – це симбіоз звичайного контракту і смарт-контракту. Саме у вигляді такого симбіозу в юриспруденції переважно застосовуватимуться смарт-контракти [3].

Особливості укладення, виконання, зміни смарт-контрактів, які дозволяють визначати смарт-контрактів як окремих вид договорів.

1. Умови смарт-контракту повинні бути конкретними (чіткими, однозначними), здійсненими (об'єктивними), правомірними. Умови смарт-контракту можуть бути сформульовані за формулою «якщо..., тоді...». Не всі умови договору можуть бути автоматизовані. Не можуть використовуватися оціночні терміни, на-

приклад «розумний строк». Смарт-контракт існує в межах платформи блокчейну, тому можливі, як правило, трансакції в межах даної платформи (здійснення трансакцій криптовалюти). Умови смарт-контракту можуть передбачати забезпечувальні зобов'язання, зокрема, коли згідно зі смарт-контрактом блокується певна сума криптовалюти, перерахунок якої кредитору здійснюється лише після вчинення певний дій боржником. Це одна з основних переваг смарт-контракту. Проблемним є отримання і підтвердження інформації зовні, тому умови про форс-мажорні обставини також не зазначаються в смарт-контракті. Тому можливими є два варіанти оформлення смарт-договорів: електронна форма повністю трансформована в програмний код або лише частина електронного договору відображена в програмному коді [4, с. 17].

2. Виконання зобов'язань, передбачених смарт-контрактом, здійснюється в автоматичному порядку цифрових трансмісій у певній послідовності у разі настання певних обставин. Виконання смарт-контракту здійснюється без участі сторін, на відміну від звичайного договору, коли сторони зобов'язані вчиняти певні дії. Засобом розрахунків за смартконтрактами є криптовалюта. Одним із стримуючих факторів поширення смарт-контрактів є відсутність правового регулювання статусу криптовалюти в Україні. Слід зазначити, що смарт-контракт може забезпечити виконання лише зобов'язань у віртуальному світі, наприклад щодо проведення платежів криптовалютою. Виконання робіт та надання послуг здійснюється в реальному світі і не може бути опосередковано смарт-контрактом.

Слід зазначити, що перед тим, як смартдоговір буде виконаний, потрібно оплатити трансакційну комісію. З метою розширення сфери застосування смарт-контрактів доцільно було б забезпечити доступ до інформації з Державного реєстру речових прав на нерухоме майно, Державного реєстру юридичних осіб, фізичних осіб – підприємців, громадських формувань та інших реєстрів [4, с. 17].

3. Відсутня можливість змінити договір. Якщо смарт-контракт почав виконуватися, його неможливо припинити або змінити. Це зумовлено технологією блокчейн. З одного боку, це є плюсом, адже сторона не може ухилитися від виконання угоди, а з іншої –

мінусом, оскільки помилка або відсутність певної умови може унеможливити виконання домовленостей, які відповідали б волевиявленням сторін. В останньому випадку можливе лише укладення нового смарт-договору [4, с. 17].

Переваги та недоліки розумних контрактів. Як у будь-якої технології, у smart-контрактів є як переваги, так і недоліки. Переваги перед традиційними договорами в цій сфері полягають, зокрема, у відсутності посередників, автоматичному виконанні, жорсткій регламентації та тлумаченні умов, неможливості втручання в заздалегідь визначений код тощо.

В ідеальному варіанті смарт-контракти мають не лише сприяти скороченню витрат на укладання правочинів та проведення транзакцій, але і зменшити кількість судових спорів. Однак більшість переваг смарт-контрактів водночас виступають і його недоліками. Так, найбільшою проблемою смарт-контрактів вважають неможливість кодування значної частини домовленостей між сторонами, тому що вони не укладаються у схему «якщо <...>, то <...>», а охоплюються абстрактними поняттями, як-от «законність», «справедливість», «розумний строк», «захист слабкішої сторони» тощо. Наступним недоліком смарт-контрактів є прив'язка до реального світу та необхідність отримання даних із-за меж системи. Для отримання даних, які розташовані поза блокчейном чи іншим розподіленим реєстром, смарт-контракту необхідно звертатися до так званих оракулів. Програми-оракули є спеціалізованими сервісами, спрямованими на забезпечення прив'язки цифрового світу до реального та надання смарт-контрактам вихідних даних для їх виконання [5, с. 103]. Використання оракулів означає притягнення третьої сторони до такої угоди з усіма ризиками, що із цього випливають, зокрема, постає питання про достовірність даних, отриманих із такого джерела. Унаслідок таких маніпуляцій інформація, що потрапляє у смарт-контракт, буде недостовірною, що визначатиме заздалегідь несправедливе виконання угоди. Автоматичність виконання смарт-контракту також породжує деякі проблеми. Зокрема, у разі наявності об'єктивних умов для зупинення виконання чи зміни домовленості смарт-контракт неможливо змі-

нити, як неможливо призупинити його виконання. Водночас, ще однією проблемою є те, що, на відміну від традиційних договорів, у смарт-контрактів практично цілком відсутня гнучкість [5, 103]

Висновки. Отже, проаналізувавши поняття смарт-контракту, ми можемо зробити такий висновок, що дана категорія – це комп’ютерні алгоритми, призначені для укладання та підтримки контрактів. Такий контракт пишеться у кодовій формі та виконується на блокчейні. Визначивши усі переваги та недоліки даного явища, можна з впевненістю сказати, що багато галузей, таких як фінанси, торгівля, нерухомість, телекомунікації та інші можуть отримати значну користь від використання смарт-контрактів.

Список використаних джерел:

1) Ліщинська Л. Б. Перспективи використання смарт-контрактів у бізнесі. – С.175 – 178. URL:<https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/31575/71037.pdf?sequence=2&isAllowed=y> (Дата звернення 12.11.2021 р.)

2) Клопов І. О. Переваги застосування технології смарт-контрактів. Біоекономіка як ключовий фактор розвитку виробництва та екологізації промислового регіону : матеріали Міжнародної науково-практичної конференції (26-27 листопада 2020 року, м. Запоріжжя). – Запоріжжя : Наук. ред. Н. Г. Метеленко. ЗНУ Інженерний навчально-науковий інститут, 2020 С.26 – 29 URL: http://dspace.wunu.edu.ua/bitstream/316497/41897/1/%D0%97%D0%91%D0%86%D0%A0%D0%9D%D0%98%D0%9A_%D0%97%D0%9D%D0%A3_31_12%20%281%29.pdf#page=26 (Дата звернення 12.11.2021 р.)

3) Сизоненко В. Смарт-контракти: з чим вони смакують. *Юридична Газета*. 2018. №46. С. 1, 16 – 17. URL:<https://corporate.interlegal.com.ua/smart-kontrakti-z-chim-voni-smakuyut/> (Дата звернення 12.11.2021 р.)

4) Верес І. Я. Правова природа смарт-договору // Підприємництво, господарство і право. – 2020. – С.16-17. URL: <http://pgp-journal.kiev.ua/archive/2020/9/4.pdf> (Дата звернення 13.11.2021 р.)

5) Некіт К. Г. Переваги та недоліки смарт-контрактів як підстав виникнення права власності. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право* випуск 3., 2020 С.101- 105 URL: <http://visnyk-psp.kpi.ua/article/view/229494/228501> (Дата звернення 13.11.2021 р.)

ПИТАННЯ ВДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА З ПИТАНЬ ЗАХИСТУ ПРАВ ЛЮДИНИ В УМОВАХ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ

Смерницький Д. В.

доктор юридичних наук, старший
дослідник, заступник директора
Державного науково-дослідного
інституту Міністерства внутрішніх
справ України

ЗАХИСТ ПРАВ ЛЮДИНИ ПРИ ВИКОРИСТАННІ СУЧАСНИХ ЦИФРОВИХ ТЕХНОЛОГІЙ: ПРАВОВІ ОСНОВИ

Проводячи відповідні дослідження дотримання прав людини в сучасних умовах використання цифрових технологій, які стрімко розвиваються та стали невід'ємною складовою суспільного життя, зазначимо, що права людини у цій сфері переважно стосуються інформації. Цифрові технології створюють відповідні умови для передачі, обробки та зберігання інформації.

Інформаційне забезпечення – це та відправна точка на якій ґрунтуються всі сфери суспільного життя.

У перекладі з латинської мови «інформація» (information) – це роз'яснення, уявлення [1, с. 717], тобто йдеться про відомості (або їх сукупність) про предмети, явища й процеси навколишнього світу. Низка авторів у дослідженнях використовують ті визначення інформації, які наведені в енциклопедичному словнику: «інформація – це відомості, що передаються людьми усним, письмовим або іншим способом [2, с. 498]. Аналізуючи визначення інформації, які наведені в енциклопедичному словнику, слід відмітити, що, на нашу думку, інформація не є лише дією, як визначено – «це відомості, які передаються людьми різними способами». Інформа-

ція може бути і рухомим (динамічним), і статичним явищем, – відомості, які за певних умов стають інформацією, але ці відомості можуть дійсно передаватися різними способами [3, с. 24].

На нашу думку, інформація – це відомості про всесвіт. Іншими словами можна сказати, що всесвіт і є інформацією. А будь-які відомості стають інформацією, якщо є суб'єкт, який їх сприймає у вигляді певних даних.

Отже, в кінцевому варіанті, на нашу думку, визначення інформації можна сформулювати у такому вигляді: «інформація – це відомості про всесвіт, які сприймаються певним суб'єктом» [4, с. 177-178].

Основоположним нормативно-правовим документом, що стосується інформації, є Закон України «Про інформацію». Види інформації за змістом встановлені у ст. 10 Закону, це: інформація про фізичну особу; інформація довідково-енциклопедичного характеру; інформація про стан довкілля (екологічна інформація); інформація про товар (роботу, послугу); науково-технічна інформація; податкова інформація; правова інформація; статистична інформація; соціологічна інформація; інші види інформації [5].

Конституцією України [6] передбачено ряд норм із зазначеного питання.

Так згідно ст. 31 Конституції кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції.

Стаття 32 передбачає, 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.

Крім того, кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір. Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання завору-

шенням 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 (ст. 34 Конституції).

Стосовно інтелектуальної власності, то кожен має право володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності (ст. 41) та громадянам гарантується захист інтелектуальної власності, їхніх авторських прав, моральних і матеріальних інтересів, що виникають у зв'язку з різними видами інтелектуальної діяльності, а також кожний громадянин має право на результати своєї інтелектуальної, творчої діяльності, ніхто не може використовувати або поширювати їх без його згоди, за винятками, встановленими законом (ст. 54).

Отже, з наведеного можна зробити висновок, що Конституцією України [6] передбачені норми щодо захисту прав стосовно конфіденційної інформації про особу, а також щодо використання або поширення інформації стосовно інтелектуальної власності без згоди на то її власника. В той же час, кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію.

Тобто, цифрові технології з метою гарантування прав людини повинні технологічними методами забезпечити вільне поширення інформації, а також передбачити створення відповідного захисту інформації, яка передається у мережі, або зберігається на відповідному обладнанні, у разі такої потреби.

Розглядаючи норму гарантування прав людини в сфері цифрових технологій, щодо забезпечення вільного поширення інформації, слід зазначити, що переважно дотримання цієї норми залежить від удосконалення технологій передачі інформації, які на сьогодні стрімко розвиваються та набули всесвітнього характеру, а також встановлення в нормативно-правових актах відповідних норм стосовно відповідальності за перешкоджання вільному розповсюдженню інформації. На сьогодні, більша частина людства у всіх сферах суспільного життя не може вже обійтися без систем електронних комунікацій, електронних ресурсів, виробництва програмного забезпечення та комп'ютерних технологій.

Щодо норми гарантування прав людини стосовно забезпечення захисту інформації, що передається чи зберігається, то забезпечення зазначеної виконання норми, на наш погляд, можливо досягти такими способами:

- обмеження розміщення інформації в інформаційних мережах – цей спосіб захисту інформації може бути забезпечений лише тільки самим власником інформації;
- створення відповідних технологій щодо захисту інформації при її передачі зберіганні, забезпечення доступу до неї тільки встановленим особам – цей спосіб повинен бути забезпечений виключно цифровими технологіями;
- встановлення в нормативно-правових актах відповідних норм щодо відповідальності за незаконний доступ до інформації та подальше незаконне її використання – цей спосіб забезпечується правовим регулюванням сфери цифрових технологій.

Розглянемо надійність кожного із способів забезпечення захисту інформації. Так обмеження розміщення інформації в інформаційних мережах є дієвим способом її збереження, особливо якщо її зовсім не розміщувати. Але в наш час розвитку цифрових технологій та впровадження їх у всіх сферах суспільного життя це вбачається неможливим.

Що стосується створення відповідних технологій щодо захисту інформації при її передачі, зберіганні, забезпечення доступу до неї тільки встановленим особам, то зазначений спосіб дає результати лише на певний проміжок часу. Адже з розвитком технологій захисту паралельно розвиваються і технології подолання такого захисту. Отже, захист буде ефективним лише на той час, до якого не будуть розроблені способи подолання цього захисту. Надалі виникає потреба розробляти нові технології захисту.

Встановлення в Кодексі України про адміністративні правопорушення та Кримінальному кодексі Україні норм щодо відповідальності за незаконний доступ до інформації та подальше незаконне її використання, на нашу думку, є дієвим способом впливу щодо забезпечення захисту інформації. В той же час, правоохо-

ронні органи не завжди мають можливість притягнути правопорушника до відповідальності враховуючи, що цифрові технології надають можливість особі здійснювати свої дії інкогніто.

Підводячи певні підсумки розгляду питання забезпечення прав людини в сучасних умовах стрімкого розвитку та використання у всіх сферах суспільного життя цифрових технологій необхідно зазначити, що ми приходимо до думки, що самим ефективним способом стосовно забезпечення вільного поширення інформації та її захисту від протиправних посягань є поєднання наведених вище способів, тобто помірковані дії власника інформації повинні поєднуватися з розвитком відповідних технологій поширення та захисту інформації, а також з належним правовим регулюванням сфери цифрових технологій.

Література:

1. Юридична енциклопедія. К., 1998. Т. 2. 744 с.
2. Советский энциклопедический словарь. М., 1983.
3. Смерницький Д. В. Інформаційне забезпечення науково-технічної діяльності. Криміналістичний вісник. 2015. № 1 (23). С. 24–38.
4. Смерницький Д. В. Адміністративно-правове регулювання науково-технічної діяльності в Україні : дис. ... док. юрид. наук. : 12.00.07. К., 2020. 636 с.
5. Про інформацію: Закон України від 2 жовтня 1992 року № 2657-ХІІ. Відомості Верховної Ради України. 1992. № 48. Ст. 650.
6. Конституція України: прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року. Відомості Верховної Ради України. 1996. № 30. Ст. 141.

Шевченко О. А.

кандидат юридичних наук, полковник
докторант Національної академії
СБ України

СТРАТЕГІЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ ЯК ДОРОГОВКАЗ ДЛЯ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Безпрецедентні світові темпи розвитку інформаційних технологій, їх стрімке проникнення буквально в усі сфери життя суспільства, крім очевидного позитивного ефекту, вираженого в значному підвищенні продуктивності та ефективності людської праці, призводять до появи ряду важко вирішуваних проблем, до виникнення нових, небачених раніше загроз національній та міжнародній безпеці.

Принципова неможливість забезпечення на поточному рівні розвитку інформаційних технологій гарантованого захисту інформаційних ресурсів і внутрішніх структур управління сучасними обчислювальними системами від випадкових або зловмисних маніпуляцій породжує безліч загроз, які несуть потенційну небезпеку як для окремо взятої людини, так і для суспільства в цілому. Спектр таких загроз надзвичайно широкий – від електронних крадіжок і прецедентів незаконного розкриття персональних даних до можливості провокування глобальних технічних катастроф, порівнянних за своїми масштабами з Чорнобильською катастрофою або витоком нафти в Мексиканській затоці у 2010 році, які стали найбільшими техногенними світовими катастрофами за останні майже 50 років.

Очевидно, що подібна уразливість дуже приваблива для злочинців, в тому числі, і терористів, оскільки потенційно дозволяє за рахунок порівняно невеликих зусиль кількох зловмисників, що діють в прихованому режимі, викликати катастрофу, яка загрожує життю сотень тисяч, а може бути, і мільйонів людей. При цьому слід враховувати, що самі технології нападу на інформаційні системи або їх злочинне використання, тобто інформаційна зброя,

швидко розвиваються і удосконалюються паралельно з розвитком самих інформаційних технологій і з часом стають доступними для все більш широкого кола потенційних зловмисників.

Саме тому, ми вважаємо, що чіткої визначеності держави у стратегічних пріоритетах та цілях потребує подальший розвиток і захист забезпечення національної безпеки саме у сфері інформаційної безпеки. Відповідні стратегії, доктрини та інші стратегічні державні документи мають відповідати сучасним світовим загрозам, на основі чого повинна вибудовуватись ефективна взаємодія з системами міжнародної і регіональної безпеки та вирішуватись проблемні питання захисту інтересів держави у сфері інформаційної безпеки причетними органами сектору безпеки і оборони нашої держави, в тому числі і Службою безпекою України.

На нашу думку, основним стратегічним документом, що є дороговказом для забезпечення інформаційної безпеки нашої держави є Стратегія національної безпеки України.

Так, у відповідності до ст. 1 Закону України «Про національну безпеку України» № 2469-VIII від 21.06.2018 року Стратегія національної безпеки України (далі – Стратегія) – документ, що визначає актуальні загрози національній безпеці України та відповідні цілі, завдання, механізми захисту національних інтересів України та є основою для планування і реалізації державної політики у сфері національної безпеки [1].

Сучасна Стратегія національної безпеки України «Безпека людини – безпека країни» затверджена Указом Президента України від 14 вересня 2020 року № 392/2020 [2].

У вищевказаній Стратегії в статтях 51-52 Розділу III «Основні напрями зовнішньополітичної та внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки» законодавець чітко закріпив тезу щодо цифрової трансформації в суспільстві:

- Україна здійснить цифрову трансформацію, забезпечить надання адміністративних послуг через безпечне «єдине вікно» з використанням сучасних інформаційних технологій, поширюватиме цифрову грамотність;

- основне завдання розвитку системи кібербезпеки – гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації [2].

Доречно зауважити, що Рада національної безпеки і оборони України своїм рішенням від 14 вересня 2020 року «Про Стратегію національної безпеки України» відповідно до ст. 26 Закону України «Про національну безпеку України» в п. 3 вказаного рішення вирішила надати доручення Кабінетові Міністрів України, державним органам за відповідними сферами національної безпеки подати у шестимісячний строк їй на розгляд проекти Стратегії інформаційної безпеки та Стратегії кібербезпеки України [3].

Зауважимо, що 15 вересня 2021 року Уряд схвалив Стратегію інформаційної безпеки України до 2025 року. Мета прийняття цього стратегічного документу – протидія внутрішнім та зовнішнім загрозам інформаційній безпеці, захист державного суверенітету і територіальної цілісності України, підтримка інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, забезпечення прав та свобод кожного громадянина [4].

Реалізація Стратегії розрахована на період до 2025 року, а результатами реалізації вищевказаної Стратегії мають стати:

- захищений інформаційний простір;
- ефективне функціонування системи стратегічних комунікацій;
- ефективна протидія поширенню незаконного контенту;
- інформаційна реінтеграція громадян України, які проживають на тимчасово окупованих територіях та на прилеглих до них територіях України;
- підвищення рівня медіакультури та медіаграмотності населення;
- забезпечення захисту прав журналістів;
- формування загальнонаціональної ідентичності [4].

В той же час, в поточного році Указом Президент України від 26 серпня 2021 року № 447/2021 була затверджена Стратегія кі-

безпеки України «Безпечний кіберпростір – запорука успішного розвитку країни». Зокрема, в першому розділі вказаної Стратегії законодавець чітко визначив, що забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі. Питома вага кіберзагроз зростає і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. Зростання такого впливу на функціонування структур управління як національних, так і транснаціональних формує нову безпекову ситуацію. Між світовими центрами сили відбувається поділ сфер впливу у кіберпросторі, посилюється їх прагнення за рахунок такого поділу забезпечити реалізацію власних геополітичних інтересів. Кіберпростір разом з іншими фізичними просторами визнано одним з можливих театрів воєнних дій. Набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інформаційної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що включає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами [5].

Таким чином, в цілому, нова Стратегія національної безпеки України значною мірою усуває досі існуючу концептуальну невизначеність і суперечливість в оцінках реальних та уявних загроз і викликів, які постали перед нашою державою, а також шляхів і засобів ефективної протидії. У разі успішної реалізації норм і положень цієї Стратегії можна сподіватися на успішне вирішення проблем оперативно-службової діяльності Служби безпеки України, а також зміцнення позицій України у протидії різноманітним зовнішнім та внутрішнім чинникам, в тому числі й у інформаційній сфері, які загрожують її функціонуванню та розвитку як сучасної демократичної й суверенної держави.

Список використаних джерел:

1. Закон України «Про національну безпеку України» від 21.06.2018 року № 2469-VIII [Електронний ресурс] // Сайт Верховної Ради України. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>
2. Стратегія національної безпеки України «Безпека людини – безпека країни» затверджена Указом Президента України від 14.09.2020 року №392/2020 [Електронний ресурс] // Сайт Президента України. – Режим доступу: <https://www.president.gov.ua/documents/3922020-35037>
3. Рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України» [Електронний ресурс] // Сайт Ради національної безпеки і оборони України. – Режим доступу: <https://www.rnbo.gov.ua/ua/Ukazy/4693.html>
4. Рішення Кабінету міністрів України від 15 вересня 2021 року [Електронний ресурс] // Сайт Кабінету міністрів України. – Режим доступу: <https://www.kmu.gov.ua/news/uryad-shvaliv-strategiyu-informacijnoyi-bezpeki-do-2025-roku>
5. Стратегія національної безпеки України «Безпека людини – безпека країни» затверджена Указом Президента України від 14.09.2020 року №392/2020 [Електронний ресурс] // Сайт Президента України. – Режим доступу: <https://www.president.gov.ua/documents/4472021-40013>

Марусенко Р. І.

кандидат юридичних наук, доцент,
Інститут права КНУ імені Тараса
Шевченка

ПРАКТИЧНІ АСПЕКТИ ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКУМЕНТІВ, ЩО МІСТЯТЬ ВІДОМОСТІ ПРО ОСОБУ

Прогрес у сфері інформаційних технологій прискорив розробку та впровадження нормативних механізмів, що дозволили визначити сутнісні характеристики документів в електронній формі, дозволити їх обіг та надати їм відповідного юридичного значення. Наразі нормативна база є досить розгорнутою, електронні документи використовуються у багатьох сферах. Особливості викори-

стання документів в електронній формі лишаються актуальними для дослідження з огляду на практику їх використання та правові чи технічні механізми реалізації окремих рішень. В даній роботі ми ставимо за мету проаналізувати окремі проблеми практики ідентифікації та автентифікації особи, яка використовує цифровий аналог власноручного підпису, а також практики використання документів, які містять відомості, що ідентифікують особу.

За загальним правилом волевиявлення особи щодо правочину, який вчиняється в письмовій формі, фіксується у вигляді власноручного підпису (ст.207 Цивільного кодексу України). Такий підпис є унікальною послідовністю виконаних людиною знаків письма, яку лише вона може повторити багатократно без спотворення. Підпис дозволяє провести автентифікацію особи, яка проставила підпис, і підтвердити, що саме дана особа його виконала.

Підпис, який виконується в присутності свідків, також дозволяє стверджувати однозначно те, що особа, яка тримає в руках ручку, є тією, воля якої буде зафіксована у підписі. У разі виникнення сумнівів щодо належності виконаного підпису певній особі, його унікальні характеристики дозволяють експерту оцінити вірогідність того, що підпис належить певній особі, і засвідчує саме її волевиявлення. І навпаки, існує можливість доведення факту підписання документа сторонньою особою (фальсифікації підпису). Фактично йдеться про автентифікацію на основі властивості суб'єкта – унікальних особливостей почерку.

Загалом автентифікація здійснюється з використанням трьох видів факторів – знання особою певної інформації, володіння чимось та властивості суб'єкта.

При накладанні електронного підпису мова йде про фактори володіння об'єктом, який має особа (закритий ключ у файлому носії удосконаленого електронного підпису чи в токени – кваліфікованого підпису) та знання (пароль захисту ключа). Теоретично може скластись ситуація, коли файловий чи захищений носій ключа було викрадено чи отримано в інший неправовий спосіб і використано для підписання документів. В такому разі, якщо власник підпису не помітив компрометацію ключа і не звернувся своєчас-

но за скасуванням сертифікату відкритого ключа, то доказування факту накладання електронного підпису неуповноваженою особою буде вкрай складним.

Криптографічні перетворення при перевірці підпису підтверджують факт використання для його генерації певного закритого ключа, який належить чітко визначеній особі. Водночас підпис ніяк не може підтвердити факт, що цим ключем скористався неуповноважений суб'єкт. В цьому кардинальна відмінність електронного підпису від власноручного. Лише другий має унікальний зв'язок з підписантом. Звідси маємо проблему у випадку пропущення електронного підпису без участі особи, яка є власником скомпрометованого ключа. Звісно, існує обов'язок бути обачним і контролювати ключ електронного підпису та його пароль захисту, проте ми розглядаємо ситуацію його втрати не з волі власника. Приклади зловмисної автентифікації, яка, як стверджується, мала місце з використанням ключа іншої особи, хоча й поодинокі, але наявні [1, 2, 3]. Зауважимо, що йдеться не про злам криптографічних алгоритмів, а саме про «злам» системи довіри, коли дійсний ключ був створений чи використаний всупереч процедурі / волі особи. Важливо зауважити, що при компрометації системи генерування ключів (людського компоненту чи виявлення вад програмної реалізації) можна ставити питання про ймовірну компрометацію усіх ключів, згенерованих за певний період часу і необхідність їх заміни. З юридичної точки зору це породжує питання про дійсність усіх документів, підписаних у період часу дії сертифікатів таких ключів.

Вважаємо, що порушене питання є комплексним і не має простої відповіді. Робота над його вирішенням має йти на випередження проблем, які неодмінно поставатимуть зі збільшенням питомої ваги електронних підписів в обігу.

З викладеною проблемою пов'язане питання використання електронних документів, які посвідчують особу за допомогою мобільних носіїв інформації. В даному разі також задіяється ланцюжок довіри. Перевірка документа про особу, який генерується на мобільному терміналі (включаючи унікальний ідентифі-

катор – QR код), проводиться шляхом інформаційної взаємодії із системою, якою користується особа, яка перевіряє документ. Проблеми, які виникають, наприклад, при використанні мобільного додатку Порталу Дія [4] полягають у тому, що поточна реалізація алгоритму перевірки вимагає наявності інтернет-з'єднання з серверною частиною системи для генерування QR коду, що не завжди є можливим (резервний код може бути з різних причин відсутнім на пристрої). Крім того, протягом нетривалої експлуатації системи вже мали місце випадки перерв у її функціонуванні на більш ніж 10 годин [5], що може бути критичним для верифікації документа для посвідчення особи в певний момент часу (наприклад, при посадці в потяг, на літак).

Експерти стверджують [6], що поточна реалізація є надмірно ускладненою і могла бути зроблена без додатків, які імперативно потребують інтернет-зв'язку для роботи. Це підтверджують і посадовці, відповідаючи на запитання щодо ситуації, коли мобільний додаток не працював: «ми навіть заздалегідь попередили поліцію про те, щоб під час переїзду, людей, яких вони зупиняли і в яких не генерувався QR-код на правах, вони перевіряли за номером посвідчення в своїй системі» [7]. Звідси маємо висновок – відсутність документа в особі при наявності такого документа в реєстрі не повинна бути підставою застосування до неї штрафних санкцій. Перевірка особи можлива шляхом співставлення інформації, яку отримує поліцейський, власне з особою.

Водночас, наведену цитату можна сприймати швидше як пояснення, що усе знаходиться під контролем у випадку збоїв у системі. Вочевидь, цьому твердженню можна протиставити численні судові рішення про застосування відповідальності в аналогічних ситуаціях [8]. Юридичні наслідки, вочевидь, залежать від норм права, які не мінялись. Наприклад, при пред'явленні водієм посвідчення водія та свідоцтва про реєстрацію транспортного засобу вимагається пред'явлення документа, сформованого засобами Єдиного державного веб-порталу електронних послуг, зокрема за допомогою мобільного додатка “Дія” [9]. Вочевидь, встановлення особи та перевірка її документів могли б бути проведені засобами

перевіряючого без використання мобільного додатка за механізмом, який був процитований вище. Втім, такої можливості наразі законодавець не надає, потрібні законодавчі зміни.

Протилежний підхід мав місце в процедурі оформлення сертифікатів вакцинації. Відбулося надмірне спрощення, що виходить за межі принципу Окама і також призвело до негативних наслідків. Європейські рекомендації передбачають, що сертифікати мають видаватись органами охорони здоров'я, які провадили імунізацію і вносили дані про вакцинованого до централізованої системи обліку [10]. У вітчизняній системі дану функцію було відокремлено, що призвело, зокрема, до уможливлення внесення до валідного сертифікату неправдивих даних [11]. З огляду на недосконалість впровадженого механізму анонсовано в майбутньому можливість видачі такого документа лікарем, але як вказується, «...це великі доопрацювання, на кілька місяців» [7]. Стверджується, що подібні недоліки є еволюційними. Водночас, якщо з технічної точки зору це є допустимим як наслідок технологій гнучкої розробки апікацій, то з юридичної сторони це є недоліком, адже юридична відповідальність може наставати у конкретний момент часу на підставі конкретних фактів. І вдосконалення технічних механізмів в майбутньому не призведе до ретроспективного переосмислення раніше вчиненого.

Розглянуті практичні ситуації яскраво ілюструють виклики, які виникають при впровадженні електронних документів і підтверджують, що даний процес має бути зваженим, поступовим та гарантувати захищеність прав та інтересів осіб, які можуть постраждати внаслідок прорахунків при відпрацюванні нових механізмів.

Використані джерела.

1. Фльонц В. Скандал з фальшивим «зламом» е-деклараций: хронологія подій URL: <https://www.eurointegration.com.ua/experts/2016/08/22/7053659/> (дата звернення: 20.11.2021).
2. Пилипенко О. Подпись Джо Байдена: ЭЦП в Украине могут подделать. Как это исправит? URL: <https://tech.liga.net/technology/article/>

podpis-djo-baydena-etsp-v-ukraine-mogut-poddelat-kak-eto-ispraviti (дата звернення: 20.11.2021).

3. Корсун К. Цифровий апокаліпсис в Україні оголошується відкритим URL: <https://dou.ua/forums/topic/33960/> (дата звернення: 20.11.2021).

