Державна наукова установа «Інститут інформації, безпеки і права
Національної академії правових наук України»

Науково-дослідний інститут інтелектуальної власності
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 ІІ ВСЕУКРАЇНСЬКОЇ
НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

КИЇВ, 25 ЛИСТОПАДА 2022 РОКУ

Київ-Одеса
2022

УДК 34:004(477)
С 69

Рекомендовано до друку
Вченою радою Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України»
протокол № 12 від 27 грудня 2022 р.

С 69 **Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання** : матеріали ІІ всеукр. наук.-практ. конф., Київ, 25 грудня 2022 р. / наук. керівник конф. О. А. Баранов ; упор.: В. М. Фурашев, С. О. Дорогих, М. В. Дубняк. – Київ-Одеса, 2022. – 108 с.

ISBN 978-966-928-856-1

У збірнику висвітлено матеріали ІІ 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 розраховане на фахівців, експертів і вчених в галузі права, студентів, аспірантів та науково-педагогічний склад вищих навчальних закладів та інших зацікавлених осіб.

Матеріали подано у авторській редакції.

УДК 34:004(477)

ISBN 978-966-928-856-1

ЗМІСТ

Харитонова О. І.
доктор юридичних наук, професор,
член-кореспондент НАПрН України,
зав. кафедри інтелектуальної
власності та патентної юстиції
Національного університету «Одеська
юридична академія»
Харитонов Є. О.
доктор юридичних наук, професор,
член-кореспондент НАПрН України,
зав. кафедри цивільного права
Національного університету «Одеська
юридична академія»

ДО ПИТАННЯ ПРО ВИЗНАЧЕННЯ ТЕРМІНО-ПОНЯТТЯ «ІНТЕРАКТИВНЕ ГРОМАДЯНСЬКЕ СУСПІЛЬСТВО»

Події останніх тридцяти років спричинили становлення на території колишніх радянських республік інститутів громадянського суспільства і як наслідок – все більше запровадження норм приватного права. Останні, як і відносини у цій сфері, у свою чергу, зазнають все більшого впливу інформаційних технологій. Таким чином, разом зі становленням інформаційного суспільства відбувається формування інтерактивного громадянського суспільства. І якщо категорія «громадянське суспільство» не є новою для права, то терміно-поняття «інтерактивне громадянське суспільство» ще чекає на спеціальне дослідження. Кореляційні зв'язки інформаційного та громадянського суспільства посилюються в умовах зростання рівня інтерактивності останнього на основі інформаційно-комунікаційних технологій, які дозволяють збирати, обробляти, отримувати та передавати інформацію на локальному, загальнодержавному та міжнародному рівнях. У сфері громадянського суспільства діють не громадяни, як суб'єкти політично-владних відносин і публічного права, а приватні особи, суб'єкти приватного права, учасники цивільних відносин, що суттєво впливає на характер внутрішньої складової правового середовища громадянського суспільства. Останню формують норми і правила приватного права, які визначають взаємини членів громадянського суспільства одне з одним і з державою, як суб'єктом приватних відносин. Вони визначаються індивідуальною та колективною правосвідомістю, правовою ментальністю учасників внутрішніх відносин громадянського суспільства та їхніх утворень (громадських рухів, об'єднань тощо). Приватне право органічно властиве громадянському суспільству,

є регулятором внутрішніх відносин у ньому і засобом забезпечення інтересів його членів стосовно одне одного.

Таким чином сутність громадянського суспільства полягає у гармонізації інтересів та відносин, які формуються між приватними особами та створеними ними об'єднаннями, що діють в умовах ринку.

Ознаками громадянського суспільства є те, що воно:

1) виникає в результаті договору між приватними особами, котрі відповідають уявленням про «модульну людину»,

2) має ідеологічним підґрунтям лібералізм,

3) припускає існування цивілізованого ринку,

4) ґрунтується на формулі свободи, вираженій як соціальні імперативи демократії,

5) основою взаємин між людьми має активність демократичного і ліберального характеру,

6) розглядається, передусім, як феномен поведінковий та інституціональний [1].

Держава не керує громадянським суспільством, але, якщо вона є правовою державою, зобов'язана забезпечити умови його функціонування і життєдіяльності [2], оскільки принцип пріоритетного функціонування громадянського суспільства стосовно державної влади є характерним для генеральної динаміки розвитку сучасної світової цивілізації [3].

Можна погодитися з розумінням громадянського суспільства як цілісної сфери громадського життя, що є відносно самостійною від державних інституцій і механізму державної влади. Громадянське суспільство – це унікальна система взаємодії суспільних індивідів, соціальних груп, верств і прошарків, що збалансовує вектори своїх складових, виявляючи рівнодіючу безлічі індивідуальних і групових прагнень та сподівань. Не держава має визначати спільний знаменник суспільних аспірацій, бо вона принципово не здатна виконувати ці функції, а може лише імітувати цей процес, а навпаки, громадський лад своїм функціонуванням об'єктивно відтворює суспільні імперативи політичній системі, одночасно зумовлюючи становлення таких державних форм, які були б спроможні адекватно реагувати на об'єктивні інтереси суспільства [4].

Кореляційні зв'язки інформаційного та громадянського суспільства посилюються в умовах зростання рівня інтерактивності останнього на основі інформаційно-комунікаційних технологій, які дозволяють збирати, обробляти, отримувати та передавати інформацію на локальному, загальнодержавному та міжнародному рівнях. Провідне місце поміж таких технологій посідає Інтернет – найбільша телекомунікаційна мережа у світі, яка зародилася у 1969 р. і, починаючи з 80-х років XX століт-

тя стала активно розвиватися та розповсюджуватися. Основною метою Всесвітньої Мережі є поширення інформації серед користувачів, обмін такою інформацією. Вона є унікальним засобом комунікації, яка не знає часових і просторових меж, оскільки обмін інформацією відбувається блискавично і незалежно від відстані і кордонів. У своєму розвитку Мережа пройшла три етапи.

Першим – було створення Web 1.0, досить обмеженої функціонально, яка дозволяла читати інформацію та купувати речі. На початку 2000-х років завдяки швидкому розвитку нових технологій з'явилися більш потужні веб-сайти і більш надійні веб-інфраструктури, що дозволило користувачам не лише споживати інформацію з Інтернету, але й публікувати її.

На етапі Web 2.0 Мережа трансформувалася у щось більш значне, ніж гігантський торговий центр і онлайн-енциклопедія. Дозволивши користувачам здійснювати в Інтернеті різноманітні дії, вона стала тим місцем, де люди могли чинити майже все. Затим з'являється соціальна мережа на основі нової платформи Facebook, завдяки якій люди отримали можливість обговорювати і ділитися інформацією про дії [5].

Таким чином, завдяки Інтернету відбувається соціальна інтеграція як процес утворення взаємозв'язків між індивідами, групами, яскравим прикладом чого є створення соціальних мереж, які набувають все більшого значення і охоплюють все ширше коло учасників.

Відтак провідного значення набувають соціальні мережі – соціальні структури, що утворюються окремими особами або організаціями з метою обміну інформацією, спілкування, комунікацій. За допомогою комунікації суспільство може визначити себе, інформувати себе про власні інтелектуальні комунікації, піддавати інформацію сумніву, відхиляти її, нормувати комунікації як допустимі чи неприпустимі тощо [6].

Таким чином, разом зі становленням інформаційного суспільства відбувається формування інтерактивного громадянського суспільства. Як здається, підґрунтям характеристики цього поняття має бути розуміння громадянського суспільства як сфери соціальної інтеракції між економікою і державою, яка складається, у першу чергу, зі сфер найбільш близького спілкування (сім'ї, родини), об'єднань (передусім, добровільних), соціальних рухів та різноманітних форм публічної комунікації, яка відбувається за допомогою засобів Інтернет.

Список використаних джерел:

1. Ховард Марк М. Слабость гражданского общества в посткоммунистической Европе / пер.с англ. И. Е. Кокарева. ― М., 2009. – С. 57.

2. Кузнєцова Н. Громадянське суспільство, держава, приватне право: проблеми співвідношення та взаємодії // Право України. – 2014. – № 4. – С. 66.

3. Оніщенко Н. До питання про пошук балансу у співвідношенні громадянського суспільства та держави: теоретико-методологічні аспекти // Право України. – 2014. – № 4. – С.55. Огляд та ґрунтовний перелік ознак громадянського суспільства див.: Колодій А. Громадянське суспільство: ознаки, структурні елементи, співвідношення із державою // Право України. – 2014. – № 4. – С.9-12.

4. Пасько І. Т., Пасько Я. І. Громадянське суспільство і національна ідея. (Україна на тлі європейських процесів. Компаративні нариси). — Донецьк, УКЦентр, 1999. – 46 с.

5. Шмідт Е., Розенберг Дж. Як працює Google / Пер. с англ. Ю. Гордієнка. – К., 2016. – С. 274-275.

6. Андреєв Д. Засоби масової інформації як механізм інтелектуальної комунікації в процесі розвитку інформаційного суспільства // Теорія і практика інтелектуальної власності. – 2015. – № 5. – С. 56.

Баранов О. А.
доктор юридичних наук, професор,
Керівник Наукового центру цифрової трансформації і права Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України»

ПЕРШОПРИЧИНА ДЕГРАДАЦІЇ ЦИВІЛІЗАЦІЇ ТА ШЛЯХИ ЇЇ НЕЙТРАЛІЗАЦІЇ

В останні десятиліття світова спільнота знаходиться в активному пошуку виходу із дуже загрозливого становища – початку деградації цивілізації, про перші ознаки якої було заявлено в середині, начебто не таких вже далеких, 70-х років минулого сторіччя. Почалося з констатації начебто доволі невинного зниження темпів розвитку людства, потім декілька тривожних дзвоників у вигляді низки світових та регіональних криз і вже на при кінці 20-х років 21 століття заговорили про крах світової економіки та руйнування планети. ООН проводить Форум тисячоліття народів (2000), приймає Декларацію та Програму дій щодо зміцнення

Організації Об'єднаних Націй у XXI столітті. З огляду на невтішні результати виконання Програми ініціює широкий процес щодо усвідомлення державами загрозливих ознак сповзання світу у прірву. Генеральна Асамблея ООН ухвалює резолюцію «Перетворення нашого світу: Порядок денний у сфері сталого розвитку на період до 2030 року» (2015). В Резолюції з метою уникнення деградації визначається 17 глобальних цілей сталого розвитку та близько 170 завдань, які охоплюють практично всі сфери життєдіяльності людства. Але вже у 2019 році констатується неприпустима повільність процесу досягнення зазначених цілей сталого розвитку цивілізації.