4. Про затвердження Порядку формування та перевірки е-паспорта і е-паспорта для виїзду за кордон, їх електронних копій: Постанова Кабінету Міністрів України від 18.08.2021 №911 URL: <https://zakon.rada.gov.ua/laws/show/911-2021-%D0%BF#n89> (дата звернення: 20.11.2021).

5. Грицик Т. В «Дія» произошел сбой, пропали документы. Что делать URL: <https://ain.ua/2021/11/02/v-prilozhenii-diya-proizoshel-sboj-polzovateli-poteryali-dostup-k-dokumentam/> (дата звернення: 20.11.2021).

6. Цифрові офлайн-документи надійніші, ніж онлайн-документи у «Дії». URL: zn.ua/ukr/TECHNOLOGIES/tsifrovi-oflajn-dokumenti-nadijnishi-nizh-onlajn-dokumenti-u-diji-kiberaljans.html (дата звернення: 20.11.2021).

7. Лукашова С. Михайло Федоров: Без «Дії» у нас кожен другий Covid-сертифікат був би, напевно, підроблений URL: www.pravda.com.ua/articles/2021/11/10/7313425/ (дата звернення: 20.11.2021).

8. Постанова Роменського міськрайонного суду від 8.11.2021, справа № 585/3236/21 URL: <https://reyestr.court.gov.ua/Review/100881750> (дата звернення: 20.11.2021).

9. Про реалізацію експериментального проекту щодо застосування електронного посвідчення водія та електронного свідоцтва про реєстрацію транспортного засобу: Постанова Кабінету Міністрів України від 23.10.2019 №956. URL: <https://zakon.rada.gov.ua/laws/show/956-2019-%D0%BF#Text> (дата звернення: 20.11.2021).

10. Guidelines on Technical Specifications for Digital Green Certificates. Volume 4. European Digital Green Certificate Applications. Version 1.3. 2021-04-21. URL: https://ec.europa.eu/health/sites/default/files/ehealth/docs/digital-green-certificates_v4_en.pdf (дата звернення: 20.11.2021).

11. The bug in the Ukrainian state portal «Dii» allows you to specify any date in the vaccination certificate. URL: twitter.com/vx_hermlt/status/1457031694293340165 (дата звернення: 20.11.2021).

Тарасенко Л. Л.

кандидат юридичних наук, доцент,
доцент кафедри інтелектуальної
власності, інформаційного та
корпоративного права юридичного
факультету Львівського національного
університету імені Івана Франка

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ЯК ОБ'ЄКТ ІТ ПРАВОВІДНОСИН

Інформаційні технології є невід'ємним атрибутом сучасного суспільства. Сьогодні всі люди використовують результати інформаційних технологій. Зокрема, йдеться про всі технічні досягнення людства у цій сфері – телефони, ноутбуки тощо.

Інформаційно-комунікаційні технології є одним з найбільш важливих факторів, що впливають на формування суспільства у 21 столітті. Окінавська хартія глобального інформаційного суспільства від 22.07.2000 р. наголошує на революційний вплив інформаційних технологій, який стосується способу життя людей, їх освіти і роботи, а також взаємодії влади та громадянського суспільства [1].

У науковій літературі слушно зауважують, що динамічне та широке впровадження інформаційно-комп'ютерних технологій та Інтернет-технологій стало причиною появи достатньо великої множини суспільних відносин в різних сегментах суспільного життя, для яких питання правового регулювання стало не зовсім очевидним, що створило суттєві бар'єри на шляху їх застосування [2, с. 15].

Інформаційні технології є важливим фактором розвитку економіки, вони надають можливість людям не лише спілкуватися між собою, а й працювати, при чому працювати більш ефективно.

У законодавстві України немає визначення поняття «інформаційних технологій». Водночас у Законі України «Про державне регулювання діяльності у сфері трансферу технологій» від 14.09.2006 р. наведено визначення поняття «технологія».

Так, відповідно до п. 11 ч. 1 цього закону технологія – це результат науково-технічної діяльності, сукупність систематизованих наукових знань, технічних, організаційних та інших рішень про перелік, строк, порядок та послідовність виконання операцій, процесу виробництва та/або реалізації і зберігання продукції, надання послуг.

На нашу думку, ознаками технології є:

- наявність результату науково-технічної діяльності;
- наявність сукупності певних систематизованих наукових знань;
- наявність технічних, організаційних та інших рішень про перелік, строк, порядок та послідовність виконання операцій, процесу виробництва та/або реалізації і зберігання продукції, надання послуг.

Доцільно також згадати про те, що цей закон виділяє також поняття і високих технологій, під якими слід розуміти технології, розроблені на основі новітніх наукових знань, які за своїм технологічним рівнем перевищують кращі вітчизняні та іноземні аналоги і конкурентоспроможні на світовому ринку наукомісткої продукції (п. 1 ст. 1 Закону України «Про державне регулювання діяльності у сфері трансферу технологій» від 14.09.2006 р.). Високі технології включають в себе новітні наукові знання, які перевершують всі відомі у світі аналоги у відповідній сфері.

Слід звернути увагу на те, що технології, які є новими і конкурентоздатними, вважаються інноваціями. Такий висновок випливає з аналізу поняття інновацій, що наведено у ст. 1 Закону України «Про інноваційну діяльність».

Результат інформаційних технологій може бути визнано інноваційним продуктом. Законодавець встановлює вимоги, яким повинен відповідати такий інноваційний продукт. Так, результат інформаційних технологій повинен бути реалізацією (впровадженням) об'єкта інтелектуальної власності (переважно йдеться про патентовані технології – винаходи, корисні моделі, промислові зразки), на які виробник продукту має охоронні документи, видані державою (зокрема, патенти, свідоцтва), чи одержані від

правовласників ліцензії, або реалізацією (впровадженням) відкриттів.

При цьому використаний об'єкт інтелектуальної власності має бути визначальним для даного продукту. Такий результат інформаційних технологій повинен підвищувати вітчизняний науково-технічний та/або технологічний рівень і повинен бути конкурентоздатним (наявність суттєво вищих техніко-економічних показників).

Сучасні інформаційні технології вже не обмежуються рамками однієї держави, а мають загальносвітове значення [3, с. 22].

Інформаційні технології допомагають розвивати інновації. Саме вони вказують на темпи зростання, розвитку та модернізації в середині країни. Також новітні інформаційні технології справили значний вплив на розвиток національних законодавств про охорону авторських прав усіх без винятку держав світу та на міжнародно-правову охорону авторських прав [4, с. 8]. Це зумовлено тим, що контент веб-сайту – це об'єкти авторського права: тексти (як літературні твори), фотографії, зображення, дизайн, музика, аудіовізуальні твори.

Інформаційні технології визначаються як цілісна система операцій щодо збирання, зберігання, обробки та передавання інформації, що здійснюється з використанням комп'ютерної техніки та телекомунікаційних каналів зв'язку [5, с. 10].

Інформаційні технології формують оновлене інформаційне суспільство, в якому кожен матиме доступ до результатів цих технологій, в тому числі через розширення доступу до мережі Інтернет і можливості здійснювати різні права в цифровому середовищі.

Інформаційне суспільство, яке формується, дозволяє людям ширше використовувати свій потенціал. Всі люди повсюдно, без винятку, повинні мати можливість користуватися перевагами глобального інформаційного суспільства через використання інформаційних технологій. В Окінавській хартії глобального інформаційного суспільства наголошується на тому, що стійкість глобального інформаційного суспільства ґрунтується на стимулюю-

чих розвиток людини демократичних цінностях, таких як вільний обмін інформацією та знаннями, взаємна терпимість і повага до особливостей інших людей [1]. Дійсно, завдяки інформаційним технологіям обмін інформаційними ресурсами і пошук необхідної інформації здійснюється в рази швидше, що сприяє здійсненню багатьох прав.

Інформаційні технології змінюють саму людину, її мислення, можливості, спосіб і ритм життя, систему цінностей [6, с. 6]. Погоджуємося з такою думкою і відзначаємо наявність суттєвого впливу інформаційних технологій на людину і її поведінку. Сьогодні ніхто з нас не уявляє себе без Інтернету та інших результатів інформаційних технологій, при чому інколи це може спричиняти навіть різні види залежності від інформаційних технологій.

Відзначаємо, що інформаційні технології тісно пов'язані з Інтернетом, завдяки якому відбувається їх пришвидшене застосування.

Правовідносини у сфері інформаційних технологій традиційно складаються з таких елементів як суб'єкти, об'єкти та зміст.

Суб'єктами цих правовідносин є:

- суб'єкти, які створюють продукти інформаційних технологій (розробники програмного забезпечення, ІТ компанії тощо);
- суб'єкти, які обслуговують ці інформаційні продукти, підтримують їх функціонування (так звані сервісні ІТ компанії),
- суб'єкти, які допомагають функціонувати мережі Інтернет (провайдери, надавачі послуг хостингу, адміністратори адресного простору мережі Інтернет, реєстратори тощо),
- суб'єкти – користувачі інформаційних технологій (користувачі Інтернету, користувачі за стосунків тощо).

Окремо відзначаємо державу, яка повинна сприяти усім учасникам відносин у сфері інформаційних технологій у здійсненні їх прав.

Об'єктами відносин інформаційних технологій є: комп'ютерне програмне забезпечення; веб-сайт, інформаційні ресурси та продукти, інформаційні послуги, доменні імена.

Ці об'єкти значною мірою співпадають з об'єктами правовідносин у мережі Інтернет. Зокрема, до останніх у науковій літературі відносять:

- 1) телекомунікаційні мережі та інше технічне обладнання;
- 2) комп'ютерне програмне забезпечення;
- 3) інформація, інформаційні ресурси, інформаційні продукти, інформаційні послуги (це основний об'єкт цих правовідносин; інформація може бути технічна, економічна, соціальна, юридична та ін. Вона стирає грані між продуктом і послугою, що знаходить своє втілення в сучасних технологіях, які об'єднують інформаційні продукти і послуги в єдине ціле);
- 4) доменні імена;
- 5) права та свободи в сфері інформації;
- 6) інформаційна безпека [7].

На основі вищенаведеного, вважаємо, що під інформаційними технологіями слід розуміти результат інтелектуальної творчої діяльності, сукупність технічних, організаційних та інших рішень щодо збирання, зберігання, обробки та передавання інформації, інших об'єктів інформаційних технологій (зокрема, програмне забезпечення), що здійснюється з використанням комп'ютерної техніки та телекомунікаційних каналів зв'язку, та спрямовані на розвиток інновацій.

Використані джерела:

1. Окінавська хартія глобального інформаційного суспільства від 22.07.2000. URL: https://zakon.rada.gov.ua/laws/show/998_163/conv#Text (дата звернення 20.10.2020).
2. Баранов О. А. Напрями перспективних досліджень у галузі інформаційного права. Інформація і право. 2016. № 2(17). С. 15-31.
3. Кормич Б. А. Інформаційне право: підручник. Харків: Бурун і К., 2011. 334 с.
4. Ващинець І. І. Цивільно-правова охорона авторських прав в умовах розвитку інформаційних технологій: автореф. к.ю.н. К., 2006. 20 с.
5. Синєокий О. В. Інформаційне право України та електронне право високих технологій. Запоріжжя: ЗНУ, 2010. 215 с.

6. Триняк В. Ю. Інформаційна безпека як соціокультурний феномен (соціально-філософський аналіз): автореф. к. філ.н. Д., 2009. 20 с.

7. Еннан Р. Правове регулювання відносин у мережі Інтернет. Матеріали Конференції «ІТ право: проблеми і перспективи розвитку в Україні». 2017. URL: <http://aphd.ua/publication-173/> (дата звернення 28.11.2021).

Чорна В. Д.

здобувач першого (бакалаврського)
рівня вищої освіти
Дніпропетровського державного
університету внутрішніх справ

Алексєєнко І. В.

доктор політичних наук, професор,
завідувач кафедри міжнародних
відносин Дніпропетровського
державного університету внутрішніх
справ

ІНФОРМАЦІЙНІ ПРАВА ЛЮДИНИ В УКРАЇНІ: ПРОБЛЕМАТИКА ПРАВОВОГО ВИЗНАЧЕННЯ

На стику XX-XXI століть у сфері інформаційних технологій відбулися відповідні зміни, які пов'язані з масовою діджиталізацією та стрімким розвитком сфери інформаційних технологій. Саме завдяки, якісним перетворенням інформаційна сфера набула домінуючого характеру. В свою чергу, сформувалася інформаційна розвиненість суспільства, яка стала основою еволюції усіх сфер суспільного життя і досить-таки стрімко просуває людство на шляху становлення інформаційного суспільства, яке розглядається багатьма вченими як нова постіндустріальна формація.

Виникнення інформаційного суспільства призвело до утвердження примату «інформаційних прав». Відповідно до ст. 3 Конституції України: права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави [3]. Держава покли-

кана охороняти та забезпечувати права та свободи людини. Саме сукупність інформаційних прав гарантують кожному можливість на власну точку зору та переконання, громадяни наділяються правом вільно висловлювати свої думки та не піддаватися переслідуванням з боку держави.

В Україні стрімко розвивається інформаційне суспільство, що сприяє популяризації інформаційних прав як прав четвертого покоління. Сукупність прав та свобод громадян в сфері інформаційного суспільства є невідчужуваними та непорушними. Дотримання та гарантування інформаційних прав покладається на державу, яка має сприяти реалізації цих прав.

В контексті зазначеного, слід надати визначення дефініції «інформаційні права». За останні роки термін «інформаційні права» не отримав поширення, адже кожен дослідник виокремлює власний перелік таких прав. Одна група науковців вважає, що під інформаційними правами слід розуміти – можливість отримувати, використовувати та оприлюднювати інформацію; інші вважають, що до інформаційних прав належить й право на приватність, честь та гідність в мережі. Третя група дослідників зауважує, що інформаційні права є новою категорією для сучасного права, адже вони формуються лише в умовах інформаційного суспільства, а відповідно до системи інформаційних прав належать: право на доступ до мережі Інтернет та право на захист персональних даних [1, с. 7].

Тому, в контексті зазначеного, слід проаналізувати не лише сутнісний зміст категорії «інформаційні права», але й виокремити їх особливості. Під інформаційними правами слід розуміти – сукупність можливостей кожної особи на доступ до інформації, можливість отримувати, використовувати, поширювати, коментувати певну інформацію; спілкуватися в мережі інтернет. Зазначимо, що інформаційні права є не обов'язком громадян, а їх можливістю. Тобто, особи мають право не використовувати інформаційні права та відповідно не реалізовувати їх. Обсяг використання та міра реалізації комплексу інформаційних прав залежить від волі кожної особи, а не від державних приписів. З приводу зазначеного, у на-

уковців виникають суперечки, більшість з них стосується різного розуміння правової категорії «інформаційні права», тому проаналізуймо деякі точки зору.

Більшість науковців вважають, що інформаційні права слід отожднювати з правом на інформацію. В контексті зазначеного, можемо виокремити два підходи, що сформувалися у сучасній науці. Відповідно до широкого підходу, інформаційні права за змістом є більш широким поняттям, яке складається з права на інформацію та права на свободу слова, вільне вираження своїх думок. Тому, інформаційні права та право на інформацію розглядаються як ціле та часткове. Інформаційні права і свободи людини та громадянина належать до так званих прав «першого покоління» – громадянських, політичних, які першочергово визначались як невід’ємна частина людської гідності. Тобто, дефініції «інформаційні права» та «право на інформацію» не є тотожними, а схема їх співвідношення: «загальне – часткове» [2, с. 156].

Основні права і свободи в інформаційній сфері підкріплюються і в деякій мірі розширюються за рахунок інших гарантованих Конституцією України прав і свобод людини і громадянина. Наприклад, ст. 41 Конституції визначає право кожного володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності та встановлює непорушність права приватної власності, що також гарантує реалізацію прав інтелектуальної власності щодо інформації та прав власності на інформаційні ресурси (хоча й не кожен результат інформаційної діяльності – продукт інтелектуальної, споглядальної, творчої, аналітичної роботи тощо – стає продукцією-об’єктом, що мають споживчу вартість і характеристики, що дозволяють використовувати його як товар, та, відповідно, об’єкт права власності) [3].

Щодо другого підходу, то прихильники цієї точки зору вважають, що більш доцільно змістовно отожднювати два поняття, адже право на інформацію не може існувати окремо від інформаційних прав, право на інформацію розглядається виключно в контексті науки інформаційного права. Прихильники вузького підходу зауважують, що право на інформацію є суб’єктивним правом

кожної особи, яке в свою чергу складається з можливостей особи виконувати відповідні операції з інформацією, незалежно від призначення та змісту. Зауважимо, що інколи, інформаційні права можуть поглинати інші суб'єктивні права у сфері інформаційного суспільства. Мова йде про такі права як право на свободу слова та на свободу обміну інформацією. За своїм змістом, інформаційні права вже включають в себе усі суб'єктивні права, що сформовані у суспільстві, а відповідно й можуть витіснити деякі з них [4, с. 115].

Тому, здійснивши аналіз різних точок зору, вважаємо, що обрати один з підходів не раціонально, адже в конкретному виборі немає сенсу. Кожен із сформованих підходів відображає різні етапи еволюції прав людини в інформаційному середовищі. Все ж таки, ми поділяємо позицію представників широкого підходу, і маємо свою точку зору щодо висловленого. По-перше, право на інформацію та інформаційні права – конкретне та абстрактне, а тому, отожднювати ці поняття неможливо. Інформаційні права за своїм обсягом ширше поняття, адже включає в себе не лише можливість збирати, використовувати, оприлюднювати інформацію у будь-який спосіб, але й суміжні права, що витікають з виконання певних дій. По-друге, запропонована науковцями схема співвідношення двох дефініцій «загальне-часткове» є правильною, адже інформаційні права – загальне поняття, а право на інформацію є складовою частиною інформаційних прав, яка перебуває у підпорядкуванні «інформаційних прав».

Крім того, сутність інформаційних прав людини проявляється в їх основних властивостях, які допомагають сформувати уявлення про те, що ж собою взагалі являють інформаційні права людини. Тому, ми виокремили такі сутнісні риси інформаційних прав [1, с. 10]:

1. Це основоположні можливості людини, які необхідні їй для задоволення потреб у інформаційному суспільстві.
2. Усі інформаційні права громадян невідчужувані та гарантовані державою.
3. Держава наділяє інформаційні права універсальністю та пріоритетністю. Нормативне врегулювання цієї категорії прав та

свобод відбувається не лише на підставі національного, але й міжнародного законодавства.

4. Становлять феномен, який можна дослідити лише через вивчення системних властивостей, що знаходить своє відображення у наявності прав та свобод інформаційного характеру майже у кожній сфері діяльності суспільства.

Отже, дослідження правової природи та сутності інформаційних прав залишається актуальним питанням для сучасної науки. Відсутність єдиного визначення поняття «інформаційні права» призводить до палких дискусій у наукових колах, незважаючи на панування різних точок зору, ми дійшли висновку, що інформаційні права – багатоаспектне правове явище, сутність якого полягає у тому, що всі громадяни держави можуть використовувати, зберігати, оприлюднювати, застосовувати ті чи інші інформаційні джерела. Інформаційні права є невідчужуваними, реалізація цих прав залежить від волі людини.

Література:

1. Брижко В. М. Інформаційний продукт як об'єкт права власності. *Інформація і право*. 2017. №4. С. 5-15.
2. Вакарюк Л. Основні підходи до розуміння поняття «інформаційні права людини». Підприємництво, господарство і право. 2018. №2. С. 155 – 159.
3. Конституція України: Закон України від 28.06.1996 р. № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96%D0%B2%D1%80#Text> (дата звернення: 20.11.2021).
4. Костецька Т. А. Конституційно-правове регулювання інформаційних прав: деякі термінологічні аспекти. *Часопис Київського університету права*. 2013. №2. С. 114-117.

Сероштан М. Г.

здобувач першого (бакалаврського)
рівня вищої освіти
Дніпропетровського державного
університету внутрішніх справ

Алексєєнко І. В.

доктор політичних наук, професор,
завідувач кафедрою міжнародних
відносин Дніпропетровського
державного університету внутрішніх
справ

**ПИТАННЯ ВДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА
З ПИТАНЬ ЗАХИСТУ ПРАВ ЛЮДИНИ В УМОВАХ
ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ
(ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ,
ЗАБЕЗПЕЧЕННЯ ІНФРАСТРУКТУРНОЇ БЕЗПЕКИ,
КІБЕРБЕЗПЕКИ ТОЩО)**

Сьогодні кожна країна потребує своїх навичок для захисту конституційних прав і свобод своїх громадян, особливо у сфері зв'язків з громадськістю, де застосовність продуктів інформаційно-комунікаційних технологій (ІКТ) має вирішальний вплив на життєво важливі послуги, бізнес та безпеку. всього зв'язку, життя громадян, суспільства і держави. Крім того, проникнення таких технологій у повсякденне життя потребує нових знань у новому середовищі – кіберпросторі, від якого можна очікувати не лише безлічі сервісів та переваг, а й розвитку існуючих та створення нових загроз. Ці загрози пов'язані з використанням механізмів несанкціонованого втручання в системи та порушенням безпеки інформації, яку вони обробляють, постійною еволюцією індустрії розробки та широким використанням різноманітного шкідливого та вразливого програмного забезпечення, використанням спеціальних операцій у кіберпросторі над критично важливою інформацією. інфраструктура тощо.

У 2010 році Україна підписала Конвенцію про захист людини з автоматичною обробкою персональних даних. Цей документ – перша міжнародна угода про необхідність захисту персональних даних – була складена в січні 1981 року [1].

З цієї причини у 1968 р. Європейська парламентська асамблея видала Рекомендацію № 509 про усунення загроз прав людини шляхом використання автоматизованої обробки даних [2]. У 1981 році була відкрита для підписання Конвенція про захист людини з автоматичною обробкою персональних даних (Конвенція 108). Цей міжнародний інструмент поширюється на будь-який процес обробки даних, який здійснюється як у приватному, так і в державному секторах. Документ став додатковою юридичною гарантією того, що особа має право контролювати потік персональних даних, зокрема знати, хто їх збирає, з якою метою, як вони використовуються, зберігаються чи комусь передаються.

Ця конвенція вводить поняття «адекватного» (або адекватного, адекватного) рівня захисту персональних даних державою. Особливо в контексті транскордонних переказів та обмінів.

«Однак розвиток цифрового світу триває і ставить перед суспільством нові виклики. Зростає проблема нелегального витоку даних та використання персональних даних. Це дало поштовх до вдосконалення чинної Конвенції 108. У травні 2018 року Рада Європи прийняла протокол CETS №223, яким внесено до нього зміни», – пояснила Шадська.

Модернізована Конвенція 108+ встановлює суворіші правила, щоб звести до мінімуму всі ризики порушення приватності через використання технологій. Зараз це стосується як автоматизованої, так і неавтоматизованої обробки даних, але жодним чином не обмежує дії осіб для власних потреб.

Документ також посилив вимоги щодо контролю за обробкою особливої категорії даних, таких як біометричні або генетичні дані, регулювання транскордонних передач та обміну даними в контексті міжнародного співробітництва.

Важливим нововведенням став обов’язок повідомляти про втік даних.

Найближчим часом перед Україною постане питання ратифікації протоколу CETS № 223, а також відповідальності за імплементацію модернізованої Конвенції 108+.

«Одною з вимог Конвенції є створення наглядового органу у сфері захисту персональних даних із далекосяжними повноваженнями. Тому надзвичайно важливими є гарантії забезпечення її незалежності та визначення її місця в системі органів державної влади.

В Україні наразі Уповноважений Верховної Ради з прав людини контролює дотримання законодавства про захист персональних даних.

У червні 2021 року в парламенті зареєстровано проект Закону № 5628 «Про захист персональних даних». Зокрема, він служить модернізації національного законодавства у цій сфері та гармонізації його з європейськими стандартами.

Документ містить, зокрема:

- гармонізація термінології у сфері захисту персональних даних з новими міжнародними стандартами;
- деталізації та роз'яснення принципів обробки персональних даних;
- більш чітке формулювання причин обробки персональних даних;
- детальні та прозорі вимоги щодо згоди на обробку персональних даних, які запобігають неправомірному використанню та маніпуляціям;
- розширення прав суб'єктів персональних даних та механізмів їх реалізації;
- чітке визначення відповідальності відповідальної особи та оператора персональних даних;
- порядок повідомлення про втрату персональних даних;
- Обробка передачі персональних даних на територію іноземних держав та міжнародних організацій;
- фінансова відповідальність, адміністративно-господарські санкції до відповідальної особи та/або оператора за порушення права на захист персональних даних та гарантії ефективності закону та дотримання його вимог [3].

Він також значно розширює права суб'єкта даних, зокрема визначає механізми захисту прав на інформацію, доступу до персональних даних, виправлення персональних даних, право суб'єкта даних бути забутим, заперечення проти обробки персональних даних. дані та їх обмеження, права суб'єктів даних на захист їх прав і збитків тощо.

Аналіз чинного законодавства України свідчить про те, що існуючі права та обов'язки людей та громадян у сфері інформації слід розглядати як особливу групу прав – інформаційні права, до яких належать: право на вільний пошук інформації, право на інформацію, право на інформацію, право на інформацію, право доступу тощо.

На думку Белєвцева В. В. у правовій системі Української держави існують дві можливості інформаційних прав і свобод людей і громадян: 1) шляхом прийняття нових нормативно-правових актів національного характеру, які закріплюють нові інформаційні права людей і громадян; 2) шляхом ратифікації міжнародних договорів, що містять нові інформаційні права людей і громадян. Дослідження законодавства України про інформаційне забезпечення показало існування такого правового явища, як правовий механізм захисту інформаційних прав і свобод людей і громадян, який є своєрідним механізмом захисту прав і свобод людей і громадян в цілому [4].

Правовий механізм захисту інформаційних прав і свобод людей і громадян поділяється на нормативно-правовий та організаційно-правовий. Нормативно-правова форма виражається в прийнятті нормативно-правових актів або у внесенні в діючі нормативно-правові акти таких змін, які можуть сприяти захисту інформаційних прав людини і громадянина. На основі аналізу елементів нормативно-правового механізму захисту інформаційних прав і свобод людини і громадянина, його характеристики як правового явища, що полягають у своєрідності інформаційної сфери, в якій цей механізм реалізується, а також об'єкти (об'єкти), з якими існують відповідні правовідносини (інформація та її носії) [5]. Слід підкреслити, що правовий механізм захисту прав людини і гро-

мадянина є частиною правового механізму захисту всіх конституційних прав та обов'язків. Однією з найважливіших складових правового механізму захисту прав людини і громадянина в Україні є їх гарантії. Зміст правових гарантій інформаційних прав і свобод людей і громадян, які закріплені в міжнародно-правових актах і національному законодавстві, практично ідентичний. Однак причини їх можливого обмеження та безпосередніх обмежень, визначені в міжнародних документах та національному праві, не завжди збігаються. У цьому контексті пропонуємо уніфікувати перелік причин обмеження інформаційних прав і свобод людей і громадян та скласти перелік випадків їх негайного обмеження з подальшим правовим закріпленням. Необхідно звернути увагу на особливості нормативно-правового механізму захисту інформаційних прав і свобод людини і громадянина [6].

Можна з упевненістю сказати, що на даному етапі розвитку всесвітньої павутини майже вся інформація, записана людьми, включаючи персональні дані, обертається та/або зберігається. Основною проблемою тут є відсутність ефективних та перевірених адміністративно-правових інструментів, які могли б забезпечити повний і комплексний захист персональних даних у віртуальному середовищі (контроль місцезнаходження, транзиту, доступу до своїх даних, можливість їх відкликання тощо).

Список літератури

1. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108)
2. Рекомендація №509
3. Законопроект №5628 “Про захист персональних даних”
4. Белєвцева В. В. Правовий захист інформаційних прав і свобод людини і громадянина в Україні: проблеми та перспективи / В. В. Белєвцева, В. Я. Настюк // Інформація і право, 2015. – № 2 (14). – С. 20-25.
5. Про інформацію: Закон України від 02.10.1992 № 2657-ХІІ (із змінами) // Відом. Верхов. Ради України. – 1992 р. – № 48. – Ст. 650.
6. Конституція України від 28 червня 1996 р. // Відом. Верх. Ради України. – 1996. – № 30. – Ст. 141.

Швед А. С.

студентка Чернівецького
національного університету
ім. Ю. Федьковича

Науковий керівник: Заморська Л. І.

доктор юридичних наук, доцент
кафедри теорії права та прав людини
Чернівецького національного
університету ім. Ю. Федьковича

ВДОСКОНАЛЕННЯ ЗАКОНОДАВСТВА З ПИТАНЬ ЗАХИСТУ ПРАВ ЛЮДИНИ В УМОВАХ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ

Сучасний світ характеризується, в першу чергу, розвитком цифрових технологій та прогресом у галузі інформаційних технологій. Активізація у розробці численних програм та додатків, які полегшують життя людей, формування персональних баз даних, впровадження електронних підписів – все це потребує використання великої кількості персональних даних осіб та інформації про них. Проте доступ до особистої інформації вимагає забезпечення надійного правового захисту її від зловмисників. На сьогодні відомо декілька серйозних випадків несанкціонованого доступу до комп'ютерних систем з метою отримання секретної інформації, що безпосередньо стосується усіх громадян та їх прав. Саме тому питання кібербезпеки постає дуже гостро.

Аналізуючи дослідження щодо питань захисту персональних даних варто вказати, що вони здійснювались рядом українських та зарубіжних вчених, як, наприклад: В. Брижко [1], Т. Обуховська [4], В. Пилипчук [5] та інші. У працях вищевказаних науковців, зокрема Т. Обуховської та В. Шуляка ретельно досліджена нормативно-правова база у сфері захисту персональних даних в Україні, визначено основні проблемні питання нормативно-правового врегулювання дій з персональними даними під час їх обробки та циркуляції в державних інформаційних ресурсах органів держав-

ної влади та органів місцевого самоврядування та шляхи їх вирішення, запропоновано конкретні пропозиції щодо вдосконалення нормативно-правової бази. [4, с. 96] Проте актуальним залишаються проблеми європезації стандартів кібербезпеки, визначення її основних принципів та підходів, а також використання досвіду інших держав.