Одночасно з'являється велика кількість теорій виходу із загрозливого становища, в якому опинилась світова економіка. В кожній з цих теорій пропонується певні підходи до побудови нової економічної моделі, але характерним є майже повна відсутність консенсусного розуміння базових причин колапсу економічної системи людства. Але, на наш погляд, не виявивши коріння причин занепаду цивілізації будувати процеси досягнення цілей сталого розвитку людства є неприпустимим в сучасних умовах гострого дефіциту часу та критичної обмеженості різноманітних світових ресурсів.

Однією із системних базових причин деградації планети та людської цивілізації слід визнати загальну ситуацію у світі з вкрай низькою якістю прийняття та виконання рішень. Більшість прийнятих рішень не відповідали критерію оптимальності та в переважній більшості випадків не були релевантними поставленим цілям та реальному стану соціальних процесів. Низьку якість рішень щодо визначення цілей діяльності також слід зарахувати до базової причини деградації планети та людської цивілізації. Крім того, свій вклад щодо нерелевантності вносила довготривалість процесу прийняття рішень.

За результатами аналізу еволюційного розвитку Homo sapiens констатується потужність впливу на розвиток його когнітивних функцій мови. Мова стала з одного боку невід'ємним атрибутом будь-якої життєдіяльності людини, а з іншого – її розвиток був необхідною умовою подальшого розширення різноманіття видів та типів такої діяльності. Отже, мова, інформаційні відносини як відносини, пов'язані зі створенням, передачею, використанням та зберіганням інформації стали необхідною, гармонійною складовою первинних соціальних процесів у конкретних предметних сферах людської діяльності.

Рішення – *це інтегральний результат людської діяльності, насамперед функціонування інтелекту, як певної сукупності когнітивних функцій мозку, метою якої є вибір найкращого варіанта поведінки або дій для*

конкретної сукупності параметрів змінних стану внутрішнього та навколишнього середовища. Тобто ефективність рішень напряму залежить від ефективності реалізації когнітивних функцій мозку людини.

В чому ж причина прийняття неякісних рішень, в дійсності першопричиною деградації цивілізації?

Якісна (своєчасна, актуальна, повна та достовірна) інформація, ефективність інформаційних відносин та інформаційної взаємодії має фундаментальне значення для прийняття людиною будь-яких рішень. Прийняття оптимальних (раціональних) рішень це базова умова забезпечення ефективності людської діяльності в будь-якій сфері соціальної активності, що, у свою чергу, є фундаментальною умовою гарантії ефективності функції самозбереження та розвитку цивілізації.

З середини дев'ятнадцятого століття людство стало явно усвідомлювати проблему збільшення труднощів у сфері інформаційних відносин та інформаційної взаємодії, яка надзвичайно загострилась в 50-60 роках минулого. Різко ускладнилось прийняття оптимальних рішень тому, що для їх прийняття стало необхідним обробляти великі обсяги актуальної, повної та достовірної інформації.

Дослідження вчених виявили недоліки у функціонуванні когнітивних функцій людини: фіксована швидкість когнітивних процесів; лімітована продуктивність діяльності мозку та точності оброблення інформації; природня схильність до застосування стандартних нейробіологічних алгоритмів в процесі прийняття рішень; обмеженість обсягу інформації, яка утримується в пам'яті та обробляється.

В результаті, приблизно до середини 20 століття сформувався та продовжував зміцнюватися фундаментальний бар'єр на шляху розвитку цивілізації, поява якого була наслідком природної обмеженості когнітивних можливостей людини у збиранні, обробці та передачі інформації. Цей бар'єр запропоновано називати ***першим цивілізаційним когнітивним протиріччям – як*** *протиріччя між наявністю природного обмеження когнітивних можливостей людини та необхідністю все з більшою швидкістю та у все більших обсягах збирати, обробляти, використовувати та передавати різноманітну інформацію для реалізації ефективної людської діяльності в інтересах забезпечення самозбереження цивілізації, що розвивається.*

Але, як це було раніше в історії людства, відповіддю на цей цивілізаційний виклик стало одне з досягнень чергової промислової революції – ***комп'ютер***, який надав можливість істотно згладити гостроту першого цивілізаційного когнітивного протиріччя.

З середини минулого століття розпочався епохальний етап в історії людства – етап широкого та повсюдного впровадження інформаційних

комп'ютерних технологій (ІКТ), що послідовно отримував назви: автоматизація, комп'ютеризація, інформатизація. Терміни змінювалися, але суть залишалася однією – людство стало широко використовувати ІКТ для вирішення проблеми протидії цивілізаційному виклику.

В роботі констатується формування наприкінці 20 століття ***другого цивілізаційного когнітивного протиріччя*** *– як протиріччя між існуванням природного обмеження когнітивних можливостей людини та необхідністю швидкого прийняття оптимальних рішень для реалізації ефективної людської діяльності в інтересах забезпечення самозбереження та розвитку цивілізації.*

Відповіддю на другий цивілізаційний виклик стало тотальне впровадження цифрових технологій: розвиток інформаційного суспільства та тотальна цифровізація.

Однак, на зламі останніх двох століть збільшується кількість проблем, пов'язаних із глобалізацією, збільшенням різноманіття, багатозв'язності та взаємозумовленості сучасного світу, всіх суспільних процесів і явищ. Швидке прийняття безперервного ланцюжка взаємообумовлених рішень задля забезпечення ефективності життєдіяльності світової спільноти, держав, суспільств та окремих людей стало потребувати використання значного обсягу різноманітних знань.

Задля кращого розуміння природи появи певних труднощів застосування знань у процесі прийняття рішень запропоновано вдосконалене формулювання ***ефекту Даннінга-Крюгера.***

До відомого ефекту Даннінга–Крюгера щодо метакогнітивного спотворення, який став майже класичним поясненням причини прийняття неправильних рішень, пропонується додати нове положення:

люди, які мають високий рівень компетенції, але не володіють достатнім обсягом знань:

- по-перше, часто можуть приймати помилкові рішення, нерелевантні поставленим цілям та реальному стану соціальних процесів, сучасним досягненням науки і техніки, можливостям нових, насамперед цифрових технологій, а також обставинам, у яких вони приймаються;
- по-друге, вони впевнені, що приймають правильні рішення, але схильні до проявів сумнівів щодо правильності прийнятого рішення, тому можуть вживати зусиль для перевірки правильності обраної стратегії.

Таким чином, сформувалось ***третє цивілізаційне когнітивне протиріччя*** *– як протиріччя між наявністю природного обмеження когнітивних можливостей людини внаслідок персоналізованого метакогні-*

тивного процесу мозку щодо опанування розмаїттям знань, які продукуються різними людьми навіть відносно одного і того ж процесу, об'єкту чи явища, та необхідністю використання різноманітних точних знань при прийнятті оптимальних рішень для реалізації людської діяльності в інтересах забезпечення самозбереження цивілізації, що розвивається.

Відповіддю на третій цивілізаційний виклик стає широке впровадження досягнень четвертої промислової революції, а саме цифрових технологій: технології Інтернету речей, Індустрії 4.0, штучного інтелекту, робототехніки, обробки великих даних, хмарних обчислень, електронних комунікацій та багатьох інших з метою підвищення ефективності групової та індивідуальної діяльності людської спільноти.

Отже, першопричиною деградації цивілізації є наявність трьох цивілізаційних когнітивних протирічь, які можуть бути усунені завдяки повсюдному використанню різноманітних цифрових технологій.

Світ стоїть на порозі проведення масштабних соціальних та цифрових трансформацій задля нейтралізації процесу деградації.

Фурашев В. М.
кандидат .технічних наук, старший науковий співробітник, перший заступник директора Державної наукової установи «Інститут інформації, безпеки і права» НАПрН України, доцент КІГАП ФСП Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

ПРОБЛЕМНІ ПИТАННЯ ОСВІТНЬОГО ПРОЦЕСУ ПІДГОТОВКИ ПРАВНИКІВ ДЛЯ РОБОТИ В УМОВАХ СОЦІАЛЬНОЇ ТА ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Проблеми самі по собі не виникають. Вони є наслідком якихось процесів, процедур або дій. Це – аксіома.

Розуміння витоків та сутності проблеми допомагає у пошуку шляхів, механізмів та засобів їх запобігання, вирішення або ігнорування.

Витоки проблем забезпечення освітнього процесу підготовки правників для роботи в умовах соціальної та цифрової трансформації, тобто

в умовах перехідного періоду від індустріального суспільства до постіндустріального, знаходяться у площині ступеня розуміння та сприйняття:

– спрямованості та темпів науково-технічного прогресу;
– широти і глибини охоплення результатами науково-технічного прогресу сфер забезпечення життєдіяльності людини, суспільства і держави;
– ступеня підготовленості людини, суспільства та держави до сприйняття результатів науково-технічного прогресу у тій чи іншої сфері забезпечення життєдіяльності людини, суспільства і держави;
– ступеня кадрової та техніко-технологічної підготовленості до повноцінного впровадження результатів науково-технічного прогресу у тій чи іншії сфері забезпечення життєдіяльності людини, суспільства і держави;
– ролі та місця систем національного та міжнародного права у процесах складових сучасного науково-технічного прогресу та їх розвитку.

Цілком зрозуміло, що впровадження у реальне життя будь-яких досягнень у науці та техніки, так чи інакше, впливають на наявні соціальні та суспільні відносини.

Також цілком зрозуміло, що світове суспільство, у тому числі, й українське, вже обрало «шлях» подальшого свого розвитку та, у даний час, знаходиться на первісній стадії перехідного етапу до постіндустріального суспільства, головними ознаками якого передбачаються [1]:

1. перехід від виробництва товарів до виробництва послуг;
2. переважання серед працівників «класу» професійних фахівців і техніків;
3. провідна роль теоретичних знань, як основи нововведень в економіці, політиці і соціальній структурі суспільства;
4. орієнтація в майбутньому на методи контролю і оцінка можливих напрямів розвитку технології;
5. прийняття рішень на засадах нової «інтелектуальної технології».