Не можна заперечувати спроби українських органів влади забезпечити захист персональних даних. Прикладом є ратифікація Україною Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних [2], прийняття Закону України «Про захист персональних даних», що набув чинності 1 січня 2011 року та 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 [7], а також Закон України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних», який набув чинності 1 січня 2014 року. [6]

З часом, у низці міжнародних документів було деталізовано принципи та умови досягнення гармонії національних законодавств у сфері захисту персональних даних. Це також сприяло зміні у Європі та Америці розуміння терміну «приватність» як право на недоторканість особистого життя, на «право на інформаційний суверенітет особи», тобто право людини самостійно та незалежно вирішувати хто, коли, з якою метою та яким чином може використовувати особисту інформацію про неї. [5, с. 61], [1, с. 46]

Принципи захисту персональних даних були розроблені експертною групою Організації з економічного співробітництва і розвитку (далі – ОЕСР). Основна проблема розробки полягала у неоднорідному ставленні країн, що є членами вищевказаної організації. Всі вони дотримувались різних підходів до побудови системи правового захисту особистих даних, а саме: генерального, секторного (галузевого) і змішаного. Певні держави підтримували всі підходи. [4, с. 97]

На національному рівні ОЕСР передбачає такі обов'язки для держав – членів:

- прийняти належні національні закони;
- заохочувати і підтримувати саморегулювання шляхом прийняття кодексів поведінки/поводження або інших правил;
- забезпечити наявність розумних механізмів реалізації індивідуальних прав;
- застосувати необхідні санкції та інші засоби захисту персональних даних на випадок невиконання заходів, що передбачені зазначеними принципами;
- забезпечити недискримінаційне ставлення до суб'єктів даних. [4, с. 97-98]

Міжнародне співробітництво передбачає дотримання таких принципів, як:

- надання іншим державам-членам на їх прохання детальну інформацію про дотримання принципів, перерахованих у базових принципах;
- вживати заходів для спрощення процедури міжнародного обміну персональними даними і захисту недоторканності приватного життя та індивідуальних свобод;
- введення в дію процедури, що сприяє взаємодопомозі в здійсненні процедур і проведенні розслідувань з питань, що представляють взаємний інтерес;
- розробка внутрішніх принципів на яких будуть базуватися закони про міжнародний обмін персональними даними. [4, с. 98]

На нашу думку, основними принципами забезпечення кібербезпеки в Україні є:

- забезпечення національних інтересів України;
- невідворотності покарання за вчинення кіберзлочинів;
- пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід'ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі;

- відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі. [8]

Також здійснення забезпечення охорони персональних даних відбувається за допомогою Конституції України (далі КУ). Наприклад, згідно з ст. 31 КУ «кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції...» [3], а згідно з ч. 1 та ч. 2 ст. 32 КУ «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...» [3].

Проте, незважаючи на формальний захист вказаних прав, проблема неправомірних дій стосовно персональних даних фізичних осіб все ще актуальна. Наприклад: 1) більшість баз персональних даних у функціонуванні не є автономними, що суперечить вимогам міжнародних правових стандартів; 2) передача персональних даних за кордон не має реального організаційно-правового механізму; 3) на багатьох ринках має місце незаконна торгівля CD з персональними даними; 5) продовжує функціонувати відповідна система збирання і продажу адресних списків персональних даних тощо. [1, с. 46]

Також до захисту персональних даних висуваються певні вимоги. На нашу думку, основними з них є:

- законність шляху отримання та обробки персональних даних;
- збереження та використання персональних даних у визначених та законних цілях;
- неможливість автоматизованої обробки персональних даних, що свідчать про расову належність, політичні, релігійні чи інші переконання, а також дані, що стосуються здоров'я або статевого життя, якщо внутрішнє законодавство країни не забезпечує відповідних гарантій;
- передбачення безпеки персональних даних від випадкового та несанкціонованого доступу, знищення, модифікації, блокування, розповсюдження та випадкової втрати. [4, с. 98]

Отже, після дослідження принципів захисту персональних даних, вимог щодо нього, а також дослідження досвіду інших держав ми зробили висновки, що питання якісного, швидкого та абсолютного захисту особистих даних все ще не вирішене. І хоч на сьогодні існує достатньо формальних способів обмеження несанкціонованих дій щодо особистих даних за допомогою законодавства, на практиці поширеним залишається зловживання доступом до персональних даних та часті випадки кібератак.

Використана література:

1. Брижко В. М Сучасні основи захисту персональних даних в європейських правових актах [Електронний ресурс] / В. М. Брижко // Інформація і право. – 2016. – №3. – С. 45-57. – Режим доступу: http://nbuv.gov.ua/UJRN/Infpr_2016_3_8
2. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних [Електронний ресурс] / : Конвенція Ради Європи № 108 від 28 січ. 1981 р. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/994_326
3. Конституція України [Електронний документ] / : Відомості Верховної Ради України (ВВР). – 1996. – № 30. – Режим доступу: <https://www.president.gov.ua/documents/constitution>
4. Обуховська Т. І. Захист персональних даних в умовах розвитку інформаційного суспільства : передумови, принципи та міжнародне законодавство / Т. І. Обуховська // Вісник Національної академії державного управління при Президентові України. – 2014. – № 1. – С. 95-103. – Режим доступу: http://nbuv.gov.ua/UJRN/Vnadu_2014_1_17
5. Пилипчук В. Г., Брижко В. М. Інформаційна безпека та приватність у сфері захисту персональних даних [Електронний ресурс] / В. Г. Пилипчук, В. М. Брижко // Інформація і право. – 2016. – №4. – С. 60-70. – Режим доступу: http://nbuv.gov.ua/UJRN/Infpr_2016_4_9
6. Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних [Електронний ресурс] / : Закон України № 383-VII від 3 липня 2013 р. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/383-18>
7. Про захист персональних даних [Електронний ресурс] / : Закон України № 2297-VI від 1 черв. 2010 р. – Режим доступу : <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2297-17>

8. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] / : Закон України № 2163-VIII від 1 серпня 2021р. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2163-19>

Чорнобай Е. О.

студентка НТУУ

«КПІ ім. Ігоря Сікорського»

Науковий керівник: Фурашев В. М.

канд. техн. наук., доцент, старший

науковий співробітник, заслужений

машинобудівник України

СИСТЕМИ РОЗПІЗНАВАННЯ ОБЛИЧ: ПРИВАТНІСТЬ ПРОТИ БЕЗПЕКИ

В епоху цифрової інформації, коли майже у кожного є смартфон, який можна розблокувати за допомогою відбитка пальця чи власного обличчя, коли будь-яку інформацію можна знайти в мережі Internet за лічені секунди, коли твоє фото чи відео може побачити будь-хто з будь-якого куточка планети, мало хто розуміє, яку небезпеку може становити таке повсюдне використання цифрових технологій.

З-поміж усієї різноманітності гаджетів та систем є такі, що призначені для виявлення та розпізнавання людей за допомогою фото- чи відеофіксації їх зображень спеціально обладнаними для цього камерами з інтегрованими до них системами розпізнавання облич (далі – СРО). Теоретичне призначення СРО – протидія злочинності та підтримка громадської безпеки, однак у «погоні» за нею держави можуть серйозно зловживати своїми технічними та технологічними можливостями, нехтуючи нерозривно пов'язаними із головними цінностями концепції прав людини правами людей на конфіденційність та приватність.

В Україні особливо актуальними є питання, пов'язані із застосуванням СРО, в рамках запуску програми «Безпечне місто» у низці міст України за підтримки Міністерства внутрішніх справ

України. На центральних площах та вулицях міст, на перехрестях та в метро встановлюються камери з функцією розпізнавання номерних знаків автомобілів, безконтактного розпізнавання облич, статі та навіть температурного скринінгу [1].

Призначення цих систем полягає у підтримці правопорядку та безпеки на вулицях міст України, протидії злочинності та розшуку порушників законодавства, визначенні місць масового скупчення людей, зокрема під час масових заворушень. Однак законність застосування СРО залишається під великим питанням, а інтеграція СРО в наявні системи спостереження створює серйозний ризик для конфіденційності і захисту персональних даних людини, а також для інших фундаментальних прав, оскільки використання цих технологій не завжди передбачає усвідомлення або співпрацю осіб, чиї персональні, зокрема, біометричні дані обробляються. Крім того, така неусвідомленість може перерости у грубі порушення фундаментальних прав людини за умови відсутності належного правового регулювання та механізмів контролю у сфері застосування таких СРО.

В Україні відеокамери, обладнані СРО, використовуються переважно органами місцевого самоврядування та комунальними підприємствами. Однак наразі у місцевої влади відсутні правові підстави для встановлення подібних комплексів відеоспостереження, не кажучи вже про інтеграцію до них СРО. Керуючись статтею 38 Закону України «Про місцеве самоврядування в Україні», органи місцевого самоврядування намагаються виправдати застосування таких систем, однак вказана стаття не надає право місцевій владі використовувати зазначені техніко-технологічні засоби для нагляду за населенням. Більш того, жоден чинний нормативно-правовий акт комплексно не регламентує ані законне застосування таких систем відеоспостереження, ані, тим паче, збір, обробку, зберігання та використання даних, отриманих за допомогою СРО.

Законодавством України гарантовано дотримання права людини на невтручання в її особисте життя, окрім окреслених законодавством випадків. Водночас якщо за допомогою відеозапису

можна прямо або опосередковано ідентифікувати особу, то він завжди є носієм персональних даних.

Зокрема, статтею 32 Конституції заборонено «збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом» [2]. Стаття 307 Цивільного кодексу України вказує на те, що знімання фізичної особи на відеоплівку, в тому числі таємне, без згоди особи може бути проведене лише у випадках, встановлених законом [3]. А Закон України «Про захист персональних даних» (далі – Закон) зобов'язує володільців і розпорядників персональних даних забезпечити їх надійний захист від незаконного доступу, обробки, втрати та знищення таких даних [4].

За даними Звіту Асоціації УМПДПЛ «(Майже) старший брат стежить за тобою: відеоспостереження за дотриманням публічного порядку в Україні» (далі – Звіт), *майже всі суб'єкти, які використовують системи відеоспостереження, всупереч усталеній практиці, зокрема Європейського суду з прав людини, не вважають зображення особи (обличчя, силуету) персональними даними, бо це прямо не передбачено Законом* [5]. Враховуючи зазначену проблему, належний захист отриманої інформації в системах відеоспостереження майже не здійснюється, а відтак ризику неправомірного доступу, обробки та розпорядження такими даними значно зростають.

Окрім того, законодавством чітко не визначено, як довго мають зберігатися такі відеозаписи в системах, внаслідок чого, згідно з даними Звіту, строки зберігання записаної на відео інформації залежать від обсягу пам'яті накопичувачів. Тобто, найстаріші відеозаписи видаляються лише тоді, коли закінчується місце на тому чи іншому накопичувачі, що призводить до виникнення «мінливих» строків зберігання, оскільки записані за одиницю часу обсяги відеофайлів не є сталими і залежать від освітлення, динаміки подій, пори року і виходу з ладу окремих відеокамер тощо [5].

А що ж з головною метою застосування СРО – використання отриманих відеозаписів як доказів у рамках кримінального провадження? З аналізу судових рішень, розміщених в Єдиному реєстрі

судових рішень, вбачається, що у разі долучення до матеріалів справи відеозаписів з відеокамер, обладнаних СРО, як доказів, суди визнають їх належними та допустимими і в подальшому керуються ними для постановлення вироків у справах. З означеним не можна погодитися з огляду на те, що, як зазначено вище, застосування СРО органами місцевої влади не має законодавчих підстав, а відтак вся інформація, отримана у такий спосіб, не може бути такою, що отримана в межах і у спосіб, передбачений законом. Окрім того, всі інші докази, здобуті на основі інформації, отриманої не в законний спосіб, будуть визнані також недопустимими, відповідно до концепції «плодів отруйного дерева».

Варто зазначити, що в Україні вже були спроби законодавчого врегулювання застосування відеокамер, обладнаних СРО. Зокрема, у 2019 році на розгляд Верховної Ради України вносився проект Закону «Про внесення змін до деяких законодавчих актів України щодо систем моніторингу стану безпеки», відповідно до якого доступ до інформації (даних) комплексів безпеки в межах своєї компетенції мали б сили безпеки, органи державної влади та місцевого самоврядування, крім результатів ідентифікації (розпізнавання) номерних знаків транспортних засобів та облич осіб, доступ до яких надавався виключно силам безпеки [6]. Однак в подальшому законопроект було відкликано.

У той час як в Україні, під гаслом підтримки безпеки та забезпечення правопорядку у суспільстві лише впроваджуються СРО, Європейський Союз закликав утриматися від використання СРО в громадських місцях органами поліцейського правопорядку, а також збереження у відповідних базах біометричної інформації, отриманої за допомогою таких СРО, з метою запобігання зловживанням ними силовими структурами, захисту фундаментальних прав людей на гідність, приватність, свободу пересування, нівелювання потенційних ризиків дискримінації тощо [7].

Підсумовуючи, слід зазначити, що застосування СРО в Україні наразі порушує всі існуючі законодавчі норми. Комплексне правове регулювання вказаної сфери наразі відсутнє, не існує єдиного підходу до застосування таких систем та контролю використання

отриманої за їх допомогою інформації, а відтак фактично всі системи відеоспостереження перебувають поза законодавчою площиною регулювання, не гарантуючи безпеку, а навпаки, знищуючи її.

Відтак, Україна має два шляхи розв'язання описаної проблеми, зокрема або використати досвід Європейського Союзу, відмовившись від використання СРО в громадських місцях та зберігання отриманої за їх допомогою інформації, або ж комплексно врегулювати вказану сферу в законодавчій площині, зокрема:

- розробити та деталізувати законодавче підґрунтя функціонування СРО з урахуванням міжнародного досвіду та практики ЄСПЛ;
- передбачити в Законі України «Про захист персональних даних» або у проєкті його нової редакції, робота над яким зараз ведеться, що зображення обличчя особи є її «чутливими» персональними даними;
- запобігти можливим ризикам, пов'язаним із зловживанням отриманою інформацією державними структурами, зокрема шляхом здійснення парламентського контролю вказаної сфери;
- запобігти використанню отриманої за допомогою СРО інформації як доказів у кримінальному судочинстві до моменту законодавчого врегулювання вказаної сфери та встановлення прямої вказівки на можливість застосування таких систем як належних та допустимих доказів у законодавстві;
- всіляко інформувати населення про використання відеокамер з функціями СРО, зокрема шляхом розміщення відповідних інформаційних повідомлень та таблиць, запуску онлайн-карти місць розташування таких відеокамер тощо.

Список використаної літератури

1. Чи легально встановлювати на міських вулицях камери із системою розпізнавання облич? // Аналітика Центру демократії та верховенства права [Веб-сайт]. URL: <https://cedem.org.ua/analytics/kamery-rozpiznavannya-oblych/>;

2. Конституція України: Закон України від 28.06.1996 р. № 254к/96-ВР (зі змінами та доповненнями) // Голос України, 13.07.1996 р. № 128;
3. Цивільний кодекс України: Закон України № 435-IV від 16.01.2003 // Голос України, 12.03.2003 р. № 45;
4. Про захист персональних даних: Закон України № 2297-VI від 01.06.2010 (зі змінами і доповненнями) // Урядовий кур'єр, 07.07.2010 р. № 122;
5. (Майже) Старший Брат стежить за тобою: відеоспостереження за дотриманням публічного порядку в Україні. Звіт. // Упор. М. Каменєв та С. Золотар. – К.: Асоціація УМДПЛ, 2019. 76 с.
6. Про внесення змін до деяких законодавчих актів України щодо систем моніторингу стану безпеки: Проект Закону №10120 від 01.03.2019. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65607;
7. Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters: European Parliament Report №2020/2016(INI). URL: https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html.

Зайцева А. В.

студентка Дніпропетровського
державного університету внутрішніх
справ

Науковий керівник: Алексєєнко І. В.

доктор політичних наук, професор,
завідувач кафедри міжнародних
відносин Дніпропетровського
державного університету внутрішніх
справ

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ ОСІБ У КОНТЕКСТІ ПРАВ ЛЮДИНИ НА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Створення умов при яких кожна людина буде відчувати себе в безпеці у всіх часи було головною ціллю у всіх напрямках діяльності держави. Більш того, необхідність держави існувати також

безпосередньо проявляється через людську потребу бути захищеною. Відсутність особистої безпеки людини можна прирівняти к відсутності будь-якого зв'язку між людськими зусиллями та досяганням цілей. І, як виявилось, саме через це громадяни згодні терпіти часткові обмеження своїх прав і свобод від спеціалізованих органів державної влади, які, на думку народу, мають усе необхідні інструменти встановлення правопорядку в своїх руках, щоб забезпечити безпеку людини.

Особливо важливим питання безпеки особистості постає в контексті впровадження новітніх технологій. Застосування відеокамер наразі прослідковується всюди : в торговельних центрах, супермаркетах, в деяких закладах освітнього процесу і навіть просто на вулиці та дорогах. Такі системи встановлюють у деяких об'єктах транспортної інфраструктури (в аеропортах, на станціях метро) з метою забезпечення транспортної безпеки. Але, не потрібно забувати, що застосування новітніх систем відеоспостереження служить не лише ефективним засобом профілактики правопорушень, а й дієвим інструментом їхнього розслідування. Більш того, програмні забезпечення настільки оновили, що, при зйомці відбувається аналіз даного потоку до якого приєднується нова технологія розпізнавання особи, нібито маючи на меті контроль положення та порушника було впізнано одразу. Як зазначають дослідники, структурна система має бути побудована таким чином, щоб при фіксації особи, підданої даному виду адміністративної покарання, воно відразу ж було затримано.

Щодо законодавчої сторони цього питання, на сьогодні будь-яке спеціальне правове регулювання використання даних технологій відсутнє, тож громадянам потрібно керуватись законом України «Про захист персональних даних». Згідно даному закону «персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована»[3]. Інформація щодо фізичних осіб, яка зібрана у результаті відеоспостереження із системою розпізнавання осіб, виступають персональними, оскільки вони характеризують фізіологічні та біологічні особливості людини. [1]

Багато дослідників вивчаючи дану тематику наголосили, що обробка даних про особу можлива лише при наявності згоди суб'єкта на сканування своєї особи, при чому дана згода повинна бути лише у письмовому варіанті. Так згідно із ст. 6 ЗУ «Про захист персональних даних», маємо: «Не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини»[3]. А також згідно із ст.8 про права суб'єкта персональних даних ЗУ «Про захист персональних даних»: «Суб'єкт має право пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних».[3]

Можна зазначити, що такі технології вищими органами можуть також бути використаними за власними цілями, наприклад вони можуть зловживати спостереженням та виявленням осіб які збираються на протестах, мітингах чи представників інших громад. На наш погляд, такий захід є надмірним, тому що повністю виключає можливість застосування досягнень цифровізації для зниження рівня злочинності. Проте для забезпечення компромісу між бажанням громадян захистити своє приватне життя, унеможливити мимовільне втручання в нього та необхідність забезпечення безпеки слід чітко регламентувати процедуру внесення особи до бази даних злочинців та суворо визначити коло тих суб'єктів, які можуть мати доступ до такої бази.[2]

Підсумовуючи вище наведене, можна відзначити, що технологія розпізнавання осіб може мати успіх якщо її використовувати із ціллю зниження рівню злочинності. Але разом із цим є і великий ризик на втручання в приватне життя громадян держави із вірогідністю їх подальшого оголошення, але потрібно пам'ятати, що згідно із Законом про Інформацію ст.301 «Фізична особа сама визначає своє особисте життя і можливість ознайомлення з ним інших осіб».

Саме тому з метою найбільш ефективної реалізації програм впровадження відеоспостереження слід законодавчо закріпити порядок роботи з базою даних, суб'єктний склад осіб, які мають

до неї доступ та відповідальність за порушення цього порядку. Крім того, ефективним методом підвищення довіри громадян до системи розпізнавання осіб буде розробка програм освіти у сфері персональних даних. Доведення до широких верств населення у доступному форматі способів їх захисту у разі неправомірного втручання у приватне життя.

Список використаних джерел:

1. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. *Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник*. К.: К. І.С., 2015. 220 с.
2. Васильєв А. А., Мухопад В. А. *Штучний інтелект: юридичний аналіз. Проблеми правового та технічного захисту інформації*. 2018. 6 Вип.
3. *Про захист персональних даних*: Закон України за станом на 1 черв. 2010 р. Верховна Рада України. Київ: Парлам. Вид-во, 2010.
4. *Про інформацію*: Закон України за станом на 22 груд. 2005 р. Верховна Рада України. Київ: Парлам. Вид-во, 2005.

Максаков О. Ю.

здобувач першого (бакалаврського)
рівня вищої освіти
Дніпропетровського державного
університету внутрішніх справ

Алексєєнко І. В.

доктор політичних наук, професор,
завідувач кафедрою міжнародних
відносин Дніпропетровського
державного університету внутрішніх
справ

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

В даний час з розвитком інформаційного суспільства ідентифікувати особистість конкретної людини не важко, ідентифікува-

ти його за індивідуальними (персональними) ознаками. Особисті дані фізичної особи необхідно захищати від третіх осіб внаслідок збільшення зростання крадіжок персональної інформації, оскільки опинившись у руках правопорушника, такі дані перетворюються на персональну зброю проти особи. Кожна людина хоч раз, але стикалася з тим, що їй на мобільний (міський) телефон дзвонила компанія, раніше з якою у людини не було взаємин (листа на електронну пошту тощо) із пропозицією, все це свідчить про те, що клієнтська база даних, що містить персональні дані, була незаконно передана третім особам.

Розглянемо найпоширеніші випадки та заходи їх припинення:

1. Публікація особистих даних фізичної особи без її письмової чи усної згоди на неї: передбачено адміністративну відповідальність з накладенням штрафу на особу, яка їх опублікувала. [1]

2. Оголошення інформації про приватне життя без згоди на це фізичної особи, поширення цих відомостей у публічних виступах: за зазначені дії передбачено кримінальну відповідальність.

3. Зламування облікових записів електронної пошти чи соціальних мереж: даний вид правопорушення визначається як порушення таємниці листування, при вчиненні якого передбачена кримінальна відповідальність.

У судовому порядку притягнення володільця або розпорядника персональних даних до адміністративної відповідальності можливе за ст. 188-39 Кодексу України про адміністративні правопорушення (далі — *КУпАП*). До того ж, за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконну зміну такої інформації (крім випадків, передбачених іншими статтями Кримінального кодексу України) особу може бути притягнуто до кримінальної відповідальності за ст. 182 Кримінального кодексу України. [2]

На сьогоднішній день існує ціла низка заходів, що сприяють уникненню «витікання» інформації. По-перше, необхідно вивчити закони, що регулюють доступ до персональних даних, визначити, хто має право використовувати, обробляти і передавати особисті відомості. По-друге, уникати організації сумнівного походження,

кожна компанія має захищати зібрану інформацію від модифікації та розголошення. По-третє, щоб захистити дані, що містяться в соціальних мережах та електронній пошті, необхідно використовувати двофакторну автентифікацію, захищене з'єднання мережі, а також нікому не передавати логіни та паролі від облікових записів.

Список використаної літератури:

1. Гуйван П. Д. Правові засади захисту персональних даних. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2018. Вип. 51(1) URL: [http://nbuv.gov.ua/UJRN/nvuzhpr_2018_51\(1\)__20](http://nbuv.gov.ua/UJRN/nvuzhpr_2018_51(1)__20) (дата звернення 25.11.2021)
2. Гронь О. В., Погореленко А. К. Проблеми захисту персональних даних у контексті сучасної комунікації. *Науковий вісник Ужгородського національного університету. Серія : Міжнародні економічні відносини та світове господарство*. 2018. Вип. 19(1) URL: [http://nbuv.gov.ua/UJRN/Nvuumevcg_2018_19\(1\)__25](http://nbuv.gov.ua/UJRN/Nvuumevcg_2018_19(1)__25) (дата звернення 25.11.2021)

Павлік О. О.

студентка Дніпропетровського
державного університету внутрішніх
справ

Науковий керівник: Алексєєнко І. В.

доктор політичних наук, професор,
завідувач кафедри міжнародних
відносин Дніпропетровського
державного університету внутрішніх
справ

ПЕРСОНАЛЬНІ ДАНІ В МЕРЕЖІ ІНТЕРНЕТ ЧЕРЕЗ ПРИЗМУ ПРАВОВОГО ЗАХИСТУ ТА РЕГУЛЮВАННЯ

Скандали з витоком персональних даних йдуть один за одним. Багато хто впевнений, що зловмисники в мережі Інтернет «полю-

ють» виключно за даними багатих і знаменитих. Але це не так. Інформація про людину, її персональні дані сьогодні перетворилися на дорогий товар, який використовується по-різному: хтось використовує ці дані для того, щоб за допомогою реклами продати вам якусь річ, комусь ви просто не подобаетесь, і в Інтернеті вас можуть намагатися образити, очорнити, виставити вас у поганому світлі, створити погану репутацію та зробити вигнанцем суспільства, за допомогою ваших персональних даних шахраї, злодії, можуть вкрати ваші гроші, шантажувати вас і змушувати робити якісь дії і багато іншого. Персональні дані звичайних користувачів, потрапляючи до рук шахраїв, дозволяють їм отримувати неправомірну вигоду.

Актуальність обраної теми полягає в тому, що в сучасних умовах основна частка атак зловмисників здійснюється крізь комп'ютерні мережі, щораз ускладнюється їх організація, стрімко збільшується чисельність комп'ютерів та мережевого обладнання. Охорона інформації є складовою частиною гарантування національної безпеки будь-якої держави і забезпечується правовими, організаційними, програмними та інженерно-технічними заходами.

Будь-яка інформація може бути персональними даними за умови, що вона стосується особи. Термін «персональні дані» включають інформацію про приватне та сімейне життя особи, але також охоплюють інформацію про діяльність, звички та спосіб життя, як-от робочі відносини або економічна чи соціальна поведінка індивіда.

Визначення персональних даних у пункті 8 статті 2 Закону визначає персональні дані як інформацію або групу відомостей, які можуть бути ідентифіковані або можуть бути конкретно ідентифіковані. Проте українське законодавство не встановлює і не може встановити чіткий перелік інформації про персональні дані з метою застосування законодавчих положень до різних ситуацій, у тому числі щодо обробки персональних даних та файлів персональних даних в інформаційній (автоматичній) базі даних. Це може статися в майбутньому через зміни в техніці, суспільстві, економіці та інших сферах суспільного життя.

Конфіденційність можна розглядати як явище, що означає звички та практику конфіденційності, або її можна розглядати як право. Явище рідко визначається чітко, тоді як права зазвичай чітко встановлені. Щоб забезпечити юридичну визначеність, чітко необхідне формулювання приватності як права. Один із способів поглянути на це – це побачити конфіденційність як цінність, яка потребує захисту, що в свою чергу відбувається за допомогою правових інструментів. Потім закон визначає, на які права та захист має кожен з нас. Конфіденційність – це глобальне занепокоєння. Майже кожна нація має пряме або непряме законодавство або правила, які захищають конфіденційність, як правило, закріплені в конституції.

В Україні є ряд законодавчих актів, які гарантують право людини на захист даних. До таких відносять: Витяг з Кримінального кодексу України (стаття 182 «Порушення недоторканності приватного життя»), Конституція України (стаття 32), Типовий порядок обробки персональних даних, затверджений Наказом Уповноваженого Верховної Ради України з прав людини «Про затвердження документів у сфері захисту персональних даних» від 08.01.2014 № 1/02-14, Витяг з Кодексу України про адміністративні правопорушення (стаття 188-39 «Порушення законодавства у сфері захисту персональних даних», стаття 188-40 «Невиконання законних вимог Уповноваженого Верховної Ради України з прав людини»).

У 2015 році був прийнятий Закон України «Про Національну поліцію», який передбачає повноваження поліції в безпрецедентному масштабі формувати і використовувати інформаційні ресурси (бази даних), зокрема, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України. Також поліція може створювати власні бази даних і має безпосередній оперативний доступ до інформації та інформаційних ресурсів інших органів державної влади. Сучасні інформаційні технології та законодавство відкривають можливості для правоохоронних органів обробляти величезний обсяг персональних даних. Проте, з огляду на численні переваги цих технологій, слід визнати, що при несанк-

ціонованому їх використанні (без дотримання вимог закону), це може призвести до серйозних наслідків. Повна відсутність прозорого управління у сфері захисту персональних даних в діяльності Національної поліції (забезпечення максимального інформування суб'єктів персональних даних про правові підстави, способи, мету обробки, строки зберігання та знищення персональних даних поліцейськими службами) привертає все більше уваги до проблем у даній сфері.[1]

В Україні функцію зі захисту персональних даних покладено на Уповноваженого Верховної Ради України з прав людини або просто – Омбудсмена. У структурі Секретаріату Уповноваженого Верховної Ради України з прав людини було створено окремий Департамент у сфері захисту персональних даних.

Основними завданнями цього відділу є: забезпечення виконання законодавчих вимог повноважень парламенту щодо нагляду за дотриманням прав людини і громадянина та вимог законодавства у сфері захисту персональних даних, застосування законодавства про захист персональних даних, та роз'яснення прав та обов'язків відповідних суб'єктів Здійснюється в межах нагляду та юридичного супроводу, організовує та бере участь у типових проектних роботах, обробці, правовій експертизі проектних нормативно-правових актів, організації та національних установ, незалежно від їх форми власності та їх посадовими і службовими особами з питань нормопроєктувальної роботи ,здійснення моніторингу стану дотримання прав людини і громадянина у сфері захисту персональних даних.[2]

В українських реаліях проблема починається з домовленості. Щодо сайту, то не всі попередили про збір інформації. Ви можете не отримувати жодних сповіщень про використання файлів cookie, і тоді ви побачите їх у налаштуваннях свого браузера. Крім того, не всі вважають, що сторінки сайту можуть містити елементи інших сайтів (реклама, соціальні мережі) і що кожен з них також збирає файли cookie. Користувачі не завжди знають. Крім того, мобільні додатки не завжди попереджають їх про те, які дані вони збирають. Наприклад, для багатьох користувачів додатку Facebook

стало новиною, що додаток збирав інформацію про їх дзвінки та смс повідомлення [3].

На жаль, реальність така, що люди видають занадто багато інформації про себе в Інтернеті, відчуючи при цьому помилкове переконання, що інформація, що їм належить, є конфіденційною, але як тільки інформація потрапляє в мережу, контролювати її подальше використання вже практично неможливо. Хто, коли і з якою метою може скористатися такими даними, прогнозувати неможливо.

Список використаних джерел:

1. Департамент з питань захисту персональних даних – Ombudsman. Уповноважений Верховної Ради України з прав людини. URL: <https://www.ombudsman.gov.ua/ua/page/zpd/info/> (дата звернення: 25.11.2021).

2. Захист персональних даних в діяльності Національної поліції України. Експертний Центр з Прав Людини. URL: <https://ecpl.com.ua/comments/zahyst-personalnyh-danyh-v-diyalnosti-natsionalnoji-politsiji-ukrajiny/> (дата звернення: 25.11.2021).

3. Персональні дані онлайн: проблеми регулювання та перспективи захисту. Реанімаційний Пакет Реформ. URL: <https://rpr.org.ua/news/personal-ni-dani-onlayn-problemy-rehuliuвання-ta-perspektyvy-zakhystu/> (дата звернення: 25.11.2021).