Це одна сторона сучасності.

Інша полягає у тому, що вже зараз спостерігається масова «дифузія» засобів інформатизації практично в усі сфери життєдіяльності суспільства, в тому числі і правову. Тобто, необхідно зважати на той факт, що ще однією з характерних рис постіндустріального суспільства буде максимальне розширення кіберпростору та суттєве підвищення ефективності його використання, у сукупності з природним простором. Це, в свою чергу, буде вимагати формалізації, незважаючи на успіхи в області ство-

рення та впровадження «штучного інтелекту», процесів, які пов'язані із забезпеченням функціювання та розвитку систем життєдіяльності суспільства. Це безперечно стосується і сфери правового забезпечення. Також необхідно враховувати те, що процеси формалізації вимагають чіткості та однозначності, структурованості, не повторюваності та ін.

Сукупність цих процесів формує напрями та визначає темпи соціальної та цифрової трансформації.

Таким чином, суцільна інформатизація майже всіх сфер забезпечення життєдіяльності та розвитку суспільства напряму або опосередковане впливають на трансформацію чинних суспільних відносин, аж до корінного їх змінення, а також формує нові суспільні відносини.

Ще раз підкреслимо, що майбутнє людства пов`язане з кіберпростором, його розвитком та поширенням, а також постійно зростаючим впливом інформації. Вже зараз очевидно, що сучасна соціалізація людини досить значною мірою пов`язана з кіберпростором та його складовими. Вже зараз можна говорити про «боротьбу» традиційної, звичної соціалізації індивідума з кіберсоціалізацією, причому з кожним поколінням кіберсоціалізація «відвойовує» все нові позиції. Кіберсоціалізація є одним зі спонукальних факторів процесів трансформації суспільних відносин.

Однією з головних функцій системи державного управління є відслідковування та регулювання у сфері суспільних відносин та забезпечення їх дотримання, яка передбачає наявність відповідних державних інституцій та кадрового потенціалу.

На даний час діє галузевий поділ системи національного права, який передбачає наявність 3-х видів:

- фундаментальні (профілювальні) галузі права, які утворюють юридичну основу та обов'язкову частину системи права, є «юридично первісні», які утворюють правовий матеріал, що використовується при формуванні інших галузей права. «Традиційно» до таких віднесені конституційне право, цивільне право, адміністративне право, кримінальне право, цивільно-процесуальне право, кримінально-процесуальне право;
- спеціальні галузі права: правові режими пристосовані до особливих сфер життя суспільства до яких наразі віднесені трудове, земельне та сімейне право;.
- спеціальні галузі права: правові режими пристосовані до особливих сфер життя суспільства до яких наразі віднесені трудове, земельне та сімейне право.

Як бачимо, у даній галузевій структурі національного законодавства та її інституцій не передбачене місце інституції, яка би повною мірою

несла «відповідальність» за регулювання суспільних відносин в інформаційній сфері та забезпеченні їх дотримання.

За логікою правової системи питання правового регулювання процесів та відносин, які виникають у частині поводження з інформацією на всіх стадіях її життєвого циклу (створення, збереження, обробка, розповсюдження та знищення) є виключно прерогативою саме інформаційного права. Саме інформаційне право повинно бути, свого роду, «конституцією» для всіх галузей права у частині поводження з інформацією, формування та використання контентної складової інформаційного простору, незалежно від платформи його походження та розташування — природного або штучного (кібернетичного).

Це – за логікою, а у реальності, як бачимо, на даний час, інформаційного права в системі галузей права не існує. На дане твердження слід очікувати заперечення – як немає, а **наукова** спеціальність 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право у формулі якої чітко вказується, що це – галузь **юридичної науки**, яка досліджує суспільні відносини у визначених сферах. Але це вже інша справа, яка не має прямого відношення до галузевого розподілу національного права.

Поглянемо на вирішення питання освітнього процесу підготовки правників для роботи в умовах соціальної та цифрової трансформації з іншого боку.

Міністерством освіти і науки України наказом № 1076 від 08.10.2021 р. затвердило Програму єдиного державного кваліфікаційного іспиту (далі – ЄДКІ) за спеціальностями 081 «Право» та 293 «Міжнародне право» на другому (магістерському) рівні вищої освіти.

ЄДКІ – обов'язковий компонент атестації спеціальних компетентностей, визначених стандартами вищої освіти та достатніх для ефективного виконання професійної діяльності за обраною спеціальністю.

Дана Програма ЄДКІ складається з 12 розділів:

– Конституційне право України;
– Адміністративне право України;
– Адміністративне судочинство в Україні;
– Міжнародне публічне право, міжнародний захист прав людини;
– Цивільне право України;
– Цивільне процесуальне право України;
– Трудове право України;
– Міжнародне приватне право;
– Кримінальне право України;
– Кримінальне процесуальне право України;

– Міжнародне кримінальне право, включаючи міжнародне співробітництво у сфері запобігання злочинності;
– Загальні етичні вимоги правничої професії.

Серед наведених розділів Інформаційне право також відсутнє.