Павлюк А. Ю.

студент Чернівецького національного
університету ім. Ю. Федьковича

Науковий керівник: Заморська Л. І.

доктор юридичних наук, доцент
кафедри теорії права та прав людини
Чернівецького національного
університету ім. Ю. Федьковича

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ

В умовах розвитку сучасного суспільства необхідним є забезпечення надійного, законодавчо визначеного захисту інформації про особу. Прогрес у галузі цифрових технологій, зокрема у сфері розробки та впровадження програмного забезпечення, активність у формуванні баз персональних даних надзвичайно загострили проблему захисту приватного життя фізичних осіб та наклала суттєві обмеження основних прав і свобод людини. У ході дослідження дістали подальший розвиток положення про баланс між правовим регулюванням відносин із захисту відомостей про громадянина та національною кібербезпекою держави. Важливо розглянути окремі правові заходи для обмеження довільного поводження з правами людини в інформаційній сфері.

Питання вдосконалення нормативно-правової бази у сфері захисту персональних даних ставало об'єктом дослідження багатьох вітчизняних і зарубіжних вчених, експертів міжнародних організацій тощо. Сьогодні жваво обговорюються проблеми впровадження всесвітніх міжнародних та європейських стандартів щодо захисту персональних даних у національне законодавство у засобах масової інформації, де свої погляди висловлюють міністри, представники владних структур, провідні політологи, правознавці інші спеціалісти з цього питання. Вагомий внесок у розв'язання цього питання належить таким фахівцям у галузі правничої науки, як О. Волков [1], Н. Докучаєва [2], Д. Павленко [5], Т. Обуховська [4] та ін.

Інститут недоторканності особистого життя людини почав розглядатися як обов'язковий фактор розбудови демократичного суспільства в 1928 р., коли суддя Верховного суду США Л. Брандейс офіційно заявив про наявність у Конституції США «права бути залишеним у спокої». Приватність – це можливість особи або групи осіб відокремити себе, інформацію про себе, і, таким чином, виявляти свою особистість вибірково. [4, с. 99]

На нашу думку, сьогодні сучасні тенденції розвитку комп'ютерних технологій та обробки персональних даних диктують необхідність у подальшому розвитку більш детального регулювання цього права. Зокрема, важливим є виокремлення таких основних складових права на інформаційну приватність:

- право на анонімність;
- право контролювати інформацію про себе;
- право «бути забутим» [6, с. 13].

На жаль, зміни, зумовлені поширенням коронавірусної інфекції COVID-19, відбулися в усіх сферах суспільного життя. Проте, найсуперечливішою стала проблема масового інформаційно-психологічного впливу на людину, суспільство та міжнародну спільноту, що виникала в умовах запровадження у більшості країн світу надзвичайної ситуації, пов'язаною з пандемією. [6, с. 16]

У зв'язку з визнанням міжнародною спільнотою доцільності створення інтернаціональної системи правового регулювання обробки і передавання даних міжнародні організації почали наголошувати на необхідності розроблення комплексу базових принципів захисту приватного життя та індивідуальних свобод у зв'язку з обробкою персональних даних і їх транскордонними потоками.

Наприклад, експерти Організації з економічного співробітництва і розвитку (далі – ОЕСР) зауважують, що для забезпечення безпеки глобального обміну персональними даними, держави – члени на національному рівні, мають:

- прийняти належні національні закони;
- заохочувати і підтримувати саморегулювання шляхом прийняття кодексів поведінки/поводження або інших правил;

- забезпечити наявність розумних механізмів реалізації індивідуальних прав;
- застосувати необхідні санкції та інші засоби захисту персональних даних на випадок невиконання заходів, що передбачені зазначеними принципами;
- забезпечити недискримінаційне ставлення до суб'єктів даних. [4, с. 96]

У країнах ЄС подальший пошук балансу між захистом приватності та потребою у безпеці розглядається через правову категорію «охорони приватних персональних даних», що передбачає забезпечення конфіденційності відомостей про особу. Згідно з конвенцією № 108 Ради Європи збирання, накопичення, зберігання і поширення персональних даних може здійснюватися лише з дозволу особи, дані про яку обробляються. Однак, допускається обмеження в інформаційних правах фізичних осіб. До прикладу, якщо це стосується:

- державної чи суспільної безпеки;
- фінансової стабільності;
- боротьби зі злочинністю;
- захисту прав та основних свобод інших осіб. [3]

На наш погляд, правове забезпечення суспільних відносин щодо захисту персональних даних має забезпечувати загальні умови для законності їх обробки, регулювання діяльності суб'єктів у сфері цифрових технологій. Згідно з Законом України «Про захист персональних даних» завданнями національного законодавства є створення правової бази державного регулювання суспільних відносин людини, суспільства і держави за умов дієвого захисту громадянських прав у сфері персональних даних. [7]

Крім того, згідно чинного законодавства та Доктрини інформаційної безпеки України ключовими ознаками інформаційної безпеки є:

- 1) конфіденційність – стан поводження з інформацією, при якому доступ до неї отримують тільки суб'єкти, які мають на це право;
- 2) цілісність – запобігання несанкціонованій або незаконній модифікації інформації;

3) доступність – запобігання тимчасовому або постійному приховуванню інформації від користувачів, які мають право на доступ.

Без сумніву, в сучасних умовах поширення інформаційно-комунікаційних систем і мереж забезпечення інформаційної приватності дедалі більше ускладнюється. Будь-які відомості або дані про людину можуть бути отримані завдяки Інтернет-ресурсам та використані не лише на її користь, а також у протиправних цілях:

- маніпулювання свідомістю;
- шантажу;
- залякування;
- агресивної реклами;
- інформаційного насилля. [6, с. 12]

На жаль, на сьогодні правове забезпечення суспільних відносин в Україні щодо персональних даних у частині їх правового захисту є недостатнім. Останні події, пов'язані з масовим витоком персональних даних громадян України через інформаційно-комунікаційні мережі підтверджують актуальність цієї проблеми і нагальну необхідність внесення змін до законів України «Про інформацію» [8], «Про захист персональних даних» [7] та Кримінального кодексу України. Вони закріплюють лише загальні принципи доступу громадян до інформації, що стосується їх особисто. Механізм реалізації зазначеного права належним чином не визначений. Відсутнє й регулювання використання конфіденційної інформації про особу.

Т. Обуховська стверджує, що вдосконалення нормативно-правової бази України у галузі забезпечення обробки та циркуляції персональних даних, має відбуватися, насамперед, шляхом систематизації, конкретизації, деталізації та доповнення необхідними документами. [4, с. 97]

Таким чином, на основі сказаного вище, при дослідженні спрямованості та ефективності механізму захисту персональних даних в умовах використання цифрових технологій, безумовно, враховувалися причини, вплив інтенсивного розвитку інформаційних технологій та глобальні соціально-правові процеси. На основі ін-

формації, зібраної з відкритих джерел, можна зробити висновок, що необхідне приведення національного законодавства кожної держави у відповідність з міжнародними орієнтирами та врахування основних принципів щодо організації заходів із контролю за виконанням законодавства в цій галузі з метою забезпечення ефективного захисту відомостей про особу.

Список літератури:

1. Волков А. Защита персональных данных: пригодится ли нам британский опыт? [Електронний ресурс] : А. Волков, Е. Царев. – Режим доступу : <http://www.ispdn.ru/publications/7312/>
2. Докучаева Н. Феномен украинской визитницы или защита персональных данных по-украински [Електронний ресурс] / Н. Докучаева. – Режим доступу : <http://pravotoday.in.ua/ru/press-centre/publications/pub-190/>
3. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних [Електронний ресурс] : Конвенція Ради Європи № 108 від 28 січ. 1981 р. – Режим доступу : http://zakon1.rada.gov.ua/laws/show/994_326
4. Обуховська Т. І. Захист персональних даних в умовах розвитку інформаційного суспільства / Т. І. Обуховська. // Соціальна і гуманітарна політика. – 2014. – №1. – С. 95–101.
5. Павленко Д. Як захистити персональні дані [Електронний ресурс] / Д. Павленко. – Режим доступу : <http://www.epravda.com.ua/columns/2011/09/30/300156/>
6. Пилипчук В. Г. Проблеми захисту приватності, прав і безпеки людини в сучасних умовах цифрових трансформацій / В. Г. Пилипчук. – 2020. – №2. – С. 11–17.
7. Про захист персональних даних [Електронний ресурс] : Закон України № 2297-VI від 1 черв. 2010 р. – Режим доступу : <http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2297-17>
8. Про інформацію [Електронний ресурс] : Закон України № 2658-XII від 02.10.92 – Режим доступу : <https://zakon.rada.gov.ua/laws/show/2657-12#Text/>

Радченко К. В.

магістр міжнародних економічних
відносин та права, аспірант Інституту
економіки промисловості НАН
України

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ МІСЦЕВОГО САМОВРЯДУВАННЯ: ДОСВІД МІСТА БРІСТОЛЬ, ВЕЛИКОБРИТАНІЯ

Право на захист персональних даних (ПД) є складовою фундаментального права на приватність, що визначається статтею 8 Європейської Конвенції про Захист Прав Людини і Основоположних Свобод. [9] Статтею 2 Конвенції 108 Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 р. визначено термін «персональні дані», як будь-яку інформацію, що стосується конкретно визначеної особи або особи, що може бути конкретно визначеною. [3] У Резолюції ПАРЄ 1653 (2009) [5], органи місцевого самоврядування розглядаються, як ключові актори ініціювання, впровадження та тестування процедур захисту ПД. Діджиталізація, концепція електронної демократії, смарт трансформація міст та регіонів призводять до зростання кількості та масштабу викликів для місцевих та регіональних влад, зокрема у сфері захисту ПД, що потребує вивчення та систематизації кращих практик, пошуку нових рішень та стратегій. Згідно з дослідженням 2017 року, органи місцевого врядування Великобританії (ВБ) зазнали 98 мільйонів кібератак протягом п'яти років, а щомісяця існує близько 37 спроб деструктивних впливів. У той же час завдяки оперативній протидії таким загрозам, ВБ досягла максимального 100% результату станом на 2019-2020 роки у рейтингу «кібер-успішності» країн світу. [7] Підходи міста Брістоль є особливо цікавими, адже його визнано лідером серед «розумних» та відкритих міст ВБ (smart city). [1] Однак, це не означає відсутність недоліків та слабких місць системи захисту ПД міста, що також еволюціонує та не є досконалою.



Рис. 1 Структура Регулювання ПД у місті Брістоль (складено автором)

Система правового регулювання ПД Брістолю включає: 1) **загальнонаціональний рівень**; 2) **акти локальної дії**, а також **проектні ініціативи**; 3) **міжнародні договори, акти м'якого права Ради Європи, право ЄС** (прийняте до 31 січня 2020 року та яке не втрачає чинності внаслідок Брекзиту).

Загальний регламент про захист персональних даних (GDPR), до якого на той час Великобританія приєдналася як країна-член ЄС, було відображено у Законі із Захисту Даних 2018 (Data Protection Act 2018) [8]. На момент написання матеріалу та аналізу змін після Брекзиту, GDPR та “добрекзितне законодавство” у сфері ПД не втратило сили. GDPR передбачає значні штрафи за невиконання положень регламенту з боку Офісу уповноваженого з інформації. Заходи із забезпечення належного рівня безпеки в процесі обробки ПД міською радою Брістоля включають, але не обмежуються наступними: (а) **контроль входу**, (б) **захищені офісні столи, шафи, тощо з сейфами чи шухлядами, що замикаються**, (с) **способи утилізації**, (d) **обладнання**, (е) **посібник з інформаційної безпеки**, (f) **навчання та тренінги**. Для Брістоля характерною є координація зусиль державних та приватних акторів. Доцільно виділити

п'ять основних одночасних кроків, що були здійснені для приведення діяльності міської ради Брістоля до стандартів GDPR: 1) призначення **Офіцера із захисту даних (DPO)** в структурі міської адміністрації; 2) **впровадження комплексної системи обробки ПД** з урахуванням трьох факторів: мети, аналізу альтернативних сценаріїв, невідворотності обробки; 3) **інтенціональна конфіденційність та конфіденційність за замовчуванням** (основні принципи: **спеціалізація мети, обмеження збору, мінімізація даних**); 4) **відомчий аналіз**; 5) **забезпечення надійності постачальників**.

Загрози чи порушення в сфері ПД повністю виключити неможливо. У критичних ситуаціях постає питання раціонального реагування міською адміністрацією на виклики, зокрема, наприклад, повідомлення суб'єкта ПД про будь-які ризики і наслідки обробки його даних. Проблемними питаннями є також соціальний моніторинг громадян (citizen scoring), алгоритмізація прийняття рішень. У контексті звернень до ЄСПЛ (зокрема, справа Big Brother Watch and Others v. the United Kingdom), Конгрес місцевих та регіональних влад Ради Європи висловив занепокоєння та акцентував увагу на необхідності пошуку нових шляхів захисту ПД. [2] Окрім того, використання камер cctv, що набуває все більшого поширення з огляду на вуличну безпеку, також стосується опрацювання великого масиву ПД та потребує особливих заходів безпеки. Щодо цього місцева адміністрація розробила окремий детальний посібник з безпеки ПД, отриманих з камер. [1] Тобто, відбувається диверсифікація підходів щодо опрацювання даних, отриманих з різних джерел, у рамках уточнення GDPR та розробки специфічних рекомендацій.

У якості висновків, для систематизації результатів дослідження, автором було проведено SWOT-аналіз системи обробки та захисту персональних даних. Було виявлено особливості, що представлені у таблиці 1. Загалом, перевірка надійності процесів обробки ПД, впроваджена на всіх рівнях, дозволяє міській раді Брістоля суттєво мінімізувати потенційні ризики зовнішнього се-

редовища, у тому числі, ризик перманентних кіберзагроз. Комплексний характер вживаних заходів безпеки дозволяє зробити висновок також про системність, інклюзивність та ефективність їхнього впровадження.

Сильні Сторони • Послідовність впровадження GDPR • Стабільна та дієва Система Система Захисту ще до впровадження стандартів GDPR • Інклюзивний Людиноцентричний підхід • Транспарентність та високий рівень due diligence співробітників місцевої адміністрації • Високі стандарти та постійний моніторинг, як з боку зовнішніх структур, зокрема, National Archives, так і структурними департаментах ради • Системне навчання з кібер-безпеки та захисту ПД • Комплементарність засобів безпеки та способів обробки даних (традиційні методи неавтоматизованої обробки знаходяться в полі рівнозначної уваги в контексті ризик-менеджменту, як і дані, отримані з новітніх джерел, зокрема записи камер, тощо) • Розробка цільових внутрішніх стандартів, посібників з захисту ПД • Система інформування у разі порушень чи зловживань щодо ПД • Проведення консультацій з громадянами з питань, що стосуються впровадження ризикованих (з потенціалом загрози ПД) технологій	Слабкі Сторони • Відсутність окремого спеціального «координуючого департаменту» з ризик менеджменту, захист персональних даних виконується всіма департаментами одночасно, повноваження DPO реалізуються ситуативно, тоді, як не вистачає централізованої координації перетворень • Відсутність Єдиного Електронного Реєстру Даних по запитах громадян, що надійшли депутатам та відповідам на них • Зменшення рівня довіри громадян до міської ради через випадки несанкціонованого поводження з даними
Загрози • Справи проти ВБ щодо впровадження систем профілювання громадян (citizen scoring) можуть мати негативний репутаційний вплив на міську раду Брістоля • Вихід Британії з ЄС може мати низку непередбачуваних правових змін на національному рівні, що може поставити під загрозу застосування регламенту GDPR та призведе до переосмислення наявної системи діяльності місцевої Ради Брістоля • Велика кількість кібер-атак на міську раду, постійна зміна каналів впливу кібер-хакерами, високий рівень невизначеності	Можливості • Використання Профілювання за впровадження ефективного захисту ПД не тільки збільшить довіру громадян, але і підвищить якість місцевого врядування, краще розуміючи та задовольняючи потреби громадян • Брістоль, як лідер серед розумних міст на базі розроблених стандартів може слугувати бенч-маркінг прикладом ефективного захисту ПД на місцевому та регіональному рівні для інших країн Ради Європи • Тестування новітніх моделей з захисту ПД на базі наявного розвиненого інституційного поля міської ради

Табл. 1 SWOT-Аналіз Системи Регулювання Захисту ПД у Брістолі (Складено автором)

Питання спостереження та витоку даних є суттєвим викликом, що може призводити до зниження довіри, тому автором рекомендовано створення **департаменту з ризик менеджменту та протидії кіберзагрозам** в структурі міської ради Брістоля, що дозволило б більш ефективно координувати заходи щодо ПД вжиті іншими департаментами. Як смарт місто, Брістоль може виступати площиною апробації різноманітних стратегій та підходів з захисту ПД. Доречно також розширити фокус цього дослідження у порівняльно-правовому аспекті, порівнявши підходи Брістоля з підходами інших міст ВБ для глибшого розуміння особливостей локального рівня системи правового захисту ПД та адаптації загальнонаціональних орієнтирів.

Список використаних джерел

1. Bristol City Council website. [Електронний ресурс] / Bristol City Council – Режим доступу: <https://www.bristol.gov.uk>.
2. Congress of Local and Regional Authorities of the Council of Europe. Debates in the Chamber of Local Authorities 37th SESSION Strasbourg, 29-31 October 2019 CPL37(2019)03 [Електронний ресурс] – Режим доступу: https://search.coe.int/congress/Pages/result_details.aspx?ObjectId=0900001680986119.
3. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Amendment to Convention ETS No. 108 allowing the European Communities to accede. – Strasbourg, 28.1.1981. – (Article 5 – Quality of data). – Режим доступу : <http://www.convention.coe.int/treaty/en/Treaties/Html/108.htm>
4. Guidelines on the protection of personal data processed by mobile applications provided by European Union institutions, 7 November 2016.
5. Parliamentary Assembly. Resolution 1653 (2009) Electronic Democracy [Електронний ресурс] / Parliamentary Assembly – Режим доступу до ресурсу: <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=17715&lang=en>.
6. The UK Data Protection Act 2018 [Електронний ресурс] – Режим доступу до ресурсу: <http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>.
7. UK National Cybersecurity Index [Електронний ресурс] – Режим доступу до ресурсу: <https://ncsi.ega.ee/country/gb/?pdfReport=1>.

8. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних (Загальний регламент про захист даних) [Електронний ресурс] // 2016 – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/file/text/63/f474904n8.pdf>

9. Конвенція о защите прав человека и основных свобод [Електронний ресурс]. – 1950. – Режим доступу до ресурсу: <https://www.coe.int/tu/web/conventions/full-list/-/conventions/treaty/005>.

Галак А. В.

студентка Чернівецького
національного університету
ім. Ю. Федьковича

Науковий керівник: Заморська Л. І.

доктор юридичних наук, доцент
кафедри теорії права та прав людини
Чернівецького національного
університету ім. Ю. Федьковича

ПРОБЛЕМАТИКА ЗАХИСТУ ПРАВ ЛЮДИНИ В КІБЕРПРОСТОРІ

Розвиток сучасних технологій, досягнення науково-технічного прогресу, неодмінно, потребують правового регулювання. Сьогодні мережа Інтернет стала універсальним способом і засобом зберігання інформації та різноманітних відомостей. В Інтернеті відбувається переплетіння величезної кількості користувачів. Процес обміну інформацією став набагато простішим, швидшим та в багатьох випадках безкоштовним.

Щосекунди в соціальних мережах реєструється близько 15 користувачів, 60% населення України вже зареєстровано. Інформаційний світ захоплює не тільки дорослих, а й дітей. 96% дітей користуються інтернетом [2,п.2].

У сьогоденні, держави зобов'язані гарантувати плідне політичне та економічне середовище, де інформаційно-технологічна інф-

раструктура розвиватиметься на благо всіх її громадян. Так, деякі держави вже включили у своє національне законодавство пряме право на доступ до мережі Інтернет. Наприклад, Іспанія гарантує своїм громадянам право на доступ до Інтернету в будь-якому місці. Також подібні права існують в Естонії, Франції, Фінляндії та Греції. Здатність людей отримувати доступ до інформації через використання інформаційних технологій – це найважливіша передумова для участі в інформаційному суспільстві. Звичайно, можливість доступу та використання зазначених технологій не настільки важлива, як інші основні права та потреби людини, проте вона все ще є ключовою вимогою для участі у сьогодиншньому дуже взаємопов'язаному світі, а тому має розглядатися як право людини. Однак, переважна більшість онлайн-споживачів не ознайомлена із своїми суб'єктивними правами та юридичними обов'язками, що й реалізуються у Всесвітній мережі Інтернет. Цей факт зумовлює необхідність захисту індивідуальних та групових прав, що і є предметом кібернетичної безпеки, яка забезпечує захист ресурсів, інформації, даних на етапі їх обміну та збереження [6,п.5].

Проблематика захисту прав людини в кіберпросторі є відносно новим поняттям, адже, Всесвітня мережа Інтернет, винайде-на Вінтоном Серфом та Робертом Еліотом Кан – 29 жовтня 1969 року. Саме ця дата є «пунктом відправлення», з якої все і розпочалося[5,т.1].

Існує безліч шахрайських схем, що найчастіше трапляються в кіберпросторі; найбільш використовувані кіберзлочинцями:

1. Махінації з картками та платіжними системами
2. Створення фіктивних інтернет-магазинів
3. Телефонні дзвінки, з метою одержання персональних даних

Згідно Конвенції Ради Європи по боротьбі з кіберзлочинністю, що була ратифікована Верховною Радою України виділена ще така класифікація злочинності в Інтернет-просторі: злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; шахрайство та підробка, що пов'язані з використанням комп'ютерів; злочини пов'язані з розміщенням у мережах протиправної інформації; злочини щодо авторських і суміжних прав[3].

Все ж таки, «фейкові» веб-сторінки та профілі в соціальних мережах (Facebook, Instagram...), які надають послуги чи товар, займають чільне місце. Шахраї створюють копії вже існуючих магазинів, де реалізують неіснуючий товар за передоплатою. В результаті такого невдалого придбання, користувач залишається без переказаних на рахунок «магазину» коштів та з відсутністю бажаної послуги/речі.

Спеціалісти в сфері комп'ютерної безпеки, надають певні поради, що унеможливлять проведення такого виду афер.

По-перше, слід звертати увагу на посилання, де вказана адреса сайту. Справжні продавці вже зайняли адреси з назвою власне бренду, тому шахраї додають туди ще якесь слівце. Зокрема, інтернет-супермаркет rozetka.com.ua, в руках злочинців, може перетворитись на powerrozetka.com.ua. Також на сайті повинен бути символ зеленого замочку, на початку адреси, що й означатиме, що сайт підтримує захищений протокол [https](https://), а отже, особиста інформація з даними платіжної картки покупця не потрапить до нечесних рук.

По-друге, кваліфікований робітник веб-сайту обов'язково розмістить умови оплати, правила доставки, можливості повернення товару. Зазвичай, шахраї не використовують еквайринг – оплату платіжними картками. Через те, що електронний платіж легко відстежити, що й може підвести під сумнів доброчесність власника картки та реальності магазину. Тому, якщо є необхідність переказу коштів на платіжну картку із сумнівним отримувачем – варто насторожитись.

Дієвим способом є примушення покупця купити прямо зараз, адже, «акція скоро закінчиться» чи навіть «магазин влаштовує повний розпродаж». Як правило, такі «акції» і «розпродажі» у шахраїв не закінчуються ніколи, а зникають разом із сайтом.

По-третє, відгуки – найкорисніша річ в мережі Інтернет. Саме в них ми можемо запевнитись в якості роботи сайту, переглянути рейтинги, що залишили попередні користувачі.

У випадку застосування шахрайських схем на власному досвіді, варто звернутися до кібернетичної поліції (далі – кіберполіції), яка розкриває та сприяє розкриттю злочинів іншим підрозділам поліції, за допомогою електронно-обчислювальної техніки. Основним

завданням кіберполіції є протидія кіберзлочинності: у Департаменті кіберполіції та Відділі протидії кіберзлочинам кажуть, що їхні працівники дбають передусім про безпечні умови громадян в кіберпросторі. Серед основних правопорушень: незаконний доступ, втручання в особисті дані, зловживання пристроями тощо [4, п.1].

Питання забезпечення кібербезпеки почало врегульовуватися на національному рівні. Нещодавно був прийнятий Закон України «Про основні засади забезпечення кібербезпеки України» [1]. Метою цього закону є створення національної системи кібербезпеки, яка сприятиме захисту важливих інтересів суспільства та держави. Закон оперує важливими поняттями, визначає основні об'єкти такого захисту та виділяє ключових осіб, які повинні слідкувати за реалізацією такого захисту. Проте після ознайомлення з текстом цього закону виникає питання, чи захищатиме закон інтереси окремої особи як індивіда? Основна увага закону зосереджена на захисті прав суспільства та держави в кіберпросторі, однак саме людина як індивід зазнає найбільших негативних впливів у сучасному інформаційному просторі. Насамперед, важливою складовою такої проблеми є відсутність розуміння того, що саме повинно захищатися в контексті інформаційної безпеки людини [6, п.11].

Аналізуючи сказане вище, можна стверджувати, що способи комунікації в суспільстві розвиваються в шаленому ритмі. Значний внесок у розвиток цієї сфери внесла пандемія, в умовах якої, кожен з нас опинився в інформаційному вакуумі; стрімко зросла кількість ресурсів, що стали повноцінним замінником справжнього життя. Так звана «віртуальна реальність» поглинула переважну більшість користувачів. Через це, виникла необхідність правового регулювання Інтернет-простору, що й здійснюється підрозділом поліції – кіберполіцією.

Список літератури:

1. Закон України «Про основні засади забезпечення кібербезпеки України» /[Електронний ресурс]: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

2. Інформаційний матеріал «Про безпеку в Інтернеті»/[Електронний ресурс]: <http://stepmnvk.net.ua/bezpeka-v-%D1%96internet%D1%96.html>
3. Конвенція про кіберзлочинність «Статус Конвенції див. (994_789)» { Додатковий протокол від 28.01.2003 до Конвенції див. (994_687)}. Міжнародний документ. 2007/[Електронний ресурс]: <https://законодавство.com/ratifikovani-dokumenti-mijnarodni/konventsija-pro-kiberzlochinnist-status-2007-1426.html>
4. Медіаресурс «Глузд» Що потрібно знати про кібербезпеку та коли звертатися в кіберполіцію?/[Електронний ресурс]: <https://gluzd.org.ua/articles/shcho-potribno-znaty-pro-kiberbezpeku-ta-koly-zvertatysia-v-kiberpolitsiiu/>
5. Тлумачення поняття «Інтернет»/[Електронний ресурс]: <http://wikipedia.ua.nina.az/Internet.html>
6. Юридична газета Online «Проблеми захисту прав людини в інформ-суспільстві»/[Електронний ресурс]: <https://jur-gazeta.com/publications/practice/inshe/problemi-zahistu-prav-lyudini-v-informsuspilstvi.html>

Пойда Д. О.

здобувач першого (бакалаврського)
рівня вищої освіти
Дніпропетровського державного
університету внутрішніх справ

Науковий керівник: Алексєєнко І. В.

доктор політичних наук, професор,
завідувач кафедри міжнародних
відносин Дніпропетровського
державного університету внутрішніх
справ

ВПЛИВ СОЦІАЛЬНИХ МЕРЕЖ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ОСОБИСТОСТІ

Особливо гостро на сьогоднішній день постає питання стану захищеності особистості, суспільства і держави від внутрішніх та зовнішніх інформаційних загроз, при якому забезпечуються реалізація конституційних прав і свобод людини і громадянина, гідні якості і

рівень життя, суверенітет, територіальна цілісність. та стійкий соціально-економічний розвиток України, оборона та безпека держави. Інформаційна безпека – це не лише стан, а й здатність особистості, суспільства та держави протистояти внутрішнім та зовнішнім інформаційним загрозам, спрямованим на заподіяння шкоди та утиск їх інтересів, що виражаються у стабільному функціонуванні та розвитку в умовах існування в інформаційному суспільстві.

На сьогоднішній день більш точним визначенням можна вважати наступне: соціальна інтернет-мережа – це інтерактивний розрахований на багато користувачів веб-сайт, що володіє рядом обов'язкових якостей:

- зміст (контент) сайту створюється виключно чи переважно його користувачами;
- сайт є автоматизованим середовищем, в рамках якого користувачі мають можливість створювати зв'язки з іншими користувачами (соціальні зв'язки) або соціальні об'єкти (тематичні групи);
- користувачі мають можливість отримувати статичну та динамічну інформацію про об'єкти, що існують у даному соціальному середовищі, про соціальні зв'язки між ними;
- користувачам доступні функції комунікації з іншими користувачами та соціальними об'єктами. [1]

Спочатку соціальні мережі замислювалися як розвага, та його стрімкий розвиток призвело до того що, що дослідники у багатьох галузях стали приділяти пильну увагу впливу соціальних мереж на людини, виділяючи як негативні, і позитивні боки явища.

Серед позитивних моментів використання соціальних мереж найчастіше відзначаються їх великі комунікативні можливості, що дозволяють як налагоджувати нові зв'язки, і підтримувати існуючі. Такою була їх функція на момент створення. Проте вже зараз дослідники стверджують, що соціальні мережі відіграють істотну роль у самовираженні людини, що відповідно до піраміди Маслоу є найвищою потребою індивіда.

Набагато більшу увагу дослідники приділяють негативним наслідкам використання соціальних мереж. Насамперед більшість

дослідників у цій галузі підкреслюють загальний негативний вплив соціальних мереж та Інтернету в цілому на людину. Безперечно, соціальні мережі є найбільш підходящим інтернет-ресурсом для збору інформації про кожного її користувача. Найчастіше саме соціальні мережі використовуються під час переслідування, фішингу та інших технологій соціальної інженерії.

Саме соціальні мережі є основним засобом комунікації для учасників та організаторів молодіжних масових заходів, таких як флешмоби, групові походи, тематичні вечірки, аматорські (втім, як і професійні) спектаклі та концерти. Отже, спілкування у соціальних мережах у вигляді обміну повідомленнями не замінює реальність, лише доповнює її, підвищуючи ефективність. Найбільший недолік сучасних досліджень полягає в тому, що в них практично не розглядаються питання, пов'язані з інформаційною безпекою користувача, яка є наріжним каменем цього питання.