З огляду на тенденції розвитку світового суспільства, спрямованість сучасного науково-технічного прогресу, чисельних різнопланових досліджень в інформаційної сфері, набутий досвід під час російської агресії та інших чисельних факторів, а також вищенаведеного, можна наступне:

1. Право з інструмента системи державного управління, яке спрямоване лише на фіксацію соціальних та суспільних відносин з подальшим встановленням найбільше значущих загальнообов`язковими повинно поступово перетворюватися в інструмент формуючий відповідні соціальні та суспільні відносини.

2. Трансформація системи права передбачає випереджувальний характер встановлення правовідносин з одночасним впровадженням результатів науково-технічного прогресу.

3. Трансформація системи права передбачає також удосконалення галузевого поділу системи національного права з урахуванням ролі та місця чинних галузей права у сучасних та майбутніх умовах та обставинах.

4. Структура освітнього процесу підготовки правників для роботи в умовах соціальної та цифрової трансформації напряму залежить від спрямованості та темпів трансформації системи права, але одна умова, причому вкрай необхідна, є – підготовка правників повинне здійснюватися з випередженням професійних знань, які отримуються, як мінімум на 5 – 7 років.

Список використаних джерел:

1. Bell D. Notes on the Post-Industrial Society // The Public Interest. — 1967. — № 7. — С. 102-118.

Бевз С. І.
доктор юридичних наук, професор, завідувач кафедри інформаційного, господарського та адміністративного права Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

ОРГАНІЗАЦІЙНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ РОЗВИТКУ СИСТЕМИ ЕЛЕКТРОННИХ РЕЄСТРІВ

Активне впровадження інформаційно-комунікаційних технологій в усі сфери суспільного життя не залишило осторонь сферу публічного управління та адміністрування. Навпаки, ця сфера зазнала найбільшого впливу відповідних трансформацій. Адже «застосування нових інформаційно-комунікаційних технологій для здійснення адміністративної діяльності та електронної взаємодії між органами виконавчої влади, юридичними особами та громадянами визначено країнами колишньої «вісімки» спільно з Європейською комісією одним із пріоритетних проєктів, що мають міжнародне значення і демонструють потенціал інформаційного суспільства» [1, с.15].

Ще у 2013 році, у Стратегії розвитку інформаційного суспільства [2], передбачено «електронну демократію як форму суспільних відносин, за якої громадяни та організації залучаються до державотворення та державного управління, а також до місцевого самоуправління шляхом широкого застосування інформаційно-комунікаційних технологій». Відповідно до Указу Президента України від 12 січня 2015 р. № 5 «Про Стратегію сталого розвитку «Україна-2020» [3], Стратегії реформування державного управління на період до 2021 року [4] у числі пріоритетів реформування системи державного управління зазначалося про розвиток електронного урядування, що, в свою чергу, за змістом Концепції розвитку електронного урядування в Україні [5] визнається «формою організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади та органів місцевого самоврядування із використанням інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян». В Стратегії реформування державного управління України на 2022-2025 роки [6] вже констатується, що «У рамках реформи створено Єдиний державний веб-портал електронних послуг, а також систему електронної взаємодії державних електронних

інформаційних ресурсів “Трембіта”, проте не в повному обсязі забезпечено обмін інформацією між реєстрами (базами даних) з використанням зазначеної системи». Тож трансформація відносин між суб’єктами владних повноважень поступово відбувається саме шляхом їх цифровізації відповідно до статегічних і концептуальних нормативних актів нашої держави.

Впровадження в діяльність суб’єктів публічної адміністрації Концепції електронного урядування [5], Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки [7], Стратегії реформування державного управління на період до 2021 року [4] та такої ж Стратегії на період 2022-2025 років [6] (продовжує впроваджуватися) зумовило виникнення нових питань, що потребують правового врегулювання.

Одним з таких є правовий режим електронних реєстрів.

В Стратегії реформування державного управління на період до 2021 року [4] основним завданням електронного урядування було визначено «створення (удосконалення) реєстрів даних громадян, юридичних осіб, земельних ділянок і нерухомості, податків, соціального страхування, забезпечення функціональної сумісності систем та здійснення обміну даними на операційному рівні замість подання довідок та інших документів». І лише 18.11.2021р. з’явився Закон України «Про публічні електронні реєстри» [8], відповідно до п.12 ч.1 ст.1 якого «публічний електронний реєстр (реєстр, кадастр, регістр тощо) – інформаційно-комунікаційна система, що забезпечує збирання, накопичення, захист, облік, відображення, оброблення реєстрових даних та надання реєстрової інформації». В той же час, незважаючи на врегулювання на законодавчому рівні ряду питань, пов’язаних з функціонуванням інформаційних ресурсів, спостерігаються певні прогалини, що потребують відповідного врегулювання. Зокрема, потребує подальшого законодавчого вирішення питання стосовно правового режиму реєстрів [9, с.311-312].

Маємо констатувати, що до прийняття Закону України «Про публічні електронні реєстри» правовий режим таких реєстрів визначався на підставі різних законів. Так, у ч. 5 ст. 7 Закону України «Про державну реєстрацію юридичних осіб, фізичних осіб – підприємців та громадських формувань» [10] передбачено, що «Єдиний державний реєстр та його програмне забезпечення є об’єктом права державної власності»; у ч. 6 ст. 12 Закону України «Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень» [11] визначено, що «Державний реєстр прав є державною власністю, складовою Національного архівного фонду і підлягає довічному зберіганню»; згідно з ч. 4 ст. 5 Закону України «Про Державний земельний кадастр» [12] Державний земельний кадастр є

державною власністю. Утім, у Законі України «Про державну реєстрацію актів цивільного стану» [13] такий режим Реєстру не визначено.

Ч.4 ст.3 Закону України «Про публічні електронні реєстри» фактично усунула цю прогалину та невизначеність правового режиму інших існуючих та потенційних публічних реєстрів шляхом їх віднесення до власності держави, відповідної територіальної громади або відповідної саморегулівної організації в особі держателя відповідного реєстру. Утім конкретизація стосовно реєстрів, що не належать до власності відповідної саморегулівної організації, що зроблено в абз.2 ч.4 ст.3 вказаного Закону, зумовлює питання про доцільність виключення з державної власності таких реєстрів та визнання їх власністю саморегулівної організації. В контексті відсутності врегулювання на законодавчому рівні діяльності саморегулівних організацій в Україні вважаємо таке рішення передчасним. Крім того, звертаємо увагу, що в ст.6 Закону, визначаючи систему реєстрів, як «сукупність реєстрів, що функціонують та взаємодіють для створення, зберігання, оброблення та використання інформації під час провадження дозвільної діяльності, надання адміністративних, соціальних та інших публічних послуг, провадження іншої управлінської діяльності та здійснення державного регулювання», тобто тієї інформації, що згідно з ч.4 ст.3 Закону міститься в реєстрах, що перебувають виключно у власності держави або відповідної територіальної громади, законодавець до такої системи включає також реєстри саморегулівних організацій. Така ситуація зумовлює необхідність подальшого дослідження і визначення правового режиму реєстрів саморегулівних організацій.

Віднесення публічних електронних реєстрів, в тому числі, до державної власності звертає нашу увагу на Закон України «Про управління об'єктами державної власності» [14], в якому визначені правові основи управління відповідними об'єктами та особливості управління окремими з них. Проте серед об'єктів управління державної власності, що визначені в статті 3, не вказано ні жодного реєстру, ні реєстру реєстрів, що потребує внесення відповідних змін. Вирішення цього питання потребує встановлення режиму реєстру як об'єкту правовідносин.

Враховуючи величезну кількість реєстрів в сучасній Україні, необхідність налагодження взаємодії між ними, актуальним є питання управління такими об'єктами державної власності як електронні реєстри. Головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізацію державної політики, зокрема, у сфері публічних електронних реєстрів є Міністерство цифрової трансформації України [15]. Адміністрування реєстрів здійснюють фактично їх держателі – орган державної влади, орган місцевого самоврядування

або саморегулівна організація, що забезпечує створення, функціонування та ведення публічного електронного реєстру. В той же час реєстри органів державної влади є об'єктами державної власності; а в Концепції оптимізації системи центральних органів виконавчої влади [16] звертається увагу на те, що «у роботі міністерств можливий конфлікт між функціями формування державної політики та окремими функціями з реалізації державної політики, зокрема щодо управління об'єктами державної власності. .. Міністерства та інші центральні органи виконавчої влади потребують визначення їх місій, а також чіткого розподілу повноважень». Тільки належне здійснення своїх повноважень державними органами може створити можливість функціонування всієї системи. З одного боку, це забезпечує стабільний розвиток держави відповідно до державних завдань у межах її програм та політики; з іншого, – стабільне життя громадян, їх особистий та професійний розвиток у безпечних умовах [17, с.23].

Тож вважаємо за доцільне створити відповідно до Закону України «Про центральні органи виконавчої влади» [18] Агентство електронних реєстрів та інформаційних ресурсів України як центральний орган виконавчої влади для виконання окремих функцій з реалізації державної політики, більшість функцій якого складатимуть функції з управління об'єктами державної власності – державними реєстрами.

Виходячи з зазначеного, можемо констатувати, що цифрова трансформація взаємовідносин суб'єктів публічної адміністрації та приватних осіб зумовила появу нового Закону України «Про публічні електронні реєстри», але залишилися питання, які потребують подальшого обговорення та врегулювання. Запропоновані вище кроки, на нашу думку, сприятимуть вдосконаленню організаційно-правового забезпечення розвитку системи державних електронних реєстрів, що, в свою чергу, матиме також наслідком вдосконалення механізму забезпечення прав і законних інтересів приватних осіб в інформаційній сфері.

Список використаних джерел:

1. Соснін О. Створимо електронну Україну разом. *Юридичний вісник України.* № 24–25 (1249–1250). 14–27 черв. 2019 р. С. 15.

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

3. Стратегія сталого розвитку «Україна-2020» : затв. Указом Президента України від 12 січ. 2015 р. № 5/2015. *Офіційний вісник України*. 2015. № 4. С. 8.

4. Стратегія реформування державного управління України на період до 2021 р. : схвалено розпорядженням Кабінету Міністрів України від 24 черв. 2016 р. № 474. URL: https://zakon.rada.gov.ua/laws/ show/ en/474-2016-%D1%80#n9.

5. Концепція розвитку електронного урядування в Україні : схвалено розпорядженням Кабінету Міністрів України від 20 верес. 2017 р. № 649-р. *Офіційний вісник України*. 2017. № 78. С. 109.