Розвиток соціальних мереж дозволяє використовувати безліч сервісів та послуг і в сучасних умовах навіть не потребує комп'ютера. Приблизно третина представників молоді використовує так званий мобільний Інтернет за допомогою гаджетів – мобільних телефонів, смартфонів, планшетів. Програми в цих гаджетах дозволяють часом використовувати навіть більше можливостей соціальних мереж, ніж стандартний спосіб. Саме факти крадіжок грошей із банківських карток та електронних рахунків викликають найбільші побоювання. Безперечно, це питання розглядається в основному фахівцями з комп'ютерної безпеки, які вже розробили програму, яку використовують більшість банків, – 3D Security, яка зобов'язує користувача підтверджувати платежі в мережі Інтернет кодом, що приходить власнику картки на мобільний телефон. Однак автору статті саме в соціальних мережах трапилася можливість обману даної системи – достатньо зламати особисту сторінку користувача, який наважився прив'язати до сторінки банківську картку, щоб зуміти отримати доступ до рахунку, оскільки прив'язана карта вимагає лише підтвердження найпершого використання, ігноруючи систему захисту надалі. Безперечно, можливість прив'язати банківську картку суттєво полегшує

процес купівлі, але також збільшує можливість крадіжки коштів. І тут криється протиріччя, згідно з яким користувачі побоюються розкрадання коштів, але не роблять дій щодо їх додаткового захисту, наприклад, не відмовляються від прив'язки електронних гаманців, не встановлюють додатковий захист у вигляді пароля на проведення операцій з банківськими рахунками. [2]

Наведений приклад показує невідповідність між декларованим почуттям незахищеності особистості в мережі Інтернет та його реальною поведінкою, що підтверджує необхідність проведення додаткових досліджень у галузі інформаційної безпеки та впливу соціальних мереж на особистість, а також подальшої розробки відповідних соціальних технологій з управління інформаційною безпекою особистості.

Підсумовуючи вищевикладене, слід зазначити те що, що соціальні мережі міцно ввійшли у життя. Для своїх користувачів вони представляють чудовий комунікаційний майданчик, який не має обмежень і правил здебільшого, але дозволяє самовиражатися та самореалізовуватися. Не викликає сумнівів і той факт, що соціальні мережі несуть у собі безліч загроз інформаційній безпеці особистості. З їхньою допомогою можна завдати як психологічної, так і економічної шкоди, маніпулювати свідомістю та вчиняти кіберзлочини. Відсутність нормативної бази з питань кібербезпеки, відсутність уявлення про важливість дотримання приватності інформації та можливі ризики спілкування в соціальних мережах є основними факторами, що становлять загрози інформаційній безпеці особистості.

Список використаної літератури:

1. Мануйлов Є. М., Калиновський Ю. Ю. Ціннісні девіації в соціальних мережах як загроза соціокультурному розвитку України. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія : Філософія, філософія права, політологія, соціологія*. 2021. № 1. URL: http://nbuv.gov.ua/UJRN/Vnyua_2021_1_5 (дата звернення 26.11.2021)
2. Орел Г. П. Правове забезпечення прав людини в умовах розвитку соціальних мереж. *Правова держава*. 2021. № 43. URL: http://nbuv.gov.ua/UJRN/Prav_2021_43_3 (дата звернення 26.11.2021)

Орел Г. П.

аспірант ДНУ «Інститут інформації,
безпеки і права Національної академії
правових наук України НАПрН
України»

ЗАХИСТ ПРАВ ЛЮДИНИ В СОЦІАЛЬНИХ МЕРЕЖАХ

Питання захисту соціальних мереж, все більше стала підніматися в обговоренні багатьох людей. Бо саме віртуальний світ, займає більшу частину життя кожної другої, сучасної людини. Молодь спілкується використовуючи сучасні технологічні програми для комунікації.

Вивчивши і проаналізувавши звіт Global Digital про стан цифрової сфери у 2021 році. Ці дані наводять We Are Social і Hootsuite в своєму щорічному звіті про стан цифрової сфери Global Digital 2021, а також було проведено своє дослідження.

Майже півмільярда нових користувачів в соціальних мережах, 1,3 мільярда років проведено в інтернеті за минулий рік, трильйони доларів витрачені в онлайн-магазинах. Основні статистичні дані і тренди по цифровій галузі в світі, які нас можуть зацікавити. Але інформація на січень 2021 року. Для того щоб використовувати соціальні мережі, людині необхідно мати засіб комунікації, іншими словами гаджет (англ. Gadget – пристосування, пристрій, дрібничка) [2] – невеликий пристрій, призначене для полегшення і вдосконалення життя.

Мобільні пристрої є одним із видів популярного гаджету в наш час: сьогодні мобільним телефоном користуються 5,22 мільярда осіб – 66,6% світового населення. З січня 2020 роки кількість унікальних мобільних користувачів виросло на 1,8% (93 мільйони), в той час як загальна кількість мобільних підключень збільшилася на 72 мільйони (0,9%) і досягла 8,02 мільярда до початку 2021 року.

Ще однією важливою складовою, для використання соціальних мереж та віртуального світу в цілому є мережа Інтернету. Інтернет: в січні 2021 року інтернетом користуються 4,66 мільярда людей у

всьому світі, що на 316 мільйонів (7,3%) більше, ніж в минулому році. Рівень проникнення інтернету зараз становить 59,5%. Однак COVID-19 значно вплинув на збір даних про кількість користувачів інтернету, тому фактичні цифри можуть бути вище.

Соціальні мережі: зараз в світі налічується 4,20 мільярда користувачів соціальних мереж. За останні 12 місяців ця цифра зросла на 490 мільйонів, що означає зростання більш ніж на 13% в річному численні. Соціальними мережами в 2021 році користуються 53,6% світового населення.

Чи не менше 98% користувачів будь-якої соціальної платформи також використовують принаймні ще одну соціальну мережу. В окремих соцмережах також спостерігається значне дублювання аудиторії. Так, 85% користувачів TikTok у віці від 16 до 64 років заявили, що використовують Facebook, і майже 95% користувачів Instagram в тій же віковій групі кажуть, що користуються YouTube. В середньому один користувач має аккаунти в 8 різних соціальних мережах, але користується ними з різною частотою із різним ступенем залученості. Як приклад, автором було проведено опитування в форматі Гугл-опитування. Можемо бачити. Майже, кожен з опитуваних, вже має декілька різних мереж, але користується, майже однією-двома, найчастіше.

Сегменти соцмереж Facebook, «ВКонтакте», Twitter, «YouTube» та інших на сьогодні є найменш застрахованими від негативних зовнішніх інформаційних впливів, і це особливо небезпечно в умовах інформаційно-психологічної війни, у яку втягнута сьогодні наша держава. Небезпека пов'язана з низкою факторів.

Серед них:

- не адаптованість сучасної людини до зростаючих масивів нової інформації, різної за якістю, достовірністю і соціальною значущістю;
- невідповідність переважної більшості учасників інформаційних обмінів у мережах у технологічному плані, відсутність навиків пошуку якісної інформації;
- надмірна ідеалізація спілкування в соціальних мережах (при низькій довірі до вітчизняних ЗМІ, політиків);

- відсутність знань про загрози, які несе із собою інформаційна війна, про збитки, яких вона може завдати державі і конкретній людині;
- інші супутні чинники, що можуть завдати серйозної шкоди особистості.

Список використаних джерел

1. Гаджет // Издательский словарь-справочник: [электрон. изд.] / А. Э. Мильчин. – 3-е изд., испр. и доп. — М.: ОЛМА-Пресс, 2006.
2. Статистичні данні [<https://wearesocial.com/digital-2021>]
3. Статистичні данні аналізу використання соціальних мереж розроблено автором [https://docs.google.com/forms/d/1GBvjD083oMdtndeqp82K_Z4Z3FZKT8GrQxHLwODgUeg/edit?usp=sharing]
4. Список соціальних мереж. URL : <https://socialmedialist.org/spysoksotsialnykh-merezh.html>

Данілевич Д. Р.

студентка НТУУ «КПІ ім. Ігоря Сікорського»

Науковий керівник: Головка О. М.

кандидат юридичних наук, старший викладач кафедри інтелектуальної власності та приватного права НТУУ «КПІ імені Ігоря Сікорського»

ПОРУШЕННЯ ЦИФРОВИХ ПРАВ ЖІНОК У СУЧАСНОМУ СВІТІ

Актуальність цієї теми полягає в тому, що сьогодні доступ до інтернету офіційно не визнається як «право людини» на міжнародному рівні, хоча часто згадується в резолюціях і рекомендаціях ООН, Ради Європи та інших міжнародних інституцій. Варто зазначити, що резолюція Ради з прав людини ООН « Сприяння, захист і реалізація прав людини в Інтернеті» засудила дії окремих

держав, спрямовані на обмеження доступу до інтернету. Резолюція прямо поширює права, передбачені Декларацією прав людини, Міжнародним пактом про громадянські та політичні права та Міжнародним пактом про економічні, соціальні та культурні права на інтернет-простір, підкреслюючи принцип «права, які належать людям офлайн, мають захищатися і у мережі Інтернет».

Нещодавні трансформації соціального середовища, поява нових прав людини, що впливають з раніше виокремлених або кардинально нові права, котрі науковці часто відносять до четвертого покоління прав людини зумовлюють потребу в чіткому визначенні їх сутності та кореляції з основоположними правами людини в усталеній парадигмі Human Rights. На відміну від традиційних підходів до аналізу змісту і сутності прав людини пропонуємо розглядати їх через призму понять “інформаційна культура” та “цифрова культура”, адже саме підвищення їх рівня, судячи з національного законодавства, має створити умови для забезпечення інформаційної безпеки людини [1; с.37].

Сьогодні доступ до Інтернету – це важливий засіб для реалізації своїх прав та свобод, а також для участі в демократичних процесах. Саме тому позбавити людину доступу до Інтернету проти її волі можна лише за рішенням суду. Тому не може бути дискримінації за будь-якими ознаками, такими як стать, раса, колір шкіри, мова, релігія або віра, політичні чи інші переконання, національність або соціальне походження, належність до національної меншини, майновий стан, походження чи будь-який інший статус, зокрема, за етнічною приналежністю, віком або сексуальною орієнтацією.

Зауважимо, що впровадження прав людини у сфері цифрових технологій (інколи їх ще називають «цифрові права») потребує від держав додаткових зусиль, спрямованих на розв’язання різних проблемних питань. Одним із них є питання забезпечення права на вільний доступ до інтернету та реалізації можливостей, що витікають із нього. До особливостей прав у сфері цифрових технологій можна зарахувати також те, що доступ до них може бути обмежено. При цьому робити це може як держава, так і звичайні надавачі цифрових послуг (наприклад, провайдер) [2; с.86].

В умовах сьогодення також гостро постає питання про цифрові права жінок. В країнах, що розвиваються жінки мають на 50 % менше шансів отримати доступ до Інтернету, ніж чоловіки. Доступ до Інтернету пропонує людям у всьому світі потужний шлях відстоювати та заявляти про соціальні, економічні та політичні права для розширення своїх можливостей. Останні дослідження показують, що цей гендерний розрив посилюється.

Так, наприклад, у Пакистані жінки відвойовують право на Інтернет. Вид переслідування, з якими жінки стикаються в Пакистані є дуже серйозним і призводить до смертельних наслідків. Цей вид переслідування утримує жінок від доступу до Інтернету. У зв'язку з цим було засновано Фонд цифрових прав для дослідження всіх необхідних питань і жіночого досвіду в Інтернет-просторі та боротьби з кібернасиллям.

Згідно останніх досліджень у Індії лише 17 % жінок, які використовують Інтернет для пошуку важливої інформації про свої права, пошук роботи або висловлювання своєї думки в Інтернеті. Саме для подолання цієї проблеми був запропонований план дій з 5 пунктів під назвою « виключення гендерної різниці ». Програма цифрового розширення прав і можливостей повинна оцінюватися з гендерної точки зору та конкретної стратегії, повинні бути розроблені цілі для розширення прав і можливостей жінок. Крім того, почали створюватися жіночі програми цифрового розширення прав, які мають на меті сприяти цифровій грамотності. Для уникнення гендерного насильства онлайн може бути недостатньо просто введення нового закону про кібербулінг чи кіберпереслідування [3].

Насильство по відношенню до жінок також зустрічається в Інтернеті. Цифрове середовище як логічне продовження інших середовищ включає нові форми , іноді дуже тонкі, насильства, які можуть стати страшенно агресивними та мати незворотні наслідки. Наразі переслідування, погрози та наклеп в Інтернеті складно контролювати та боротися з ними. Жіночий технічний інститут цифрових прав (Women`s Digital Rights), міжнародна приватна організація, місцезнаходження якої в Барселоні націлена на цифро-

вий захист жінок, яка діє за допомогою передових технологічних інструментів і розкриває цілий проект з приводу консультування, підтримки та навчання. Women's Digital Rights пропонує негайні рішення, усуваючи небажаний контент або контент, що порушує права жінок і надає стратегії самозахисту, які дозволяють нам безпечно використовувати Інтернет перед конфліктами.

Хоча на більшість прав та свобод, пов'язаних з інтернетом, уже поширюються гарантії захисту чинних міжнародних актів, проте такий захист наразі є радше мінімальним, тоді як серйозніші гарантії потребують часу для того, щоб отримати свій розвиток у правозастосовній практиці, зокрема, міжнародних судів. “Цифрові права” – це умовна категорія, яка якраз і визначає особливості реалізації та гарантії захисту прав людини в інтернеті. Термін digital rights сьогодні широко використовують на Заході, зокрема в контексті прав на доступ до інтернету, свободи вираження поглядів та приватності онлайн.

Конвенція про захист прав людини і основоположних свобод має високий потенціал для забезпечення дотримання існуючих прав і свобод в цифровому середовищі. Серед них варто виділити недоторканність приватного життя і таємниця листування, захист честі та гідності, право на доступ до інформації, свобода інформації та анонімність.

В Україні питання про порушення цифрових прав наразі також є актуальним, оскільки зростає кількість блокувань веб-сайтів. Розрізняють факти цифрового порушення прав загального характеру у вигляді обмеження доступу до Інтернету та порушення цифрових прав індивідуального характеру, які стосуються порушення права на свободу вираження поглядів у цифровому середовищі.

Тому розробка як міжнародних, так і національних нормативно-правових актів щодо нормативного регулювання та захисту цифрових прав має стати одним із ключових завдань як самих держав так і міжнародних інституцій. А саме захист та популяризація цифрових прав жінок як і в розвинутих країнах, так і в країнах, що розвиваються мають бути вирішенні міжнародними організаціями в найближчий час.

Література:

1. Головка О. М. Цифрова культура та інформаційна культура: права людини в епоху цифрових трансформацій. Інформація і право. № 4 (31).- 2019.- с.37-44
2. Перепьолкін Д. С. Типологія прав четвертого покоління.-2019.- с.86-89
3. Women's rights online. Report card. World wide web foundation.- 2016.- р.- 4

Дергачова А. О.

Науковий керівник: Алексєєнко І. В.

доктор політичних наук, професор,
завідувач кафедри міжнародних
відносин Дніпропетровського
державного університету внутрішніх
справ

ВПЛИВ ЦИФРОВИХ ТЕХНОЛОГІЙ НА ПРАВА ЛЮДИНИ

Цифрова трансформація, що відбувається в світі, прискорена внаслідок пандемії COVID-19 впливає на всі сфери життя, включаючи права людини. З одного боку цифрові технології надають позитивний вплив на здійснення прав людини, відкриваючи нові можливості для їх забезпечення та захисту, а також нові напрямки міжнародного співробітництва у цій сфері. Цифрова революція формує нові права в цифровому просторі Інтернету, інших інформаційно-комунікаційних технологіях, надає нові, часом несподівані аспекти реалізації основних прав і свободи громадянина.

З іншого боку, цифрові технології мають і негативний вплив, породжуючи нові загрози реалізації правами людини. Особливий негативний вплив має наявність цифрової нерівності між державами і всередині країн, що викликає певною мірою дискримінацію певних груп населення, які не мають якісного доступу до цифрових технологій.

Цифрова трансформація впливає як на теорію, так і на практику прав людини. Вона сприяє появі нових понять та концепцій у галузі прав людини, нових інститутів та механізмів, збагачуючи теорію прав людини та розширюючи коло дослідження та програм навчання з питань прав людини [1, с.17]. Безперечно, це знаходить закріплення у міжнародних стандартах та у національному законодавстві, яке має відбивати існуючі тенденції.

Метою дослідження є наукове та теоретичне обґрунтування впливу цифрових технологій на права людини, виділити позитивні та негативні наслідки впливу цифрових технологій на права людини.

У науковій літературі є велика кількість праць, які були присвячені питанням цифрових технологій і прав людини. Варто згадати роботи таких науковців, як Н. Б. Болотіна, Л. П. Гаращенко, С. В. Вишневецька, В. В. Жернаков, А. М. Бурко, Г. М. Зацепи [2, с. 130].

Цифрові технології відкривають нові можливості для реалізації прав людини як: особистих, політичних, соціальних, економічних, культурних.

Насамперед, цей позитивний вплив позначається на реалізації права на інформацію. Цифрові технології забезпечують різноманітність джерел інформації – крім друкованих ЗМІ та телебачення, сьогодні інформація доступна на офіційних веб-сайтах державних органів та відомств, установ, а також у соціальних мережах.

Важливо відзначити, що не тільки державні відомства, але більшість інститутів громадянського суспільства активно користуються можливостями цифрових технологій, що дозволяє отримати повніше уявлення про ті чи інші питання.

Створення веб-сайтів, наявність соціальних мереж дає можливість не лише отримувати інформацію, але й висловлювати свою думку щодо подій, що відбуваються. Таким чином цифровий простір розширює також можливість свободи вираження поглядів. Цифрові технології сприяють також зміцненню взаємодії державних органів та простими громадянами ми нашої держави, що має важливе значення і є одним із критеріїв оцінки ефективності державної політики у галузі прав людини.

Соціальні ЗМІ та такі засоби, як система шифрування комунікацій, допомагають об'єднанню та зростанню рухів правозахисників. Співробітники з прав людини можуть збирати інформацію в соціальних ЗМІ, крім того, що розслідування в галузі прав людини покращуються та доповнюються завдяки знімкам із супутників, а система шифрування повідомлень забезпечує більш ефективні моніторинг, розслідування та аналіз.

Цифрові технології надають сприятливий вплив і на реалізацію права на звернення, створюючи умови для звернення в режимі онлайн, що часто сприяє економії часу та фінансових витрат для обігу. Величезний вплив цифрові технології надають соціально-економічні права людини. Зокрема, дивлячись на ситуацію, що пов'язана з поширенням вірусної інфекції більшість навчальних закладів працює в форматі онлайн, це породжує багато можливостей для реалізації права на освіту, здобуття не лише базової освіти, а й підвищення кваліфікації та перепідготовки кадрів.

Благотворно це позначається і на сфері зайнятості, створюючи можливості роботи в віддаленому режимі та застосування гнучких робочих графіків. Завдяки цифровим технологіям найбільші можливості відкриваються і для реалізації культурних прав людини, наприклад: для реалізації права на наукову творчість. Крім забезпечення прав, цифрові технології створюють нові можливості і для їхнього захисту, оскільки створюють нові способи поведіння зі скаргами.

Крім того, цифрові технології дозволяють привернути більше уваги до випадків порушення прав людини. Не можна залишити поза увагою і той факт, що розширення доступу до інформації сприяє підвищенню правової культури суспільства та культури прав людини, створює нові можливості для ухвалення креативних стратегій у галузі освіти з прав людини.

Таким чином, цифрові технології мають позитивний вплив на забезпечення та захисту прав людини, відкриваючи нові можливості для реалізації всіх категорій правами людини.

Водночас цифрові технології створюють і нові загрози для забезпечення прав людини і несуть у собі певні ризики. Один з го-

ловних факторів, які може знизити позитивний вплив цифрових технологій на права людини, – це наявність цифрової нерівності, яка існує як між країнами, так і в рамках однієї країни, між сільськими та міськими районами.

Одним із способів попередження пандемії, як і раніше, залишається соціальна ізоляція, її заходи зажадали часткового чи повного закриття освітніх установ. Незважаючи на проведення уроків з радіо, телебачення та в інтернеті, а також на всі зусилля вчителів і батьків, багато учнів, як і раніше, залишаються поза досяжністю. Учні з обмеженими можливостями, представники меншин та малозабезпечених сімей, жителі віддалених районів наражаються на найбільший ризик безнадійно відстати у навчанні.

Найважливіше питання захисту прав людини в умовах цифрового простору – це захист інформації про приватне життя [3, с. 64]. Це викликано тим, що у цифровому середовищі інформація про приватне життя поширюється набагато ширше і набагато швидше, ніж раніше. Дані про людину та її особисте життя можуть бути використані зловмисниками. Розголошення приватних відомостей може вплинути на становище людини у суспільстві. Міжнародні громадські організації наголошують, що інтернет дедалі більше стає простором, що загрожує правозахисникам [4, с. 82]. Люди все частіше зазнають нападів і зловживанням з боку приватних суб'єктів лише через їх діяльність у всесвітній павутині на підтримку прав людини.

В результаті нашого дослідження, було проведено соціальне опитування, серед громадян України, щодо впливу цифрових технологій на суспільство в цілому. Вибірка опитування складала 119 повнолітніх осіб. Слід зазначити, що 68 % опитуваних визначили тільки користь, 25 % – обрали негативний вплив, 10 % – обрали відповідь «складно відповісти».

Таким чином, можна стверджувати, що цифрові технології неоднозначно впливають на права людини. Необхідно, з одного боку, використовувати позитивні аспекти, що надаються цифровими технологіями. З іншого боку, постаратися звести негативний вплив до мінімуму через грамотне, розумне ставлення до цифрового простору.

Список використаних джерел:

1. Антонович М. Україна в міжнародній системі захисту прав людини: монографія. – К.: “КМ Academia”, 2000. – 262 с.
2. Госепат Ш. До обґрунтування соціальних прав людини // Філософія прав людини / За ред. Ш. Госепата та Г. Ломанна. – 2-ге вид. – К.: Ніка-Центр, 2012. – С. 129–162.
3. Право на приватність: *conditio sine qua non* / Харківська правозахисна група. – Харків: Фоліо, 2003. – 216 с.
4. Milanovic M. Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age // *Harvard International Law Journal*. – 2015. – Vol. 56. – N. 1. – P. 81–146.

Голубєва Д. В.

курсант Дніпропетровського
державного університету внутрішніх
справ

ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ПРАВ І СВОБОД УРАЗЛИВИХ КАТЕГОРІЙ НАСЕЛЕННЯ (ПІДЛІТКІВ) В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Проблема безпеки, охорони прав та свобод в інформаційному просторі є надзвичайно актуальною у сучасних умовах, особливо коли мова йде про вразливі категорії населення, зокрема малолітніх та неповнолітніх дітей. Із розвитком інформаційних технологій, зростає проблема захищеності дітей у інформаційному просторі, який є не лише зоною розвитку для них, але й потенційною зоною ризику для їх фізичного та психічного здоров'я і соціального самопочуття.

Окреслена проблема знаходить відображення у численних працях зарубіжних та вітчизняних дослідників. Так, її вивченням займалися такі дослідники як: Д. Майерс, Р. Берон, Д. Річардсон, В. С. Батиргарєєва, О. В. Волянська, О. Ю. Дроздов, В. В. Куницький, О. Р. Михайленко, Д. Н. Срібняк, І. К. Туркевич та ін. Однак, не можемо сказати, що проблема безпеки підлітків в інформацій-

ному просторі є повністю дослідженою, адже їй приділяється недостатньо уваги у сучасній науковій літературі.

Насамперед зазначимо, що відповідно до статті 52 Конституції України, дитинство охороняється державою [2]. Також діє закон України «Про охорону дитинства», який передбачає заборону пропагування у ЗМІ культу жорстокості та насильства, розповсюдження порнографічної інформації та інформації, яка зневажає людську гідність та завдає шкоди моральному благополуччю дитини [1]. Однак, досить часто відбувається нехтування та порушення цих законів і норм, що тягне за собою ряд негативних наслідків.

Беззаперечним є той факт, що світ інформаційних технологій надає підліткам безмежні можливості для навчальної діяльності та спілкування, але в той же час, створює низку серйозних проблем, що пов'язані з недотриманням прав та свобод дітей в інформаційному просторі [4].

Так, інформація, яка містить елементи жорстокості, насильства та агресії формує у підлітків неправильні моральні якості, переконання, естетичні смаки, які моделюють їх поведінку у реальному житті. Крім того, встановлено, що існує причинно-наслідковий зв'язок між «розважальним насильством» та проявами агресії серед підлітків. Як стверджують науковці, негативна інформація здійснює вплив на ціннісні орієнтації особистості і молодь, у якої ще недостатньо сформована психіка, вважає, що насильство є допустимим шляхом вирішення соціальних конфліктів. Підтвердженням цього є і той факт, що часто неповнолітні правопорушники вказують серед причин, що штовхнули їх на скоєння злочину, перегляд відповідних відеоматеріалів [3].

Окрім телебачення, ЗМІ та різноманітних комп'ютерних ігор на поведінку підлітків значний вплив мають Інтернет-технології. Адже, з їх допомогою молоді люди дізнаються про секс та мають доступ до матеріалів порнографічного характеру, розповсюджують фото- та відеозображення із аморальним та насильницьким змістом, виникає проблема булінгу та кібербулінгу.

З огляду на це, можемо зробити висновок, що на сьогоднішній день дуже важливим завданням є захист молоді від мораль-

ного, психологічного та фізичного насильства у інформаційному просторі, а також захист їх прав та свобод. Тому, суспільство має активно протистояти численним викликам та загрозам, які несе інформаційний простір, а державна політика повинна спрямовуватися на захист свобод і прав громадян, забезпечення безпечного інформаційного простору та пропагування й відродження моральних та духовних цінностей.

Список використаних джерел:

1. Закон України про охорону дитинства: за станом на 1 груд. 2001 р. Відом. Верхов. Ради України. 2001. № 30. С. 142.
2. Конституція України. URL: <https://konstitutsiya.com.ua/st-52> (дата звернення: 15.11.2021).
3. Куницький В. В. Захист неповнолітніх в інформаційному просторі як об'єкт гуманітарної експертизи: український та зарубіжний досвід. URL: <http://academy.gov.ua/ej/ej14/txts/Kunitskiy.pdf> (дата звернення: 15.11.2021).
4. Права дітей в Інтернеті. URL: https://ndipzir.org.ua/wp-content/uploads/2017/07/Yefremova/3_5.pdf (дата звернення: 15.11.2021).

Баюрчак М. І.

студентка Чернівецького
національного університету імені
Юрія Федьковича

Науковий керівник: Заморська Л. І.

доктор юридичних наук, доцент
кафедри теорії права та прав людини
Чернівецького національного
університету імені Юрія Федьковича

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

XXI століття – це століття нових технологій, проривних відкриттів та доленосних рішень. Зокрема, розширення знань особи

в області інформації та мережі Інтернет призвело як і до позитивних результатів, так і до виникнення великої кількості ризиків та загроз, що можуть нанести шкоди. Оскільки ми є частиною «новітнього» суспільства, саме від нас залежить подальший розвиток безпечного користування кіберпростором в Україні.

На нашу думку, одним із головних чинників модернізації будь-якої країни, що є правовою, є інформатизація усіх частин її політики та забезпечення кібербезпеки. Оскільки держава відповідає за особисті свободи і права своїх громадян, вона мусить гарантувати їх надійну захищеність та законодавче закріплення. Статистика кібератак в світі зовсім не втішна, за дослідженнями організації ISACA, на сьогодні тільки 30% респондентів вважають свої персональні дані захищеними, інші є сприймають цифрові злочини як найнебезпечніші для життя суспільства. Такі цифри, на нашу думку, ще раз підкреслюють важливість офіційного правового регулювання відносин, що стосуються інформаційного простору та людської діяльності у ньому в цілому [1, ст. 100-101]

Окрім втручання в особисте життя особи та посягання на її основоположні права, кіберзлочинці можуть шкодити і юридичним особам та навіть державам. Так, зокрема, найбільша кількість кібератак припадає на очільників США (близько 46% на рік), за статистикою Microsoft. Невтішна статистика і для України – ми другі в цьому рейтингу, на інформаційну безпеку нашої держави припадає цілих 19 %. Доречно і виділити винуватців наших бід – серед найбільш активних хакерських груп Microsoft виділила російську групу Nobelium, яка, зокрема, здійснювала атаки на галузь держуправління, дипломатії, оборони. Не відстає й угруповання Thallium, що базується у КНДР. [2]

Наслідки для держав від такого втручання стають колосальними. Збої в комп'ютерних системах призводять до таких явищ як втрата конфіденційних даних, коштів та відновлення процедур інформаційного обігу. Проте, з кібератаками зустрічаються й звичайні громадяни. Вони втрачають приватні документи, банківські рахунки, коди та навіть документацію. Сьогодні шахраї ледь не на кожному кроці, а види обману подекуди шокують. В період пандемії

мії хакери приводили розсилки електронних листів з нібито підписом Всесвітньої Організації Охорони Здоров'я, такі “послання” часто супроводжувалися звинуваченнями, граючи на нашому страху. Деякі і зовсім перехоплюють файли в мережі, шифруючи документ починають шантажувати адресата. [3]

Наразі українське законодавство з питань кіберзахисту вже протягом досить довгого періоду часу знаходиться на етапі розвитку, проте як же законодавство може захистити громадянина та на що розраховувати особі, що стала жертвою кіберзлочинця? Зокрема, Основним Законом передбачена юридична відповідальність за будь-які правопорушення у сфері електронних комунікацій та захисту інформаційних джерел. Також слід зазначити, що кожна особа має право доступу до будь-якої інформації чи даних та право на безпечне користування інтернет-джерелами. Закон України «Про основні засади забезпечення кібербезпеки України» також зазначає, що будь-яка непогодженна обробка даних, їх використання чи ушкодження, неправомірне накопичення, поширення чи оплата доступу до персональних даних – вважаються правопорушенням та тягнуть за собою відповідальність, встановлену законом. [4, 5]

Ми впевнені, що в Україні повинна існувати окрема національна система інфраструктури та законодавства, діяльність якої повинна спрямовуватися на захист від кіберзагроз та їх виявлення та більш жорстка міра покарання за такого роду правопорушення, що стало б стимулом для утримання осіб від застосування кіберзброї та створення небезпечного кібер середовища.

Отже, можна підсумувати, що законодавство України з питань кіберзахисту знаходиться на етапі розбудови. Правове забезпечення кібербезпеки на сьогодні є досить хитким та ненадійним, що надає можливості для виникнення загроз стосовно наших громадян та держави. Незважаючи на такі негативні показники, потрібно чітко спрямувати діяльність національних органів безпеки в напрямку розвитку кібербезпеки та безпосереднього органів державної влади для вдосконалення законодавчої основи кіберзахисту в Україні.

Список використаної літератури:

1. Бакалінська О., Бакалінський О. Адміністративне право і процес. Правове забезпечення кібербезпеки в Україні. Режим доступу: <http://pgp-journal.kiev.ua/archive/2019/9/18.pdf>

2. Слово і діло. Аналітичний портал. Країни-жертви та країни-агресори у хакерських війнах. Режим доступу: <https://www.slovoidilo.ua/2021/10/22/infografika/svit/krayiny-zhertvy-ta-krayiny-ahresory-hakerskykh-vijnah>

3. ГО “Спільно”. Найпопулярніші види кібератак у 2021 році. Режим доступу: <https://spilno.org/news/naipopulyarnishi-vydy-kiberatak-u-2021-rotsi>

ЗАКОН УКРАЇНИ. Про основні засади забезпечення кібербезпеки України. [Електронний ресурс] : Закон України № 2297-VI від 1 червня 2010 року. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2297-17>

ЗАКОН УКРАЇНИ. Про основні засади забезпечення кібербезпеки України. [Електронний ресурс] : Закон України № 2163-VIII від 1 серпня 2022 року. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2163-19>

Годлевська В. Ю.

доктор історичних наук, професор

НАЦІОНАЛЬНИЙ КРИПТОЛОГІЧНИЙ ЦЕНТР В СИСТЕМІ КІБЕРБЕЗПЕКИ ІСПАНІЇ

Масове використання інформаційно-телекомунікаційних технологій у всіх сферах суспільства створило новий простір, кіберпростір, де виникають конфлікти, існують кіберзагрози, які можуть загрожувати національній безпеці, верховенству права, економічному процвітання, державі добробуту та нормальному функціонуванню суспільства та державного управління. Усе це обґрунтувало необхідність створення національних стратегій кібербезпеки, які дають змогу сформулювати цілі та заходи для досягнення та підтримки високого рівня безпеки державних інформаційних систем і мереж.

Значних успіхів у розробці власної системи Національної кібербезпеки досягла Іспанія. Глобальний індекс кібербезпеки

(GCI), підготовлений Міжнародним союзом телекомунікацій Організації Об'єднаних Націй, ставить Іспанію на 7-е місце у світі (попереду лише Сполучене Королівство, США, Франція, Литва, Естонія та Сінгапур) [3, Р. 5]. Досвід цієї країни є цікавим для пізнання та аналізу.

Окреме місце в забезпеченні безпеки у кіберпросторі Іспанії займає Національний криптологічний центр (CCN), який знаходиться в підпорядкуванні Національного розвідувального центру при Міністерстві оборони.

Основна інформація про особливості функціонування центру міститься у відповідних законодавчих актах та постановах. Так, зокрема, закон 11/2002 від 6 травня, який регулює функціонування Національного розвідувального центру, покладає на нього виконання функцій, пов'язаних із безпекою інформаційних технологій (стаття 4.e) та захистом інформації (стаття 4.f.), в той же час на його директора покладено відповідальність за керівництво Національним криптологічним центром (стаття 9.2.f) [2, Р. 16442].

Зазначений центр було створено у 2002 р., а його діяльність регулюється Королівським указом 421/2004 від 12 березня [6, Р. 12203].

На Національний криптологічний центр покладені такі функції:

- 1) підготовка та поширення стандартів, інструкцій, посібників та рекомендацій в сфері інформаційних технологій та комунікаційних адміністративних систем (CCN-STIC Guides). Вони періодично оновлюються та доповнюються новими, залежно від загроз і вразливостей, виявлених CCN-CERT. Основна частина спеціально орієнтована на персонал державних адміністрацій, компаній та організацій, що становлять стратегічний інтерес.

- 2) Підготовка спеціалізованих управлінських кадрів у сфері безпеки систем інформаційно-комунікаційних технологій.

- 3) Оцінювання та акредитація здатності засобів і систем шифрування безпечно обробляти, зберігати або передавати інформацію.

- 4) Координація поширення, розробка, придбання, експлуатація та використання технологій безпеки вищезгаданих систем.

5) Забезпечення дотримання нормативно-правових актів щодо захисту секретної інформації у сфері своїх компетенцій.

6) Встановлення необхідних відносин та підписання відповідних угод з подібними організаціями в інших країнах для розвитку вищезгаданих функцій [6, Р. 12204].

В структуру CCN інтегровані два підрозділи:

- *Національний криптологічний центр реагування на надзвичайні ситуації (CCN-CERT).*
- *Орган з сертифікації (ОС) Національної схеми оцінки та сертифікації безпеки інформаційних технологій (ENECSTI) [4, Р. 38790].*

Національний криптологічний центр реагування на надзвичайні ситуації був створений з метою покращення іспанської кібербезпеки, є національним центром оповіщення та реагування, який допомагає швидко та ефективно реагувати на кібератаки та активно протистояти кіберзагрозам, включаючи координацію на державному рівні.

З цієї причини кілька років тому центром було створено профілі в соціальних мережах LinkedIn, Twitter, YouTube і Telegram каналах, які сьогодні є одним з основних засобів масової інформації, через які CCN- CERT повідомляє про свою діяльність, маючи аудиторію з понад 22 500 підписників у LinkedIn і понад 21 500 у Twitter.

У 2017 р. відділ запустив платформу Atenea Challenge Platform, де користувачі можуть продемонструвати свої знання та навички, вирішуючи завдання різної складності та різних тем: криптографія та стеганографія; експлуатація, криміналістична експертиза, аналіз трафіку, реверс тощо. Серед основних цілей Atenea Challenge Platform: підвищити обізнаність персоналу ІКТ щодо ризиків у сфері кібербезпеки.

Досягнувши успіху, Національний криптологічний центр у 2018 р. запустив нову платформу з більш базовим рівнем для розповсюдження знань серед менш обізнаних користувачів: Atenea Escuela [1].

Нарешті, однією з останніх ініціатив, запущених CCN для навчання кібербезпеці, стало створення BNGELES, порталу з численними ресурсами, спрямованими на розширення знань у цій сфері.

Варто виділити розділ Cyber Tips, де зібрані рекомендації щодо уникнення кіберзагроз, боротьби з дезінформацією, а також безпечного використання соціальних мереж і технологій. Усі ці ініціативи сприяють підвищенню професійного рівня знань, навичок та вмінь, бо лише в такий спосіб, як зазначено в Національній стратегії кібербезпеки Іспанії, «можна буде реагувати на великі виклики кібербезпеці» [5, Р. 43449].

Національний криптологічний центр Іспанії реалізував ефективний підхід до розробки, впровадження та вдосконалення загальної схеми національної кібербезпеки. На основі розробок, здійснених в Іспанії за останні десятиліття, можна стверджувати, що Національний криптологічний центр зумів забезпечити модель розвитку для вирішення на національному рівні різних проблем, які пов'язані з захистом інформаційних мереж.

Література

1. ATENEA Escuela. Режим доступу: <https://atenea.ccn-cert.cni.es/escuela/home>
2. Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia // Boletín Oficial del Estado. – 2002. – 7 de mayo. – № 109. – P.16440-16444 .
3. Ballesteros Martín M. B. El ciberespacio lleva acos consolidándose como un entorno de alta relevancia económica y social, pero también de inseguridad // Actuarios. – 2021. – № 48. – P.4-7. Режим доступу: <https://www.actuarios.org/wp-content/uploads/2021/03/Actuarios-48-web-low.pdf>
4. Orden PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información // Boletín Oficial del Estado. – 2007. – 25 de septiembre. – №230. – P. 38781-38805.
5. Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional // Boletín Oficial del Estado. – 2019. –№ 103. – 30 de abril. – P. 43437- 43455.
6. Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional // Boletín Oficial del Estado. – 2004. – 19 de marzo. – № 68. – P. 12203- 12204.

Мурашкіна Я. Ю.

Науковий керівник: Алексєєнко І. В.

доктор політичних наук, професор,
завідувач кафедри міжнародних
відносин Дніпропетровського
державного університету внутрішніх
справ

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ГАРАНТІЯ ПРАВ ЛЮДИНИ

В сучасному світі, особливо під час пандемії, актуальності набуває проблема співвідношення інформаційної безпеки та прав людини. Права людини є фундаментом сучасної правової держави. Удосконалення інформаційних технологій супроводжується розширенням можливостей їх недобросовісного використання, яке створює загрози інформаційній безпеці та може призводити до порушень прав людини. У зв'язку з цим виникає проблема співвідношення інформаційної безпеки та прав людини, насамперед права на недоторканність і приватного життя.

Метою даного дослідження є опрацювати наукову літературу та з'ясувати чи є інформаційна безпека – гарантією прав людини.

В Україні поняття «безпека», «інформаційна безпека» та «національна безпека» розкриваються через стан захищеності життєво важливих інтересів особистості, суспільства та держав. Інформаційна безпека у даному разі визначається як стан захищеності національних інтересів України в інформаційній сфері, що складається з сукупності збалансованих інтересів особистості, суспільства та держави, від внутрішніх та зовнішніх загроз.

У правовій літературі також використовується визначення «інформаційної безпеки» через стан захищеності інформаційної сфери, при якому неможлива реалізація відомих загроз щодо її складових елементів. При цьому поняття «інформаційна безпека» розглядається як більш загальна категорія по відношенню до поняття «захист інформації», в якому акцент робиться на комплексі

заходів та дій, спрямованих на забезпечення безпеки інформації [1, с.5].

У разі йдеться про стан захищеності інформації, а не інтересів особистості, нашого суспільства та держави. У правовій доктрині Європейського Союзу визначення «інформаційної безпеки» здійснюється через перерахування конкретних елементів інформаційної сфери, на захист яких вона спрямована і пов'язується з правовими принципами конфіденційності, цілісності та доступності інформації та інформаційних систем.

Реалізація цих принципів дозволяє забезпечити баланс інтересів різних учасників правовідносин, виступаючи, таким чином, гарантією прав людини у сфері забезпечення інформаційної безпеки. За дотримання принципу конфіденційності ознайомлення з конфіденційною інформацією, її обробка та пред'явленні вимоги про її надання допускаються лише для особи, яка має право доступу до такої інформації.

Роль принципу конфіденційності полягає в запобіганні шкоди, яка може бути заподіяний суспільним відносинам внаслідок неправомірного надання та розповсюдження інформації, що зберігається в таємниці через її значення для безпеки особистості, суспільства чи держави. Даному принципу відповідає свого роду право зберігати її в таємниці, обмежувати доступ третіх осіб до неї контролювати її цільове використання.

Інформаційна безпека є однією з проблем, з якою зіткнулося сучасне суспільство у процесі масового використання автоматизованих засобів її опрацювання. Проблема інформаційної безпеки обумовлена зростаючою роллю інформації у суспільному житті. Сучасне суспільство дедалі більше набуває рис інформаційного суспільства.

Вирішення проблеми інформаційної безпеки, як правило, починається з виявлення суб'єктів інформаційних відносин та інтересів цих суб'єктів, пов'язаних із використанням інформаційних систем. Це обумовлено тим, що для різних категорій суб'єктів характер розв'язуваних завдань може суттєво відрізнятися. Наприклад, завдання адміністратором локальною мережі по забез-

печення інформаційної безпеки, значною мірою відрізняються від завдань, що вирішуються користувачем домашнього комп'ютера, не пов'язаному мережею.

У юридичних відносинах все частіше використовуються особливі державні інформаційні системи, для повного функціонування яких необхідне розширення повноважень органів влади у сфері обробки в автоматизованому режимі різного роду особистої інформації. Дані процеси поряд з заходами, які вживаються для забезпечення національної безпеки, призводять до формування в законодавстві обмежень права на недоторканність приватного життя [2, с.34]. При цьому запобігання незаконному втручання у приватне життя та зловживань з боку органів влади стає одним із пріоритетних напрямів забезпечення інформаційної безпеки особистості.

З одного боку, як гарантії права на недоторканність приватного життя виступають заходи щодо забезпечення інформаційної безпеки, безпосередньо спрямовані на захист цього права. При цьому вироблення відповідних заходів здійснюється шляхом конкретизації правових принципів конфіденційності, цілісності та доступності з урахуванням суті права на недоторканність приватного життя та його можливі порушення.

З іншого боку, під час встановлення обмежень права на недоторканність приватного життя відповідні гарантії повинні попереджати можливі зловживання такими обмеженнями, що призводять до загроз інформаційній безпеці особистості.

Одним з принципів захисту права на недоторканність особистого життя, які висвітлені у деяких правових принципах, є згода особи на обробку персональних даних та її повідомлення про таку обробку. Таким чином конфіденційність особистої інформації визначається шляхом надання доступу або можливості отримання та обробки такої інформації тільки тим особам, які мають відповідну згоду її власника. Коли доступ або можливості збору та опрацювання надаються на підставі чинного законодавства, то обов'язковим є повідомлення про обробку персональних даних їх власника. Повідомлення також є обов'язковим при інших ви-

падках, визначених суб'єктом персональних даних або встановлених законодавством, наприклад, при порушенні конфіденційності або цілісності персональних даних. Зазначені механізми надають суб'єкту персональних даних правові можливості контролю за їх використанням гарантії недоторканності його приватного життя.

У державах з демократичними правовими режимами, як правило, встановлено пріоритет прав людини перед забезпеченням національної безпеки. Такий пріоритет виявляється у тому, що заходи щодо забезпечення національної безпеки, пов'язані зі збором та обробкою відповідної інформації, приймаються при дотримання спеціальної процедури, яка забезпечує їх пропорційність загрозам, що виникають. В основі цього підходу лежать положення Конвенції, в якій визначено умови обмеження права людини на недоторканність приватного життя – «встановлення обмеження лише законом» та «необхідність у демократичному суспільстві» [3, с.76]. Обмеження має відповідати цілям його встановлення. Це дозволяє не тільки визначити доцільність чи обґрунтованість встановлення або застосування такого обмеження, але також оцінити можливість ефективного досягнення тих же цілей у відсутності обмеження права або його меншого обмеження [4, с.91].

У підсумка можна сформулювати, що в розвиток технологічних умов у забезпечення інформаційної безпеки видається однією з важливих гарантій прав людини. В змісті таких правових гарантій лежить дотримання принципів конфіденційності, цілісності і доступності інформації щодо інформаційних систем. Щоб забезпечити інформаційну безпеку особистості, здійснюється напрацювання спеціальних правових засад для захисту права на недоторканність приватного життя, а також щодо механізмів його захисту, пов'язаних із встановленням особливих вимог у сфері збору та опрацювання особистої інформації. Забезпечуючи національну безпеку як одну з складових важливих гарантій прав людини є дотримання принципу пропорційності. Втілювати дані принципи і механізми захисту прав людини при забезпеченні інформаційної безпеки може набувати різних форм, які певним чином залежать від правових особливостей та політичного режиму держави.

Список використаних джерел:

1. Правова ідеологія і право України на етапі становлення тоталітарного режиму (1929-1941) / Усенко І. Б., Мироненко О. М., Чехович В. А. та ін.; За ред. О. М. Мироненка, І. Б. Усенка. – К.: Інститут держави і права ім. В. М. Корецького НАН України, 2001. С. 128.
2. Сидорчук Ю. М. Механізми захисту прав людини та громадянина: сутність і перспективи розвитку в Україні. Науковий вісник Чернівецького університету. 2013, Випуск 682: Правознавство. С.33-35
3. Фурашев В. М., Солончук І. В. Інформаційне право: інформаційне судочинство. Право та державне управління. № 3 (36). Том 1. 2019. С. 241 – 251.
4. The Future of Jobs. Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution (The World Economic Forum 2016) 157.

Свистонюк В. А.

курсант Дніпропетровського
державного університету внутрішніх
справ

Науковий керівник: Миронюк Р. В.

доктор юридичних наук, професор
кафедри адміністративного права,
процесу та адміністративної
діяльності Дніпропетровського
державного університету внутрішніх
справ

АДМІНІСТРАТИВНО-ПРАВОВІ ЗАХОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОГО ПРАВОПОРЯДКУ

Вступ. Інформаційні перетворення, які здійснюються останнім часом у світовому просторі, настільки глибокі та масштабні, що при усій їх непослідовності та суперечності неважко помітити процес докорінного оновлення інформаційного суспільства. При цьому змінюється роль та місце держави, суспільства та особи у сфері інформаційних правовідносин, виникають нові вимоги та

правила здійснення інформаційної діяльності, а також цінності у сфері інформаційного правопорядку, що проголошуються та захищаються державою.

Принципи правової держави в інформаційній сфері поки ще не стали реальністю. Більш того, на цей час держава не в змозі у повному обсязі забезпечити надійний захист та охорону інформаційного правопорядку, інформаційних прав і свобод людини і громадянина, організувати та проводити належну діяльність щодо протидії правопорушенням у сфері інформаційного правопорядку. У зв'язку з цим, охорона та забезпечення інформаційної безпеки, попередження та припинення правопорушень у сфері інформаційного правопорядку були та залишаються найважливішими завданнями державних органів і суспільства у цілому.

Управління інформаційним суспільством, забезпечення інформаційної безпеки і правопорядку здійснюється за допомогою активних засобів цілеспрямованої дії на свідомість і поведінку людей, в якості яких виступають адміністративно-правові заходи [1].

Адміністративно-правові заходи забезпечення інформаційного правопорядку полягають в психологічному та фізичному впливі з боку суб'єктів владних повноважень на посадових осіб учасників інформаційної діяльності, громадян, які мають право на інформацію, та свідомо, навмисно чи з необережності, не виконують або не намагаються виконувати діючі правила, процедури. У першу чергу застосуванню підлягають заходи психологічного плану, що не допускають обмеження свободи дій, пересування, розпорядження майном, особистої недоторканості об'єкта управління. Але якщо учасник інформаційної діяльності не вживає самостійно зусиль для повернення до стану інформаційного правопорядку, після законної вимоги посадової особи суб'єкта владних повноважень не порушувати інформаційний правопорядок, виправданим виступає застосування до нього більш жорстких, інтенсивних владних заходів фізичного примусу, як реакції на продовжувану протиправну поведінку. Таким чином, заходи фізичного примусу застосовуються як крайній засіб, для припинення особливо зухвалого порушення інформаційного законодавства. Вони передбачають суттє-

ве обмеження особистісної і майнової сфери правопорушника. Це обумовлює необхідність їх докладного законодавчого визначення.

Адміністративно-правові заходи протидії правопорушенням у сфері інформаційного правопорядку можуть застосовуватися як самостійно (закриття у зв'язку із закінченням ліцензії суб'єкта інформаційних правовідносин), так й у сукупності з адміністративними стягненнями, при цьому вони забезпечують можливість стягнення і, як правило, їм передають (затримання порушника інформаційного порядку з подальшим накладенням на нього адміністративного штрафу)[2].

Тобто, виходячи з теорії адміністративного права, адміністративно-правові заходи поділяються на три види заходів:

- адміністративні стягнення (штраф, конфіскація);
- заходи припинення (особисте затримання, позбавлення спеціального права, тощо);
- адміністративно-попереджувальні заходи (огляд, перевірка документів, вимога припинення окремих дій тощо).

Кожен з цих заходів має своє призначення, специфіку та водночас спільні риси, що витікають з державно-владного характеру управлінських функцій та є обов'язковим для виконання.

Можна виділити наступні особливості адміністративно-правових заходів щодо протидії правопорушенням у сфері інформаційного правопорядку, а саме:

- застосовуються для негайного припинення порушення закону, вимог та правил здійснення інформаційної діяльності;
- носять вольовий і достатньо жорсткий характер
- носять як правило стисло тимчасовий характер
- застосовуються владними суб'єктами, що мають функції із забезпечення інформаційного порядку[3].

В адміністративно-правовій літературі існують різні переліки адміністративно-правових заходів. Однак, відносно переліку таких заходів щодо протидії правопорушенням у сфері інформаційного правопорядку слід урахувувати повноваження основних суб'єктів інформаційних правовідносин, тобто у процесі односторонньої реалізації їх юридично-владних повноважень. Заходи та-

кого роду багатоманітні, застосовуються у різних сферах суспільного життя й різними суб'єктами. В основному вони носять галузевий профіль, але можуть здійснюватися й органами із загальною управлінською компетенцією.

Необхідно визначити, що адміністративно-правові заходи попередження, припинення, профілактики правопорушень у сфері інформаційного правопорядку покликані забезпечити максимально можливе їх обмеження та доведення до такого стану, при якому ці правопорушення перестали би бути загрозою інформаційній безпеці України[4].

Висновки. Підсумовуючи вище викладене можна надати наступне визначення поняттю адміністративно-правових заходів протидії правопорушенням у сфері інформаційного правопорядку, зокрема – це законодавчо закріплена сукупність взаємопов'язаних заходів владного впливу компетентних органів держави організаційно-правового та спеціального характеру, які спрямовані на забезпечення захисту інформаційного правопорядку, інформаційної безпеки та інформаційних прав і свобод держави, суспільства, людини та громадянина.

Список літератури:

1. Битяк Ю. П. Гаращук В. М., Дьяченко О. В. Адміністративне право України. Київ: Юрінком Інтер, 2007. 367 с 813
2. Інформаційне право та інформаційна безпека / редкол.: В. П. Філонов (відп. ред.), Р. А. Калюжний, Є. А. Тихонова та ін. Донецьк-К.: ДІВС МВС України, Ін-т економіки та права «КРОК», 2001. 230 с.
3. Інформаційне право та правова інформатика у сфері захисту персональних даних: монографія / авт. кол.: В. М. Брижко, М. В. Гуцалюк, В. С. Цимбалюк, М. Я. Швець; за ред. М. Я. Швеця. Київ: НДЦГП АПРН України, 2006. 450 с.
4. Настюк В. Я. Белєвцева В. В. Адміністративно-правовий захист інформації: проблеми та шляхи вирішення. Київ: Ред. журн. «Право України»; Харків: Право, 2013. 128 с. (Наук. зб. «Академічні правові дослідження». Дод. До юрид. журн. «Право України»; вип. 28)

Власюк Є. П.

студент Чернівецького національного
університету ім. Ю. Федьковича

Науковий керівник: Заморська Л. І.

доктор юридичних наук, доцент
кафедри теорії права та прав людини
Чернівецького національного
університету ім. Ю. Федьковича

ВІДПОВІДАЛЬНІСТЬ ЗА РОЗПОВСЮДЖЕННЯ НЕДОСТОВІРНОЇ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТ

У ХХІ столітті інтернет став для людства вже звичайною, буденною справою, до якої вже всі звикли та котрою активно користуються у всіх сферах свого життя. Щодня мільйони людей з головою занурюються у соціальні мережі, сприймаючи, таким чином, велику кількість інформації. Тому, постає питання якості, точності та достовірності тієї інформації, яку так активно потім будуть використовувати інші. Сотні джерел інформації, якими користуються інтернет-ресурси, не завжди є перевіреними, не завжди саме в них міститься правда.

Інтернет, безсумнівно, вже залишив величезний слід в історії і ігнорувати процес регулювання відносин в інтернеті, як раніше, вже не вдасться. В багатьох розвинутих країнах вже почали існувати спеціалізовані органи, які контролюють діяльність громадян в інтернеті. В Україні такий орган називається кіберполіція який входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює, відповідно до законодавства, оперативно-розшукову діяльність.

На жаль, не всі суб'єкти інформаційних відносин, так само як і суспільних, є відповідальними та правослухняними, тому деякі з них використовують інтернет зовсім не в правовірних цілях. Часто недостовірна інформація розповсюджується навмисно, за

спеціально підготовленим планом. В Україні в більшості випадків єдиною можливістю захистити свої права в разі поширення недостовірної інформації є звернення за захистом до суду. Право на свободу думки та вільне вираження своїх поглядів є одним із фундаментальних немайнових прав будь-якої особи. А розвиток інформаційних технологій значно спростив можливість для реалізації зазначеного права, оскільки дозволяє за кілька хвилин поширити будь-яку інформацію невизначеному колу осіб. Але нерідко трапляються ситуації, коли поширена в інтернеті інформація стосовно певної особи, групи осіб, або будь-якого іншого суб'єкта інформаційних відносин не тільки є недостовірною, а й такою, що порушує її право на повагу до честі та гідності. Іноді відновити порушені права можливо в досудовому порядку, проте в більшості випадків єдиною можливістю відновлення таких прав є звернення за захистом до суду.[2]

Відповідно до *Закону України «Про інформацію»* від 02.10.1992 № 2657-ХІІ «інформація» – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді, тобто інформація, яка поширюється в інтернеті так само підпадає під норми цього закону.

Основними принципами інформаційних відносин згідно ст.2 *Закону України «Про інформацію»* 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. Тобто, окрім того, що інформація повинна бути достовірною, вона повинна бути повною, не вирваною з контексту, доступною, відкритою.

Основними напрямками державної інформаційної політики згідно ст.3 *Закону України «Про інформацію»* є : забезпечення доступу кожного до інформації; забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації; створення умов для формування в Україні інформаційного суспільства; забезпечення

відкритості та прозорості діяльності суб'єктів владних повноважень; створення інформаційних систем і мереж інформації, розвиток електронного урядування; постійне оновлення, збагачення та зберігання національних інформаційних ресурсів; забезпечення інформаційної безпеки України; сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору.[3]

Ми розглянули, що таке інформація, та основні принципи інформаційних відносин, але що ж таке недостовірна інформація? Недостовірною вважається інформація, яка не відповідає дійсності або викладена неправдиво, тобто містить відомості про події та явища, яких не існувало взагалі або які існували, але відомості про них не відповідають дійсності (неповні або перекручені).

До способів захисту основоположних прав людини, зокрема права на повагу до гідності та честі, права на недоторканість ділової репутації, відносяться, наприклад, спростування недостовірної інформації та/або право на відповідь, заборона поширення інформації, якою порушуються особисті немайнові права тощо. Різницею права на спростування недостовірної інформації та права на відповідь полягає в тому, що при реалізації права на відповідь особа має право на висвітлення власної точки зору щодо поширеної інформації та обставин порушення особистого немайнового права без визнання її недостовірною, а також те, що недостовірну інформацію спростовує особа, яка її поширила, а відповідь дає особа, стосовно якої поширено інформацію.

В окремих випадках, фізична особа має право на захист особистих немайнових прав, спричинених розповсюдженням недостовірної інформації у випадку, коли вона поширена стосовно інших осіб. Насамперед, це стосується членів сім'ї фізичної особи, наприклад, щодо другого з подружжя, батьків, дітей, баби, діда, прабаби, прадіда, внуків, правнуків тощо. Однак, таке поширення неправдивої інформації стосовно членів сім'ї фізичної особи повинно порушувати особисті саме цієї фізичної особи.

Відповідно до п. 12 Постанови Пленуму ВСУ у справах про захист гідності та честі фізичної особи, а також ділової репутації

фізичної та юридичної особи немайнові права, належним відповідачем у разі поширення оспорованої інформації в мережі Інтернет є автор відповідного інформаційного матеріалу та власник веб-сайту, особи яких позивач повинен установити та зазначити в позовній заяві.

Якщо автор поширеної інформації невідомий або його особу та/чи місце проживання (місцезнаходження) неможливо встановити, а також коли інформація є анонімною і доступ до сайту — вільним, належним відповідачем є власник веб-сайту, на якому розміщено зазначений інформаційний матеріал, оскільки саме він створив технологічну можливість та умови для поширення недостовірної інформації.

Дані про власника веб-сайту можуть бути витребувані відповідно до положень Цивільного процесуального кодексу України в адміністратора системи реєстрації та обліку доменних назв та адреси українського сегмента мережі Інтернет.

Водночас, відповідно до положень Цивільного процесуального кодексу України позивач у вказаній категорії справ має належним чином довести, що поширена про нього недостовірна інформація є саме фактичним твердженням, а не оціночним судженням.

Відповідно до ст. 30 Закону України «Про інформацію» ніхто не може бути притягнутий до відповідальності за висловлення оціночних суджень. Оціночними судженнями, за винятком наклепу, є висловлювання, які не містять фактичних даних, критика, оцінка дій, а також висловлювання, що не можуть бути витлумачені як такі, що містять фактичні дані, зокрема з огляду на характер використання мовно-стилістичних засобів (вживання гіпербол, алегорій, сатири). Оціночні судження не підлягають спростуванню та доведенню їх правдивості.

Якщо особа вважає, що оціночні судження або думки принижують її гідність, честь чи ділову репутацію, а також інші особисті немайнові права, вона вправі скористатися наданим їй законодавством правом на відповідь, а також на власне тлумачення справи у тому самому засобі масової інформації з метою обґрунтування безпідставності поширених суджень, надавши їм іншу оцінку.

Якщо суб'єктивну думку висловлено в брутальній, принизливій чи непристойній формі, що принижує гідність, честь чи ділову репутацію, на особу, яка таким чином та у такий спосіб висловила думку або оцінку, може бути покладено обов'язок відшкодувати завдану моральну шкоду.

За поширення недостовірної інформації особу може бути притягнуто до цивільно-правової відповідальності, а шкода, завдана таким розповсюдженням, може бути нанесена як фізичній так і юридичній особі.

Якщо особа, яка розповсюдила недостовірну інформацію, відмовляються її спростувати, а також компенсувати матеріальну та (або) моральну шкоду, особа, стосовно якої поширено таку інформацію, має право на захист своїх прав та інтересів шляхом звернення до суду.

До вимог про спростування недостовірної інформації, поміщеної у засобах масової інформації, застосовується позовна давність в один рік, яка обчислюється від дня поміщення цих відомостей у засобах масової інформації або від дня, коли особа довідалася чи могла довідатися про ці відомості (п. 2 ч. 2 ст. 258 Цивільного кодексу України).

В деяких випадках до винної особи може бути застосована адміністративна відповідальність за поширювання неправдивих чуток, що можуть викликати паніку серед населення або порушення громадського порядку, що тягне за собою накладення штрафу від десяти (170 грн.) до п'ятнадцяти (255 грн.) неоподатковуваних мінімумів доходів громадян або виправні роботи на строк до одного місяця з відрахуванням двадцяти процентів заробітку (ст. 173 Кодексу України про адміністративні правопорушення).[1]

Отже, реалізація прав і свобод людини і громадянина, а також захист їх від недостовірної інформації в інтернеті, наразі, належним чином не відбувається, адже складно розібратися у кожному випадку порушення прав та розповсюдження недостовірної інформації. Але, не зважаючи на складність такого процесу, в законодавстві України все ж існує відповідальність за поширення такої інформації, що відповідає нашому демократичному та прогресивному розвитку.

Список використаної літератури:

1. ВІДПОВІДАЛЬНІСТЬ ЗА РОЗПОВСЮДЖЕННЯ НЕДОСТОВІРНОЇ ІНФОРМАЦІЇ [Електронний ресурс] // Міністерство Юстицій. 2020. Режим доступу до ресурсу: <https://minjust.gov.ua/m/vidpovidalnist-za-rozprovsyudjennya-nedostovirnoi-informatsii>.

2. Гончаренко Є. Розповсюдження недостовірної інформації в мережі Інтернет: як захистити свої права? [Електронний ресурс]. 2021. Режим доступу до ресурсу: <https://blog.liga.net/user/yehoncharenko/article/40027>.

3. Закон України «Про інформацію» від 02.10.1992 № 2657-ХІІ [Електронний ресурс]. Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.

Лаптева Т. О.

Phd-аспірантка Київського
національного університету імені
Тараса Шевченка

МЕТОДИ ВИЯВЛЕННЯ ТА ПРИПИНЕННЯ РОЗПОВСЮДЖЕННЯ НЕДОСТОВІРНОЇ ІНФОРМАЦІЇ В ІНТЕРНЕТЕ

Світова спільнота всерйоз стурбована розповсюдженням у мережі інформації, яка не відповідає дійсності. Ситуація навколо коронавірусу показала важливість припинення фейкових повідомлень: за безневинними і безглуздими чутками з'являються потенційно небезпечні для життя і здоров'я людей теорії змови[1]. Провідну роль розповсюдженні фейків грають соцмережі і месенджери, де фактчекінгу приділяється значно менше уваги, ніж було б. З метою припинення розповсюдження недостовірної інформації, найефективнішою буде повноцінна участь усіх органів влади та чиновників різного рівня щодо висвітлення своєї діяльності у соціальних мережах. Потрібно більше інформаційної відкритості, більше розмов із людьми, більше контенту, більше новин. Це породжує атмосферу довіри до новин, і це буде найкращою відсіч розповсюдженню такого роду інформації. Суть проблеми полягає

в тому, що у людей просто недостатньо інформації, або вона написана незрозумілою мовою, не дається достатньо роз'яснень, і на цьому тлі таки виникають всі ці спекуляції.

Виклад основного матеріалу

У сучасних умовах, коли будь-хто може поширити будь-які відомості практично зі швидкістю світла, необхідність факчекінгу та контролю за недостовірною інформацією стає нагальною необхідністю. Необдумані заяви, чутки та плітки, а іноді й навмисна брехня формують думки мільйонів людей, і відрізнити правду від брехні часом не в змозі навіть професіонали. Великі ІТ-корпорації, такі як Google, Facebook і Twitter, анонсують запуск нових інструментів боротьби з фейками та іншими деструктивними відомостями, проте жоден з цих механізмів поки не довів своєї ефективності.

Як зазначають експерти, модерація контенту в іноземних соцмережах найчастіше здійснюється упереджено, тобто над алгоритмами переважають людський чинник та захист власних політичних чи комерційних інтересів [2]. Так, у мережі регулярно публікуються відомості, що дискредитують українські здобутки у галузі науки, спорту, космічної програми чи військових заслуг. Щоб не допустити спотворення образу держави, було ухвалено рішення про розробку програми протидії фальсифікаціям та спотворенням вітчизняної історії.

На мою думку, подібний дата-сервіс зможе зіставляти «максимальну кількість фактів, які стосуються повідомлення» та виявляти невірні. Під час перевірки агрегатор врахує авторитетність джерела, час публікації та додані фото та/або відео. Сервіс повинен допомогти автоматизувати пошук авторів та розповсюджувачів дезінформації в мережі, а значить підвищити швидкість реагування на подібний контент. Передбачається, що вітчизняна розробка, аналог якої поки що не вдалося створити навіть Facebook, буде доступна як приватним користувачам та компаніям, так і наглядовим відомствам.

На даний час нашими науковцями, планується розробка моделі та методів виявлення недостовірної інформації в інформа-

ційному просторі на основі експертно-машинних методів ранжування в умовах інформаційного протиборства для захисту інформаційних ресурсів організації та підприємств. Дане наукове завдання має суттєве для розробки методів виявлення недостовірної інформації в інформаційному просторі в умовах інформаційного протиборства.

Вважається, що найнебезпечніші технології майбутнього – насправді майже сьогодення – це дипфейки, тобто фейки, що створюються нейромережею. Йдеться про відео та аудіозаписи, на яких нібито відомі люди роблять різні фейкові заяви. Такі фейки генеруються за допомогою штучного інтелекту, зазначає експерт [3,4]. У найближчому майбутньому ця технологія, призведе до збільшення злочинів. І не економічних, а якихось інших. І може реально стати інструментом терористів.

Державні органи в принципі почали задумуватись про боротьбу з поширенням інформації деструктивного характеру, але вони, ні бачать низку потенційних проблем при реалізації пропозицій. «Навіть Facebook намагається вже не перший рік створити якусь «машинку», якийсь алгоритм, який займатиметься боротьбою з фейками. Я вважаю, що поки це зробити досить складно, бо якщо говорити про український сегмент, то самих фейків ще не так багато, щоб алгоритм міг звіряти, оцінювати. Коли двигун працює, він звіряється з базою даних. А для самої бази даних ще не так багато інформації.

Зрозуміло, зазначені труднощі не означають, що від вирішення проблеми потрібно відмовитись – просто рішення буде не таким простим, як хотілося. Оскільки з кожним роком виявити дипфейки буде все важче, згодом люди просто перестануть довіряти будь-якій інформації. Тому що розібратися, що правда, що брехня буде неможливо. І ось тоді будуть потрібні нові способи передачі даних та новин. Це найсерйозніший виклик нашого часу, і хто відповість на нього першим, той переможе.

Висновки

Проведене дослідження, та запропонований метод виявлення та припинення недостовірної інформації в Інтернеті показало, щоб

зорієнтуватися у світі інформації та вміти відокремлювати достовірну інформацію від недостовірної, необхідно виконати такі дії:

1) володіти навичками грамотного пошуку інформації чітко уявляти, що треба знайти у мережі, правильно формулювати пошуковий запит;

2) дослідити джерела інформації;

3) навчитися критично відбирати та оцінювати інформацію;

4) вміти перевіряти фактичні помилки;

5) порівнювати зміст, закладений в інформаційному повідомленні зі своїми базовими знаннями з тієї чи іншої проблеми, у разі їх нестачі звертатися до додаткової літератури, інших джерел інформації;

6) систематизувати інформацію, шукати прихований зміст.

Публікувати відповідь-спростування на фейк потрібно на тій же платформі, де він з'явився, причому не через добу-дві, а протягом двох годин. «Потрібно відстежувати цю інформацію, потрібно постійно перебувати на зв'язку та в контакті».

На мою думку, найкращим варіантом будуть комплексні заходи щодо боротьби з поширенням хибної інформації. І одним із способів боротьби з брехнею має стати правда.

Література

1. Юдін О. К., Бучик С. С. Концептуальний аналіз уразливості державних інформаційних ресурсів. Наукоємні технології. 2013. № 3(19). (Технічні науки). С. 299-304

2. Тенденції розвитку системи інформаційної безпеки України [Електронний ресурс]. Бібліофонд. – Режим доступу: <http://bibliofond.ru/view.aspx?id=652263>

3. Михайлов А. П., Петров А. П., Прончева О. Г. Математическое моделирование информационного противоборства в эпоху Интернета. Труды XVIII Всероссийской конференции Научный сервис в сети Интернет, 2016. С. 264-270.

4. Дудатьєв А. В., Войтович О. П. Інформаційна безпека соціотехнічних систем: модель інформаційного впливу. Інформаційні технології та комп'ютерна інженерія, 2017. №10. С. 16-21

5. Кузнецова А. П., Монахова Г. Е., Монахов М. Ю. Репутация Интернет-источников данных в информационно-аналитической деятельности администратора безопасности. Динамика сложных систем – XXI век Т.10, №4, 2016. С.78-81

Шикір Д. О.

студент Інституту права Київського
національного університету імені
Тараса Шевченка

УДОСКОНАЛЕННЯ НАДАННЯ АДМІНІСТРАТИВНО- ІНФОРМАЦІЙНИХ ПОСЛУГ В УМОВАХ ДІДЖИТАЛІЗАЦІЇ

Світова практика надання адміністративних послуг публічною адміністрацією – це перш за все якість, швидкість, зручність обслуговування громадян і надання якомога більше послуг он-лайн за допомогою е-сервісів. Тому, говорячи про реформи у сфері надання адміністративних послуг, варто розуміти мету, яку переслідує держава щодо вдосконалення сервісної діяльності публічною адміністрацією. Мета є простою: з одного боку, спростити порядки (процедури) отримання послуги, з іншого, підвищити якість обслуговування.

На мою думку, досягнути цю мету можна шляхом координації зусиль у трьох напрямках: 1) розроблення й запровадження нових е-сервісів, а саме діджиталізації адміністративних послуг; 2) максимального наближення адміністративних послуг, зокрема децентралізації адміністративних послуг; 3) вдосконалення системи моніторингу якості обслуговування у ЦНАПах.

У вересні 2019 р. Президентом України було запропоновано низку шляхів удосконалення систем надання адміністративних послуг, у результаті чого був виданий Указ Президента «Про деякі заходи із забезпечення надання якісних публічних послуг», яким було затверджено деталізований перелік заходів, які необхідно впроваджувати органам публічної адміністрації, та доручено Ка-

бінету Міністрів України (далі – КМУ) забезпечити їх реалізацію [1].

На виконання заходів, спрямованих насамперед на діджиталізацію послуг, окреслених у цьому Указі, було розроблено Концепцію «Держава у смартфоні», що надалі трансформувалась у Концепцію «Цифрова держава». Концепція містить конкретні практичні кроки, зокрема низку пілотних проєктів, наприклад он-лайн-сервіс «Дія» – сайт, а згодом і мобільний застосунок, які об'єднують в єдиному електронному вікні всі послуги, що надає держава громадянам і бізнесу [2, с. 26].

На сьогодні концепція «Цифрова держава» передбачає реалізацію таких проєктів:

- e-Health, електронної системи охорони здоров'я, що запроваджується з метою отримання максимально можливої кількості медичних послуг он-лайн.
- створення у структурі КМУ Міністерства цифрової трансформації, що відповідає за впровадження електронного урядування задля прозорості, доступності державних послуг і мінімізації корупції.
- повноцінне запровадження онлайн-сервісу «Дія», в межах якого можна отримати державні послуги у сферах реєстрації бізнесу, будівництва й соціального захисту тощо.
- проєкт «e-Малютко», який надаватиме послуги реєстрації народження дитини та її місця проживання, реєстрації немовляти в ЕСОЗ, отримання фінансової допомоги в разі народження дитини, отримання посвідчення дитини та батьків з багатодітної сім'ї та інші важливі проєкти [2].

Незважаючи на позитивну статистику світові практики надання адміністративних послуг постійно модернізуються саме в бік розроблення нових е-сервісів, які оптимізують процес отримання послуги.

Перспективи діджиталізації адміністративних послуг за планом Міністерства цифрової трансформації – переведення за п'ять років 100% адміністративних послуг в он-лайн, з яких 20% – без втручання чиновників, у повному автоматичному режимі.

Так, міністр цифрової трансформації Михайло Федоров указує, що діджиталізація на місцевому рівні функціонування публічної адміністрації передбачає надання адміністративних послуг на базі ЦНАПів, які планується реорганізувати в центри «Дія». Своєю чергою центр «Дія» повинен стати офісом застосунку та сайту Міністерства цифрової трансформації, щоб коли людина прийде до Центру в селищі чи в місті, там не бігали й не носили папери, а просто відкривався портал і адміністраторка надавала цю послугу [3, с. 46].

Однак, говорячи про діджиталізацію послуг, треба розуміти, що діджиталізація передбачає не лише переведення 100% публічних послуг для пересічних громадян і бізнесу в он-лайн, а насамперед забезпечення 100% населених пунктів і їх соціальних об'єктів доступом до високошвидкісного Інтернету й залучення мільйонів українців до програми розвитку цифрових навичок і компетенцій.

З цього приводу в межах діджиталізації адміністративних послуг варто відзначити запровадження органами публічної адміністрації та іншими державними органами е-сервісів «Електронний кабінет» (наприклад, «Кабінет ужгородця», «Електронний кабінет водія» та інші). Разом із тим зараз триває процес автоматизації ЦНАПів, що охоплює систему «Електронна черга», «Електронний запис до ЦНАП», системи електронного документообігу («Універсам послуг»), он-лайн-консультування, відеонагляду, звукозапису [4, с. 45].

У контексті реформи судочинства Міністерство юстиції України запровадило е-сервіс «Електронний суд», який спрямований на удосконалення процедур розгляду справ, зокрема публічно-правових спорів і справ про адміністративні правопорушення, а також інших категорій юридичних справ шляхом надання таких е-послуг, як сплата судового збору он-лайн, надсилання процесуальних документів електронною поштою учасникам судового процесу, отримання інформацій щодо стадій розгляду справ, доступ до єдиних реєстрів судових рішень, надсилання судових повісток СМС-повідомленнями.

Говорячи ж про перспективи удосконалення практик надання адміністративних послуг у частині децентралізації послуг, в першу чергу варто відзначити співпрацю об'єднаних територіальних громад (далі – ОТГ) за програмою «U-LEAD з Європою», що передбачає технічну й методологічну підтримку створення й облаштування ЦНАПів спеціалізовано ІТ (комп'ютерною технікою) та меблями й під'єднання ОТГ до програмного комплексу автоматизованої роботи ЦНАП «Вулик».

Відносно системи моніторингу якості обслуговування варто відзначити окремі практики вдосконалення зворотного зв'язку. Зокрема, це запровадження проекту «Таємний клієнт» на вебсайті ГСЦ МВС, який передбачає заповнення розділів он-лайн-анкети клієнтом сервісного центру МВС на предмет оцінювання за встановленою шкалою окремих процесів обслуговування в сервісних центрах. Вважаю, що варто продукувати практику сервісних центрів МВС стосовно е-сервісу «Таємний клієнт» іншим органам публічної адміністрації, зокрема розробляти е-сервіси, які б надали змогу відвідувачам ЦНАПів критично оцінювати процес обслуговування й подавати власні пропозиції щодо вдосконалення окремих процесів роботи ЦНАПу [5, с. 17].

Таким чином, сучасний стан діяльності публічної адміністрації щодо надання адміністративних послуг в Україні дає змогу констатувати вдосконалення практик сервісної діяльності в площині діджиталізації, децентралізації та моніторингу якості обслуговування. Тому певною мірою можна стверджувати, що практика надання адміністративних послуг є однією з форм взаємодії органу публічної адміністрації з громадськістю.

Проте найперспективнішим напрямом удосконалення практик надання адміністративних послуг, на мою думку, є діджиталізація, оскільки відповідний напрям дає змогу модернізувати шляхом комп'ютеризації (запровадження е-сервісів) процедуру звернення й отримання послуги. Більше того, застосування е-сервісів обумовлюватиме розвиток процесу електронного документообігу в органах публічної адміністрації, у тому числі подальшу автоматизацію мережі ЦНАПів.

Джерела використаної літератури:

1. Про деякі заходи із забезпечення надання якісних публічних послуг : Указ Президента України від 4 вересня 2019 р. № 647/2019. URL : <https://www.president.gov.ua/documents/6472019-29441>.
2. Федоров розповів, коли запуснуть «державу в смартфоні». URL : <https://nv.ua/ukr/biz/tech/derzhava-v-smartfonidata-zapusku-novini-ukrajini-50055307.html>.
3. Сервіс без чиновників. Як буде виглядати і працювати «державна в смартфоні» Зеленського. URL : <https://www.epravda.com.ua/publications/2019/09/30/652085/>.
4. Державні послуги онлайн. URL: <https://plan.diia.gov.ua/>.
5. Реформу адмінпослуг необхідно продовжувати одночасно за 5 напрямками – експерт. URL: <https://www.ukrinform.ua/rubric-regions/2752747-reformu-adminposlugneobhidno-prodovzuvati-odnocasno-za-5-napramkami-ekspert.html>.

Ворона Ю. С.

курсант Дніпропетровського
державного університету внутрішніх
справ

Миронюк Р. В.

викладач кафедри адміністративного
права, процесу та адміністративної
діяльності Дніпропетровського
державного університету внутрішніх
справ

НЕОБХІДНІСТЬ ЗАПРОВАДЖЕННЯ МЕДІАЦІЇ У АДМІНІСТРАТИВНЕ СУДОЧИНСТВО

У сучасному українському суспільстві наявна сформована ідея про судові вирішення будь-яких питань, даний аспект призводить до перевантаженості суду та затягування розгляду провадження. Саме тому важливим аспектом для нашого суспільства на даному етапі виступає впровадження поняття медіації у даний процес.

Необхідно зазначити, що для України судова медіація є новим видом вирішення конфліктів, в той час, коли в зарубіжних країнах вона вже досягла значного успіху в своєму використанні. Так, медіація в адміністративному процесі вже активно застосовується в США, Австралії, деяких країнах Європи, серед яких Німеччина та Голландія.

Саме тому ми повинні наголосити на тому, що на сьогодні доцільно використовувати практику інших держав з метою врегулювання даного питання у законодавстві нашої країни.

Відтак вивчаючи дану тематику ми повинні зазначити, що поняття медіації у сучасному законодавстві нашої країни відсутнє. Тому ми пропонуємо звернути особливу увагу визначення що пропонує нам такий науковець, як Самохвалов В. П., а саме це процес врегулювання конфлікту за допомогою медіатора, який виступає третьою стороною з метою взаємовигідного та добровільного результату [1].

Вивчаючи даний аспект ми не можемо оминати увагою той аспект, що відповідно до статті 180 Кодексу адміністративного судочинства України, суддя у ході підготовчого провадження повинен з'ясувати чи бажають сторони врегулювати даний спір шляхом примирення, та надати їх строк для його врегулювання[2]. Ми вважаємо дане твердження не зовсім логічним, оскільки медіація має на увазі розв'язання спору без участі судді. Саме тому доцільно було б надати можливість сторонам до підготовчого провадження врегулювати даний спір шляхом укладення мирової угоди. У такому разі ми пропонуємо зобов'язати сторони до початку підготовчого провадження надіслати до суду заяву про завершення розгляду провадження за досягнення ними згоди.

Ми повинні зауважити, що даний аспект значно полегшить розгляд справ, оскільки особам котрі бажають врегулювати даний спір можливо буде це зробити до початку розгляду справи, що зекономить не лише час учасників, але й насамперед розвантажить суди.

Також вивчаючи даний аспект більш детально ми розуміємо, що в нашій державі відсутній механізм поза судового врегулюван-

ня спору, саме тому ми наголошуємо на необхідності впровадження до законодавства нашої країни саме даного аспекту. Відтак ми наголошуємо на необхідності визначення хто саме та за яких умов може розглядати дані спори та укладати договір примирення. Також важливим аспектом на нашу думку виступає визначення процесуального статусу даного договору, ми пропонуємо прирівняти його за статусом до рішення суду, з метою уникнення проблемних питань в даному аспекті.

Відтак ми можемо дійти висновку, що на сьогодні необхідно впроваджувати систему медіації у законодавчу базу нашої держави, а також більш якісно надавати тлумачення нормам та прописати у законодавстві випадки коли особа має право розглядати справу у позасудовому порядку. Також необхідно зауважити, що необхідно закріпити саме поняття медіація, а також визначити хто саме може її проводити.

Література:

1. Самохвалов В. П. Медіація як інститут відносного й примирного правосуддя. Перспективи застосування альтернативних способів вирішення спорів (ADR) в Україні : матеріали II Львів. міжнар. форуму. Львів, 2009. С. 175–178.
2. Кодекс адміністративного судочинства України : закон України від 06.07.2005, № 2747-IV, поточна редакція 05.08.2021, URL : <https://zakon.rada.gov.ua/laws/show/2747-15#top> (дата звернення : 24.11.2021)

Малиш Н. В.

курсант Дніпропетровського
державного університету внутрішніх
справ

Науковий керівник: Мітусова К. С.

викладач кафедри цивільного права
та процесу Дніпропетровського
державного університету внутрішніх
справ

СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ ПРАВОВОГО РЕГУЛЮВАННЯ ДИСТАНЦІЙНОЇ ПРАЦІ

Розвиток світу у ХХІ столітті характеризується активним удосконаленням у різних сферах життя цифрових технологій, електронних мереж, що є важливим чинником існування постіндустріального суспільства. Це зумовило появу нових можливостей для реалізації прав людини у сфері соціально-трудових відносин. По суті, створюються передумови для віртуалізації економічного простору, поєднаного з реальною соціальною взаємодією учасників суспільно-правових відносин. Збільшення масштабів використання мережі Інтернет, мобільного й електронного зв'язку, відеоконференцій зумовлене й новими неочікуваними причинами, зокрема поширенням у світі пандемії COVID-19, потребою дотримання людьми соціальної дистанції тощо. Цілком очікувано, що все більше працівників і роботодавців надають пріоритет нетиповим формам організації праці. Це дає змогу більш гнучко планувати й організовувати свій робочий час, використовувати творчі здібності та навички самоорганізації, розширювати можливості для додаткового заробітку. Наслідком розвитку цифрових технологій є поширення нестандартних форм зайнятості, серед яких – дистанційна, віддалена робота, що постійно збільшується за масштабами використання [1, с. 234].

Становлення ринкових відносин на пострадянському просторі спричинило суттєву трансформацію концепції стабільних трудо-

вих відносин. Зміни в економіці та суспільстві, зокрема зменшення питомої ваги великих промислових підприємств, що практикували використання традиційно організованої праці з наданням робочого місця, суворим обліком і контролем робочого часу та необхідністю щоденного відвідування роботи, розвиток малого й середнього бізнесу, спрямованого на створення інноваційних і технологічних продуктів, призводить до зміни форм і методів залучення громадян на ринок праці. У правовому регулюванні трудових відносин посилюється гнучкість, для характеристики якої використовується термін «флексибілізація» [2, с. 24]. Формами її прояву називають поширення атипових трудових договорів, зокрема, на умовах неповного робочого часу з працівниками агентств тимчасової зайнятості (роботи), економічно залежними, самозайнятими, домашніми працівниками, телепрацівниками тощо. Серед цих форм зайнятості дистанційна праця набула поширення. Для її позначення використовуються різні терміни, зокрема телепраця, тобто різновид трудової діяльності, що виконується поза межами центрального офісу, що виключає можливість безпосереднього контакту працівника з його керівниками та колегами по службі [3, с. 113].

Утім як правовий феномен дистанційна праця в Україні перебуває на стадії становлення, хоча в багатьох країнах світу вона набула поширення й становить серйозну конкуренцію усталеним формам зайнятості [4, с. 101; 5, с. 466]с. Легальне визначення дистанційної праці законодавець спробував надати, уносячи зміни до Кодексу законів про працю України (далі – КЗпП) на підставі 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)» від 30.03.2020 № 540-IX (далі – Закон № 540-IX). Так, відповідно до ч. 10 ст. 60 КЗпП, дистанційна (надомна) робота – це форма організації праці, при якій робота виконується працівником за місцем його проживання чи в іншому місці за його вибором, у тому числі за допомогою інформаційно-комунікаційних технологій, але поза приміщенням роботодавця. На перший

погляд не доміком цієї дефініції є змішування категорій «дистанційна» й «надомна» праця, які за своєю сутністю та характеристиками суттєво різняться [1, с. 235–238]. Варто зауважити, що в літературі відсутня єдність поглядів на дистанційну працю. Серед ознак дистанційної зайнятості А. М. Колот найважливішими називає віддаленість робочого місця, ненормований робочий час, віртуальність середовища, у якому протікає трудова діяльність, використання інформаційних і комунікаційних технологій, гнучкість соціально-трудова відносин. Дистанційна зайнятість – це нестандартна форма зайнятості, яка заснована на гнучких соціально-трудова відносинах між працівником і роботодавцем і відбувається у віртуальному середовищі з використанням інформаційних і комунікаційних технологій [6, с. 6].

На переконання О. О. Герасименко, дистанційну зайнятість правомірно розглядати не лише з позицій нестандартності, а й під кутом зору інноваційності, оскільки така форма соціально-трудова відносин передбачає комплекс нововведень щодо взаємодії держави, найманих працівників, роботодавців, яка на практиці породжує низку соціально-економічних зисків і загострює організаційно-правову визначеність [7, с. 229].

Беззаперечно, дистанційна праця має як позитивні, так і негативні наслідки для учасників трудових правовідносин. Застосування дистанційної зайнятості, як показав досвід запровадження карантину в Україні навесні 2020 року, дає можливість суттєво зменшити виробничі витрати роботодавців на організацію праці, оренду й утримання офісних приміщень. На працівників частково були перекладені витрати на ресурси, зокрема електроенергію, зв'язок, воду. Менше обов'язків мають роботодавці в питаннях охорони праці, оскільки ними фактично перекладено на самих працівників обов'язки з організації охорони праці, забезпечення здорових і нешкідливих умов праці. Та й навряд чи можливо забезпечити в помешканні працівника, що має інше цільове призначення, рівень виробничої безпеки, призначений для промислових чи офісних будівель. Водночас роботодавці можуть повноцінно використовувати здатність особи до праці, устанавлюючи вироб-

ничі завдання й підтримуючи ефективну комунікацію всередині колективу. З'являється можливість розширити межі підбору персоналу за рахунок осіб, зацікавлених у неповному робочому дні й частковій зайнятості, зокрема з частковою зайнятістю. Крім того, фактично в безкоштовне користування отримані сучасні канали комунікації, наприклад, соціальні мережі або месенджери.

Поширення дистанційної зайнятості має позитивні сторони й для працівників. Зокрема, це запобігає звільненню тих, хто з певних причин не може надовго полишати помешкання, опікуючись непрацездатними членами сім'ї або дітьми. За певних умов, виключаючи безпосередній контакт між працівниками, дистанційна робота може запобігати проявам мобінгу та іншим проявам дискримінаційних дій. Позитивним моментом є доступність цієї форми зайнятості для різних категорій населення, передусім для осіб з обмеженими можливостями, людей, які не можуть відлучитися з дому на тривалий час. Важливу роль дистанційна праця може відігравати й у розширенні транскордонної мобільності робочої сили, коли можливість працювати на іноземного працедавця не пов'язана з вимушеною еміграцією та отриманням дозволів на працевлаштування в іншій країні. Пропонується укладати трудові договори про дистанційну роботу в письмовій формі на підставі типової форми, затвердженої центральним органом виконавчої влади, що забезпечує формування державної політики у сфері трудових відносин. На нашу думку, ухвалення саме типової форми договору є неприйнятним. По суті, вона є нормативно-правовим актом і сторони не зможуть її змінювати, а лише доповнювати. Це суттєво скорочує можливості індивідуалізації змісту трудових відносин у кожному конкретному випадку.

При виконанні дистанційної роботи працівник самостійно обирає власне робоче місце та персонально відповідатиме за забезпечення безпечних і нешкідливих умов праці на ньому. При цьому на роботодавця покладається обов'язок проводити інструктажі з охорони праці та протипожежної безпеки, пов'язані з використанням інформаційно-комунікаційних технологій. Проте багато питань залишає запропонована форма підтвердження факту

проведення інструктажів шляхом обміну електронними документами, адже відсутність широкого поширення електронних довірчих послуг не забезпечує достовірності спілкування.

Цілком очевидно, що подальший розвиток трудового права України в умовах відсутності кодифікованого нормативного акта, що забезпечує комплексне регулювання трудових відносин, є досить ускладненим. Тому нагальним завданням, яке буде вирішуватися під час кодифікації трудового законодавства, є забезпечення єдності правового регулювання праці в частині гарантування основних трудових прав працівників, у т. ч. дистанційних, із широкими можливостями для диференціації правового регулювання дистанційної праці. При цьому важливо спиратися як на позитивний досвід інших країн, що вже мають досвід такого регулювання, так і на визнані міжнародні стандарти. Нагальним же є посилення договірних засад щодо регламентації дистанційної праці за допомогою впровадження примірної форми трудового договору з дистанційним працівником, яка може прийматися за основу під час укладення відповідних трудових договорів.

Список використаних джерел:

1. Герасименко О. О., Щетініна Л. В., Рудакова С. Г. Дистанційна зайнятість: сучасні тренди організації та оплаті праці. БізнесІнформ. 2017. № 11. С. 233–239.
2. Морозов П. Е. Современные тенденции развития зарубежного трудового права в условиях глобализации : монография. Москва : Проспект, 2016. 256 с.
3. Киселев И. Я. Новый облик трудового права стран Запада (прорыв в постиндустриальное общество). Москва : ЗАО «Бизнес-школа «Интел-Синтез», 2003. 160 с.
4. Вапнярчук Н. М. Дистанційна зайнятість: Проблеми правового регулювання. Право та інновації. 2016. № 1. С. 101–106.
5. Колот А. Трансформація інституту зайнятості як складова глобальних змін у соціально-трудої сфері. Україна: аспекти праці. 2009. № 8. С. 3–14.

6. Герасименко О. О. Дистанційна зайнятість тренд цифрової економіки: нові можливості, нові соціальні ризики. Сфера зайнятості і доходів в умовах цифрової економіки: механізми регулювання, виклики та домінанти розвитку : збірник тез доп. учасників Міжнар. наук.-практ. конф., (Київ, 23–24 жовт. 2019 р.). Київ : КНЕУ, 2019. С. 228–231.

Кукурік А. В.

студентка НТУУ «КПІ ім. Ігоря Сікорського»

Науковий керівник: Головка О. М.

кандидат юридичних наук, старший викладач кафедри інтелектуальної власності та приватного права, НТУУ «КПІ імені Ігоря Сікорського»

ВТІЛЕННЯ ВІДНОВНИХ ПРАКТИК ПІД ЧАС ПАНДЕМІЇ COVID-19

Останнім часом потенціал відновних практик, зокрема медіації, починає зростати, завдяки стимулюванню інтересу широкого загалу населення шляхом ЗМІ, а також ознайомлення урядів держав з відносно новим методом врегулювання конфліктів за допомогою міжнародних документів, наприклад, тієї ж Рекомендації N R (99) 19 Комітету міністрів Ради Європи державам – членам Ради, які зацікавлені в організації медіації у кримінальних справах, яка виділяє «використання медіації у кримінальних справах як гнучке, всеохоплююче, спрямоване на вирішення проблем доповнення, або як альтернативу традиційному судовому розгляду» [1]. З'являються нові методи врегулювання конфліктів, виникнення яких обумовлено необхідністю появи альтернативи у реагуванні на протиправні дії учасників правовідносин, яка покликана доповнити офіційне правосуддя шляхом використання окремого способу владнання спірних ситуацій. Офіційне правосуддя не завжди може дійсно примирити сторони конфлікту та усунути спричинену шкоду, тобто нечасто сповна забезпечується консенсус між сторонами.

Для того аби вирішити спір почали використовувати медіацію – одну з технологій урегулювання зіткнення інтересів за участі третьої нейтральної сторони. Медіація може бути застосована для вирішення будь-якого спору і навіть тоді, коли справа по розв'язанню спору знаходиться у суді. Основними принципами методу є: добровільність участі, свобода виходу з процесу медіації для всіх учасників; конфіденційність зустрічі та обмеження доступу до інформації; нейтральність, безсторонність та незалежність медіатора [2, с. 3]. Перевагою зазначеного способу є те, що за мету взято досягнення спільного рішення та відновлення справедливості шляхом участі обох сторін у процесі. Позитивною рисою є також економія таких ресурсів як: час, кошти та сили, вона сприяє полегшенню роботи судів, які не справляються з тією кількістю справ, яка до них надходить, за допомогою неї вони зможуть не відкривати провадження у справі і не витратити на них багато часу. Оскільки медіація може бути застосована вже на ранній стадії спору, то врегулювання конфліктів відбувається значно швидше, ніж у суді.

Розвиток відновних практик почав помітно зростати, але на шляху впровадження практичного застосування відносно нового методу вирішення конфліктів постала непередбачена ситуація, яка потребує оперативного реагування та підводить до роздумів щодо можливості використання інноваційних заходів у судовій системі. Пандемія COVID-19 змінила сучасну реальність, поставивши серйозну проблему соціальної та економічної стабільності, а також захисту прав та інтересів кожного з нас. Хоча система правосуддя через епідемію стала повільною, вона все рівно має продовжувати вирішувати суперечки та захищати права сторін. Найкращим вибором для сторін сьогодні є відновлення вирішення спорів шляхом посередництва або інших форм альтернативного вирішення суперечок.

Пандемія COVID-19 є новим викликом для суспільства і потребує серйозних змін у судовій системі, щоб відповідати принципам, викладеним у Загальній декларації прав людини, особливо статті 8, яка визначає право кожної людини на ефективне поновлення у

правах компетентними національними судами в разі порушення її основних прав, наданих їй конституцією або законом [3].

Поширення пандемії COVID-19 на території України показує, що наявність непередбачених факторів, впливає на судові процеси, які в свою чергу значно втрачають свою ефективність. Через карантинні обмеження судова влада не має змоги справлятися з навантаженнями, але як вже зазначалося вище, альтернативою вирішення даної проблеми є медіація, за допомогою якої можна вирішувати спірні питання дистанційно, тим самим дбаючи про здоров'я населення. На державі лежить обов'язок забезпечення своїх громадян гарантією встановлення чітких прав та обов'язків у всіх можливих суспільних відносинах, що виникають. Відповідно, при виникненні концептуально нових суспільних відносин, таких, наприклад, як інформаційні, їх необхідно врегульовувати відповідними правовими нормами. Держава, встановлюючи права, обов'язки та відповідальність у новій сфері правовідносин, виконує свій початковий обов'язок – врегулювання суспільних відносин загальноприйнятими правилами поведінки. [4, с. 82] Враховуючи розвиток інформаційних технологій, процедура впровадження медіації в онлайн режим здається нескладною, але все ж таки тут є свої переваги та недоліки.

По-перше, проблемою є те, що в Україні бракує законодавчих положень щодо можливості процедур посередництва, таким чином ускладнюється доступ до отримання судової допомоги великою кількістю людей. Тому було б непогано прийняти Закон України «Про медіацію». Закон повинен передбачати медіацію в мережі, містити в собі її визначення, а також повноваження медіаторів та сторін.

Тим більше у законодавстві ЄС вже давно передбачені положення про медіацію. Декларація «Вивчені уроки і виклики, з якими стикнулась судова влада протягом і після пандемії COVID-19» містить в собі важливі принципи, серед яких є принцип доступу до правосуддя, який говорить про те, що: «Функціонування правосуддя як державної послуги необхідно якомога більше підтримувати, включаючи забезпечення доступу до правосуддя іншими

альтернативними засобами такими, як онлайн-послуги або надання інформації через веб-сайти суду та інші засоби комунікації (телефон, електронна пошта тощо). Більш широкі консультації та координація з усіма фахівцями у сфері правосуддя (включаючи адвокатів, працівників виконавчої служби, медіаторів та працівників соціальних служб) допоможуть забезпечити належний рівень доступу до правосуддя.» [5, с. 22].

По-друге, онлайн переговори можуть переноситися через технічні перешкоди, так як платформи, на яких проводять відео-конференції можуть містити певні обмеження, і взагалі вони не є досить надійними, так як комунікація може перерватися у будь-який важливий момент.

По-третє, труднощі можуть виникнути через відсутність окремої платформи задля проведення переговорів. На сьогоднішній день існує безліч арен для проведення онлайн конференцій, зокрема ZOOM, Google Meet, TrueConf, Skype і т.д., але все ж таки варто проаналізувати, які технології та онлайн-системи можна використати, щоб вони підпадали під вимоги українського законодавства та аби була можливість забезпечити до неї вільний доступ усім користувачам.

По-четверте, для того, щоб у населення була можливість ознайомитися з процедурою проведення медіації та відповідною спеціальною онлайн платформою, на якій реалізовується даний метод врегулювання конфліктів, потрібно надати йому доступну інформацію та проконсультувати з окремих питань, які виникають у ході прийняття рішень щодо подальших дій, тобто для того аби задовільнити потреби клієнтів потрібно створити центри, які б надавали консультації щодо окремих запитів щодо медіації.

По-п'яте, до недоліків можна також віднести психологічні особливості сприйняття один одного в онлайн-просторі, а саме: 1) розмова через комп'ютер, як і телефонна розмова, підсвідомо сприймається сторонами як короткострокова, в той час як медіативна сесія в середньому триває 2–3 години; 2) відчувається відмінність у спілкуванні з людиною, яка поруч, і зображенням її на екрані. В силу зазначених психологічних причин зменшується і емоційний

вплив медіатора, виникають перешкоди для встановлення довіри, обмежуються можливості безперервного контакту очей як інструменту встановлення каналу комунікації (рапорту), обмежуються можливості медіатора щодо аналізу невербальної інформації. З цих причин розвиток онлайн-медіації має здійснюватися з використанням відеоконференцз'язку, котрий дозволяє максимально наблизити процедуру спілкування до реальності [6, с. 63].

Отже, проаналізувавши вище викладену інформацію, можна зробити висновок, що на даному етапі розвиток вирішення спірних ситуацій набуває нових форм їх владнання, тобто починають використовувати альтернативні методи, які в свою чергу дозволяють без зайвих витрат прийти до консенсусу сторін. За допомогою розвитку інформаційних технологій ми маємо змогу впоратися з труднощами сьогодення, зокрема з пандемією COVID-19, яка своєю появою сприяла певним змінам проведення переговорних процесів, але все ж таки не завадила медіації, можливість здійснення якої припустима в режимі онлайн.

Список використаних джерел

1. Рекомендація N R (99) 19 Комітету міністрів Ради Європи державам – членам Ради, які зацікавлені в організації медіації у кримінальних справах. – *Рекомендації*, Міжнародний документ від 15.09.1999. – № R(99)19// *Рада Європи, Комітет Міністрів Ради Європи*.
2. Національна асоціація медіаторів України. Медіація та судова система: Що? Як ? Навіщо? URL: http://namu.com.ua/ua/downloads/promomaterials/DODATOK_6_BROSHURA_MEDIATCHIA_TA_SUD.pdf
3. Загальна декларація прав людини. Декларація, Міжнародний документ від 10.12.1948 р.// *Голос України*. – 2008. від 10.12.2008. – № 236. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text
4. Головка О. М. Право людини на безпечне інформаційне середовище в контексті природних прав людини. – 2014. Вип. – № 4 (44). – С. 79-85.
5. Katsh E., Rabinovich-Einy O. Digital Justice: Technology and the Internet of Disputes. – Oxford University Press. – 2017. – 22 p.
6. Чванкін С. А. Онлайн медіація – перспективи розвитку в сучасних умовах. – Одеса. – 2020. – С. 61-64.

Васько В. А.

аспірант ДНУ «Інститут інформації,
безпеки і права НАПрН України»

ПРОБЛЕМА ВИЗНАЧЕННЯ ЗМІСТУ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ ДЕЦЕНТРАЛІЗОВАНИХ СЕРВІСІВ ОБМІНУ КРИПТОАКТИВІВ

Децентралізовані фінансові сервіси або децентралізовані фінанси (англ. Decentralized Finance, DeFi) в широкому розумінні – це фінансові інструменти, які застосовують технологію блокчейн з метою децентралізації фінансових послуг за рахунок відмови від посередництва традиційних брокерів, бірж та/або банків. Технологічна система децентралізованих фінансових сервісів включає в себе фінансові смарт-контракти, цифрові активи та децентралізовані сервер-клієнтські додатки (англ. decentralized application, DApp, dApp).

Ринкова капіталізація найпопулярніших криптовалют наприкінці 2020 року та на початку 2021 досягала рекордних показників, це в свою чергу стало причиною активізації інвестицій в криптоактиви та значного збільшення операцій по їх обмінах. Як наслідок, урядами багатьох держав та міжурядовими організаціями відбулось посилення правового регулювання діяльності сервісів обміну криптоактивів (криптобірж), які знаходяться в їх юрисдикціях, а це потягло за собою збільшення судових процесів учасниками яких є вищезазначені суб'єкти. Відтак постає питання, за яких істотних умов діяльність криптобірж не буде суперечити закону, і як винних за його порушення притягти до юридичної відповідальності. Для того щоб дати відповіді на ці питання необхідно в першу чергу розуміти різницю між децентралізованими та централізованими сервісами обміну криптоактивів.

На сьогодні централізований обмін криптоактивів є найбільш поширеним серед інвесторів, а найпопулярнішими біржами є Coinbase, Gemini, Kraken [1]. Централізовані криптобіржі (англ. Centralized Exchange, CEX) – це суб'єкти приватного права, які за-

реєстровані в установленому законом порядку та які надають послуги з купівлі або продажу криптоактивів за фіатні/цифрові кошти або криптовалюту за рахунок спеціально створених для цього платформ. CEX виконують роль посередника в таких транзакціях. Також останні не рідко виступають в якості зберігачів криптоактивів їх користувачів. Однією з головних особливостей CEX є те, що останні за рахунок технології блокчейн лише зберігають дані про проведені транзакції натомість сама торгівля криптовалютою здійснюється без застосування цієї технології [2].

На централізовані біржі поширюється сфера дії закону, де вони зареєстровані або іншим чином створені згідно з правом цієї держави. Таким чином CEX несуть юридичну відповідальність на загальних підставах, як будь-які інші суб'єкти господарської діяльності. Наприклад, у США регулювання діяльності централізованих сервісів обміну криптоактивів здійснюється на основі федеральних законів, тому вони підпадають під нагляд агентства по боротьбі з фінансовими злочинами (англ. Financial Crimes Enforcement Network, FinCEN) також на них поширюється вимога «знай свого клієнта» (англ. know your customer, KYC) та інші вимоги встановлені федеральним урядом, а ліцензування таких платформ здійснюється на основі законів окремих штатів [2]. Тому притягнення CEX до правової відповідальності у разі порушення закону звісно має свої особливості, але не є таким складним, як притягнення до такої ж відповідальності децентралізованих сервісів обміну криптоактивів.

Децентралізовані криптобіржі (англ. decentralized exchanges, DEX) – це платформи, які забезпечують здійснення безпечного обміну криптоактивами у одноранговій (децентралізованій) блокчейн мережі. За своєю природою DEX не є суб'єктами господарювання на відміну від CEX, по факту децентралізовані сервіси обміну криптоактивами це не більше ніж програмне забезпечення, яке працює в публічному блокчейні. Найбільш популярними DEX є Uniswap, MDEX (BSC), BurgerSwap, SushiSwap та PancakeSwap. Щоденний обсяг торгів на цих децентралізованих біржах перевищує 4 мільярди доларів [3].

Транзакції на таких платформах здійснюються за рахунок смарт-контрактів без участі посередників. Управління DEX здійснюється зацікавленими учасниками блокчейн-мережі без централізованого контролю, тому в них не може бути єдиної фізичної чи юридичної особи відповідальної за здійснення операцій та безпосередньо функціонування самої платформи. Враховуючи P2P відносини на яких будуються децентралізовані фінансові сервіси користувачі не втрачають контроль над своїми активами на відміну від CEX, тому DEX не виступають в якості зберігачів криптовалюті їх користувачів [4]. Ще однією істотною відмінністю децентралізованих фінансових сервісів є те, що валідатори транзакцій з купівлі/ продажу криптоактивів не можуть використовувати для цих цілей фіатні/цифрові кошти.

Оскільки операції на DEX платформах здійснюються в публічній блокчейн мережі за допомогою різних алгоритмів смарт-контрактів, то такі біржі не можуть бути уніфікованими. Це в свою чергу створює додаткові перепони в правовому регулюванні їх діяльності [4]. Технологічно нейтральні правила розроблені для регулювання діяльності CEX в переважній більшості випадків не застосовуються для DEX. Враховуючи, що транзакції з купівлі/ продажу криптоактивів на децентралізованих фінансових сервісах відбуваються без участі третіх сторін, то на таких платформах дуже важко дотримуватись вимог законодавства щодо протидії відмивання коштів (AML), зокрема правил «знай свого клієнта» (KYC), «належної перевірки клієнтів» (CDD), «розширеної перевірки клієнтів» (EDD) та інших [5].

Тим не менш, глобальна міжурядова організація Група з протидії відмивання коштів (англ. Financial Action Task Force on Money Laundering, FATF) у 2019 році випустила Інструкцію щодо подолання ризиків пов'язаних з віртуальними активами та постачальниками послуг віртуальних активів (англ. Virtual Asset Service Providers, VASP) (далі – Інструкція FATF). Не дивлячись на те, що правила FATF носять рекомендаційний характер, вони відіграють дуже важливу роль для постачальників та/або користувачів віртуальних активів, оскільки останні зможуть зрозуміти як буде від-

буватись регулювання їх діяльності, адже все більше країн імплементують положення Інструкції в своє національне законодавство.

У оновленій редакції Інструкції FATF від 28 жовтня 2021 року значна увага приділяється проблемі регулювання однорангових (P2P) транзакцій та децентралізованих фінансів (DeFi). Автори документа стверджують, що децентралізовані угоди з обміну криптоактивів за загальним правилом не підпадають під стандарти FATF та під дію національного законодавства щодо протидії відмивання коштів, оскільки такі транзакції здійснюються без залучення посередників. Проте, якщо протоколи смарт-контрактів P2P платформ розраховані на пошук або добір інших однорангових транзакцій останні можуть підпадати під визначення VASP навіть якщо вони не є посередниками у таких транзакціях [6].

Що стосується децентралізованих фінансів, то в Інструкції FATF сказано, що вони не є VASP у відповідності до стандартів FATF, оскільки останні не застосовуються до програмного забезпечення та технологій [6]. Проте, як і у випадку з одноранговими транзакціями є винятки, зокрема, в Інструкції сказано: «... якщо власники, розробники, оператори або інші особи, які зберігають контроль чи достатній вплив на механізми DeFi, то вони підпадають під визначення VASP надане FATF, у тому разі, коли вони надають, або іншими чином сприяють наданню послуг VASP»[6]. Зазначених суб'єктів можна відрізнити від інших учасників DeFi за наступними ознаками:

- 1) можуть впливати на активи та/або алгоритми, які використовуються в транзакціях на децентралізованих платформах;
- 2) можуть отримувати прибуток за використання DApp;
- 3) можуть встановлювати, або в будь-який час змінювати параметри для послуг, котрі надаються децентралізованими платформами.

Але в той же час, автори Інструкції FATF наголошують на тому, що дуже часто не можливо ідентифікувати таких централізованих суб'єктів VASP на платформах DeFi, враховуючи особливості децентралізованих сервер-клієнтських додатків [6].

У цілому, правила FATF узгоджуються з позицією регулюючих органів США. Так, наприклад, Комісія з цінних паперів і бірж

США (англ. The United States Securities and Exchange Commission, SEC) притягла розробника і власника децентралізованого сервісу обміну криптоактивів EtherDelta побудованого на базі Ethereum до юридичної відповідальності за порушення законодавства у сфері обігу цінних паперів. SEC встановила, що EtherDelta розробила децентралізовану платформу на якій за рахунок використання смарт-контрактів створила зовнішню книгу замовлень, у якій зберігались записи про замовлення на купівлю або продаж криптоактивів. Тим самим, розробник платформи порушив закон про цінні папери, оскільки він: *по-перше*, повністю контролював усі операції, які здійснювались на платформі; *по-друге*, отримував винагороду за розміщення замовлень; *по-третє*, книга замовлень зберігалась на централізованому сервері, а не в блокчейні; *по-четверте*, контролював алгоритм виконання смарт-контракту та міг його одноосібно змінити [7].

Проте, це один із небагатьох казусів, на прикладі якого здається, що розробників DApp доволі легко притягли до юридичної відповідальності за порушення законодавства, але насправді – це зовсім не так. Залежно від типу DEX, варіюється складність визначення змісту правової відповідальності розробників вихідного програмного коду децентралізованих сервер-клієнтських додатків. Так у тому випадку, якщо жоден центральний орган не веде книгу замовлень, а винагорода за проведені транзакції виплачується трейдерам, які забезпечують ліквідність криптоактивів, а не власникам платформи, то притягти будь-кого за порушення законодавства у сфері обігу цінних паперів в т.ч. криптоактивів – не можливо. Власне, так само, не можливо притягти до юридичної відповідальності розробників відкритого вихідного програмного коду DEX навіть якщо DApp будуть використовуватись для явно незаконних цілей [8].

Таким чином, регулюючим органам необхідно приділяти більше уваги проблемам правового регулювання діяльності DEX, оскільки на сьогодні існують значні ризики перетворення DeFi у тіньовий фінансовий ринок, який може завдати істотної шкоди CEX. Враховуючи особливості технології блокчейн зробити це

дуже складно, але рекомендації надані FATF значно полегшують цей процес, і тому країнам, які ще не впровадили ці правила в національне законодавство необхідно як найшвидше це зробити. Також це допоможе дещо вирішити не менш важливу проблему вибору юрисдикції при зверненні до суду у разі порушення прав фізичних чи юридичних осіб децентралізованими сервісами обміну криптоактивів.

Список використаної літератури

1. Що таке централізовані криптовалютні біржі. URL: bit.ly/3IXMRIG
2. Can You Sue a Cryptocurrency Exchange? URL: bit.ly/3IT0Klb
3. What is a Decentralized Exchange and How it Works. URL: bit.ly/3e08jsc
4. What are decentralized exchanges, and how do DEXs work? URL: bit.ly/3e12E4W
5. Some Thoughts on the Applicability of AML/CFT Requirements to Decentralized Crypto Exchanges. URL: bit.ly/3IS7tvI
6. FATF (2021), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FATF, Paris. URL: bit.ly/32bLSO4
7. SEC Charges EtherDelta Founder With Operating an Unregistered Exchange. URL: bit.ly/3mdO0vE
8. Васько В. А. Проблема визначення змісту юридичної відповідальності розробників відкритого вихідного коду блокчейн-проектів. *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. – С.160-166.

Стрельник В. В.

кандидат юридичних наук, доцент,
доцент кафедри приватного та
соціального права Сумського
національного аграрного університету

Мироненко А. О.

здобувачка вищої освіти рівня
бакалавр юридичного факультету
Сумського національного аграрного
університету

ПРАВА ЛЮДИНИ ЧЕРЕЗ ПРИЗМУ РОЗВИТКУ ШТУЧНОГО ІНТЕЛЕКТУ

XXI сторіччя – епоха інноваційних технологій, що відкривають нові можливості для стрімкого розвитку всіх сфер нашої життєдіяльності. Питання штучного інтелекту, що в недалекому минулому здавалося фантастичним, сьогодні, в умовах стрімкого розвитку технологій, стає звичним і повсякденним. Штучний інтелект як унікальний продукт технічного прогресу, дає змогу машинам вчитися, використовувати людський і власний досвід, пристосовуватися до нових умов, виконувати різнопланові завдання, прогнозувати події й оптимізувати ресурси різного характеру. Так званий алгоритм – послідовність дій вирішення поставленої задачі, залишається невідомим. Наука про штучний інтелект немає конкретного визначення як філософія не знайшла відповіді на питання про природу та статус.

Поряд з величезними перспективами, що відкриваються людству з розвитком і використанням штучного інтелекту, існує високий ступінь небезпеки для суспільства. Усвідомлюючи загрози прогресу технологій штучного інтелекту окремі вчені висловлюють думку про необхідність встановлення суворого контролю за їх впровадження. Про можливі ризики відкрито говорив Білл Гейц: «Розвиток цілковито штучного інтелекту може означати кінець людської раси» [1]. Здатність «інтелектуальних машин»

до самовідтворення може призвести до втрати контрольованості людиною. Шведський вчений, професор Оксфордського університету Нік Бостром стверджує, що до 2022 р. системи штучного інтелекту будуть мислити як людина – 10%, до 2040 р. – 50%, до 2075 р. – процеси мислення неможливо буде відрізнити від людських. Стрімкий розвиток технологій штучного інтелекту викликав наукові дискусії [2].

Право на приватність та конфіденційність персональних даних визнано основоположним правом людини. У зв'язку з цим розвиток та активне застосуванням штучного інтелекту обумовлює актуальність. Найбільш проста форма штучного інтелекту в роботі правника проявляється в моделях юридичних актів (судових рішень, нотаріальних актів, договорів). Представник правничої професії лише вибирає вид юридичного акту, що відповідає його справі. Такі форми штучного інтелекту в роботі юристів використовуються в різних державах вже з кінця 90-х рр. минулого століття. Так, наприклад, у Фінляндії й Італії існують електронні онлайн системи (Tuomas і Minerva), що дозволяють суддям і прокурорам спростити роботу у складанні окремих правових актів [3, с.153].

Автоматизованість судових рішень є прикладом використання штучного інтелекту в роботі судді. Мова йде про складання актів правосуддя, що породжує високу відповідальність у разі помилки. Система штучного інтелекту передбачила результати сотень справ у Європейському суді з прав людини, прогножуючи рішення з точністю до 79%.

Україна також застосовує досвід провідних європейських держав у сфері публічного адміністрування із впровадженням технологій штучного інтелекту. Міністерство цифрової трансформації розробило Концепцію розвитку штучного інтелекту в Україні. Даний нормативно-правовий акт передбачає розвиток підприємництва у сфері штучного інтелекту, активне впровадження «розумного інтелекту» в державне регулювання, дотримання права людини на приватність [4].

На сьогоднішній день найефективнішою е-послугою визнається сервіс «Дія», що складається з двох складових єдиної інфор-

маційної системи: (1) єдиний державний портал з надання державних послуг, (2) сховище електронних документів з даними реєстрів фізичних осіб. У майбутньому зазначений сервіс повинен повністю замінити центри надання адміністративних послуг. Вказані підходи дозволяють усунути корупційну складову надання адміністративних послуг державою. Згідно плану до 2024 року всі державні послуги будуть доступні українцям он-лайн. В свою чергу дані заходи вимагають найбільшого захисту приватної інформації. Реформа державних послуг з цифровізацією країни потребує кіберзахисту особистих даних.

У контексті порушення права на приватність, враховують право на свободу висловлення (ст. 19 Загальної декларації прав людини та ст. 10 Європейської конвенції з прав людини) та право мирних зборів (ст. 20 Загальної декларації прав людини та ст 11. Європейської конвенції з прав людини) [5, 6]. Прикладом обмеження права на висловлення власної думки є тимчасове/постійне блокування акаунтів. Це відбувається через те, що штучний інтелект оцінює як загрозу, дискримінацію або булінг. Аналіз персональної інформації дозволяє технологіям визначити уподобання, психологічні особливості кожної людини, що реалізується в отриманні нав'язливої реклами чи пропозицій. Об'єктивно доступ до особистих даних може мати негативні наслідки для суспільства. Уявімо, якщо керівництво таких компаній, як Apple, Meta почнуть використовувати штучний інтелект з власних потреб, ми опинимося в світі, де вся інформація буде належати домінуючим корпораціям, кожен буде їм підвладним.

Таким чином стан національного законодавства у сфері штучного інтелекту знаходиться на початковому етапі формування. При цьому вважаємо важливим звернути увагу на необхідність дотримання принципів верховенства права, громадянських свобод і права людини при регулюванні відносини що пов'язані зі штучним інтелектом. Україна не забезпечує належного контролю щодо схоронності особистої інформації у сферах взаємодії із штучним інтелектом. Враховуючи зазначене законотворчий процес у сфері застосуванням штучного інтелекту має будуватися на основі мак-

симального недопущення порушення основних прав і свобод людини, права на приватність.

З кожним новим роком розвитку наукового прогресу у сфері штучного інтелекту ми стаємо все ближче до невідомого, неосяжного майбутнього.

Список використаної літератури

1. Парасюк Є. О., Джалілова В. Р. Аналіз базової нормативної, правової, організаційної політики США, Китаю та Японії у сфері штучного інтелекту, штучно інтелектуальних робіт та робіт. Науковий огляд. 2019. № 9. URL: <http://oaji.net/articles/2019/797-1577640613.pdf> (дата звернення 20.11.2021 р.).

2. Радутний О. Е. Юридична освіта та сфера надання правових послуг в контексті штучного інтелекту. Інформація і право. 2019. №2 (29). С.40-54.

3. Шпиленко Б. П. Актуальні питання застосування інформаційних технологій у правовій діяльності. Збірник наукових статей молодих учених, аспірантів та студентів Сумського національного аграрного університету. – Суми, 2021. – С.153-156.

4. Про схвалення Концепції розвитку штучного інтелекту в Україні: розпорядження Кабінету Міністрів України від 02.12.2020. 1556-2020-р URL: <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text> (дата звернення: 20.11.2021).

5. Загальна декларація прав людини URL: https://zakon.rada.gov.ua/laws/show/995_015?ang=uk#Text (дата звернення: 20.11.2021).

6. Європейська конвенція з прав людини. Електронний ресурс. URL: https://www.echr.coe.int/documents/convention_ukr.pdf (дата звернення: 20.11.2021).

Алексєєва А. Р.
студентка Чернівецького
національного університету
ім. Ю. Федьковича

Науковий керівник: Заморська Л. І.
доктор юридичних наук, доцент
кафедри теорії права та прав людини
Чернівецького національного
університету ім. Ю. Федьковича

ПЕРСПЕКТИВИ РОЗВИТКУ КІБЕРБЕЗПЕКИ ЯК МЕТОДУ ЗАХИСТУ ПРАВ ЛЮДИНИ

Актуальність питання стосовно кібербезпеки сьогодні безсумнівно постає одним з найосновніших в наш час. Це безпосередньо пов'язано зі вседозволеністю та доступністю до певних джерел та їхніх даних, що забезпечується користувачам кіберпростору. Таким чином, зростає кількість загроз, що можуть завдати шкоди самій інфраструктурі та людям загалом. Саме тому держава повинна гарантувати громадянам України безпеку національного сегменту кіберпростору, адже динамічний цифровий світ потребує формування збалансованої та ефективної національної системи кібербезпеки, яка зможе гнучко адаптуватися до змін безпекового середовища [1].

Кіберзлочинність порушує не тільки загальний порядок в мережі Інтернет, так само це стосується основоположних прав громадянина. Випадки порушення прав людини в Інтернеті найчастіше пов'язані з неконфіденційністю даних, закликами до насильства, можливістю анонімного користування інформаційними джерелами, труднощами підтримки загального правопорядку тощо. Так, сьогодні існує ряд документів та актів, що кваліфікують посягання на права людини, будь-яке насильство, дискримінацію як злочин, проте жоден з них не може забезпечити впевненість особи в повній мірі щодо захисту її прав саме у віртуальному середовищі. Цим і пояснюється значення створення надійної системи регулю-

вання відносин в Інтернеті та законодавчому забезпеченні кібербезпеки в Україні.

Основним кроком України в напрямку осучаснення законодавства з питань захисту прав людини в Інтернеті стало прийняття Закону України «Про основні засади забезпечення кібербезпеки України» [2]. Він визначає головні принципи забезпечення кібербезпеки, напрямки державної політики, відповідальність за скоєння кіберінцидентів та основні координації органів державної влади з питань кібербезпеки. Ми вважаємо, дуже важливим є саме системний підхід до кібербезпеки та оцінки усіх можливих ризиків, викликаних швидкістю розвитку технологій, адже лише в такий спосіб можливий ефективний захист прав людини і громадянина. Така думка ґрунтується на забезпеченні довіри особи до держави стосовно процесів інформаційних змін.

Безумовно, одним із поштовхів для України до розвитку національного законодавства у даному контексті також стало використання кіберзброї Росією у своїй гібридній агресії проти нашої держави. Проведення кібератак на органи державної влади України, винайдення нових технік застосування небезпечних сегментів кіберпростору, кібертероризм спричиняють постійну необхідність розширення можливостей забезпечення кібербезпеки. На нашу думку, Україна має достатню кількість кваліфікованих фахівців та чудові перспективи для зростання рівня безпеки громадян у цифровому просторі. Це завдання є спільним як для держави, так і для суспільства в цілому, оскільки особливістю кіберпростору є відсутність кордонів і меж, а тому забезпечення безпеки є питанням кожного [3]. Незважаючи на те, що шлях до створення міцного підґрунтя та охоронної моделі національного законодавства щодо прав людини є тернистим та досить тривалим, слід зауважити, що стратегія функціонування такого регулювання вже вироблена.

На нашу думку, доцільно також проводити навчання на таку тематику із взаємодією відповідних державних органів. У таких спосіб буде формуватися обізнане суспільство, що згодом складе надійний фундамент не тільки задля забезпечення активної та

ефективної протидії кіберзлочинності та іншим кіберзагрозам, а і утриманням від них.

Отже, Україна повинна розробити власну систему захисту прав і свобод своїх громадян у кіберпросторі, таким чином забезпечивши тісний зв'язок держави і особи; попіклуватися про доступність для усіх верств населення та прозорість цієї системи; створити механізми контролю за такою діяльністю, де участь повинна брати не лише держава, а і громадяни України.

Використана література:

1. Проєкт «БЕЗПЕЧНИЙ КІБЕРПРОСТІР – ЗАПОРУКА УСПІШНОГО РОЗВИТКУ КРАЇНИ» [Електронний ресурс] – Режим доступу : <https://zakon.rada.gov.ua/laws/show/447/2021#Text>

2. Закон України «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс] – Режим доступу : <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

3. О. Бакалинський, О. Бакалінська «Правове забезпечення кібербезпеки в Україні» [Електронний ресурс] – Режим доступу : <https://doi.org/10.32849/2663-5313/2019.9.17>

Наукове видання

**СОЦІАЛЬНА І ЦИФРОВА ТРАНСФОРМАЦІЯ:
ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ ПРОБЛЕМИ
ПРАВОВОГО РЕГУЛЮВАННЯ**

**МАТЕРІАЛИ ВСЕУКРАЇНСЬКОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
2 ГРУДНЯ 2021 РОКУ**

Науковий керівник конференції ***О. А. Баранов***
Упорядники: ***В. М. Фурашев, С. О. Дорогих***

Підписано до друку 18.12.2021.
Формат 60х84/16. Ум-друк. арк. 18,83.
Наклад 100 прим. Зам. № 2112-14.
Видано і віддруковано 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