6. Стратегія реформування державного управління України на 2022-2025 роки : схвалено розпорядженням Кабінету Міністрів України від 21 липня 2021 р. № 831-р. URL: https://zakon.rada.gov.ua/laws/show/831-2021-%D1%80#Text

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

8. Про публічні електронні реєстри: Закон України від 18.11.2022 № 1907-IX. URL: https://zakon.rada.gov.ua/laws/show/1907-20#Text

9. Бевз С. І. Адміністративно-правове регулювання державного управління у сфері господарської діяльності в Україні. Дис. на здоб. ступ. доктора юридичних наук за спеціальністю 12.00.07. Київ, Національний авіаційний університет. 2020. 425 с.

10. Про державну реєстрацію юридичних осіб, фізичних осіб – підприємців та громадських формувань : Закон України від 15 трав. 2003 р. № 755-IV. *Відомості Верховної Ради України.* 2003. № 31. Ст. 263. URL: https://zakon.rada.gov.ua/laws/show/755-15.

11. Про державну реєстрацію речових прав на нерухоме майно та їх обтяжень : Закон України від 1 лип. 2004 р. № 1952-IV. *Відомості Верховної Ради України.* 2004. № 51. Ст. 553. URL: https://zakon.rada.gov.ua/laws/show/ 1952-15

12. Про Державний земельний кадастр : Закон України від 7 лип. 2011 р. № 3613-VI. *Відомості Верховної Ради України*. 2012. № 8. Ст. 6. URL: https://zakon.rada.gov.ua/laws/show/3613-17

13. Про державну реєстрацію актів цивільного стану : Закон України від 1 лип. 2010 р. № 2398-VI. *Відомості Верховної Ради України.* 2010. № 38. Ст. 509. URL: https://zakon.rada.gov.ua/laws/show/2398-17

14. Про управління об'єктами державної власності : Закон України від 21 верес. 2006 р. № 185-V. *Відомості Верховної Ради України*. 2006. № 46. Ст. 456. URL: https://zakon.rada.gov.ua/laws/show/185-16.

15. Питання Міністерства цифрової трансформації : постанова Кабінету Міністрів України від 18 вересня 2019 р. № 856. URL: https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text

16. Про схвалення Концепції оптимізації системи центральних органів виконавчої влади : розпорядження Кабінету Міністрів України від 27 груд. 2017 р. № 1013-р. URL: https://zakon.rada.gov.ua/laws/show/1013-2017-%D1%80

17. Yuriy Pyvovar, Svitlana Bevz, Valerii Kolpakov, Oksana Myronets, Sergiy Ostrovskiy (2022). State authorities' service function implementation under epidemic threats with the use of legal technologies. *Revista Tecnologia de Sociedade.*v.18, n.50. p.19-36. URL: https://periodicos.utfpr.edu.br/rts/article/view/13921 (ISSN: 1984-3526)

18. Про центральні органи виконавчої влади : Закон України від 17 берез. 2011 р. № 3166-VI. *Відомості Верховної Ради України*. 2011. № 38. Ст. 385. URL: https://zakon.rada.gov.ua/laws/show/3166-17

Радзієвська О. Г.
кандидат юридичних наук, старший дослідник, провідний науковий співробітник Державної наукової установи «Інститут інформації, безпеки і права» НАПрН України

ІНФОРМАЦІЙНІ ПРАВА ТА БЕЗПЕКА ОСОБИ В УМОВАХ СОЦІАЛЬНИХ І ЦИФРОВИХ ТРАНСФОРМАЦІЙ

Технічний та технологічний прогрес створив умови для становлення і розвитку нової формації – суспільства знань, або інформаційного суспільства. Динамічний розвиток та впровадження нових інформаційно-комунікаційних технологій спровокував суттєві соціальні та цифрові трансформації. Сьогодні будь-яка діяльність суспільства нерозривно пов'язана з інформацією та інформаційними технологіями.

Пандемія коронавірусу Covid-19 та спровоковані нею масштабні тривалі карантинні обмеження у всьому світі суттєво прискорили соціальні та цифрові трансформації. Інтенсивний інноваційний розвиток та подальше впровадження нових технологій у виробничій, соціальній та управлінській сферах призводить до дедалі більшої цифровізації суспільства та суттєвих змін у суспільних відносинах. Збільшення кількості та частоти інформаційних обмінів виробничого і невиробничого характеру неминуче призводить до підвищення рівня інформаційної небезпеки у суспільстві. Масштабність та транскордонність інформаційних загроз для людини потребують формування відповідної системи захис-

ту. Система забезпечення інформаційної безпеки в державі вимушена постійно модернізуватися, трансформувати власні підходи і механізми протидії інформаційним небезпекам, пристосовуючись під нові виклики глобального інформаційного простору.

Поряд з видимими викликами для особи, суспільства та держави в інформаційній сфері, такими як інформаційне шахрайство, кіберзлочинність та кібертероризм, неправомірне використання даних з обмеженим доступом, у тому числі порушення правомірності використання персональних даних та ін., є й такі, які приховано діють на індивідуальну і суспільну свідомість. Мова йде про маніпулювання свідомістю за допомогою нових технологій для досягнення економічних чи соціально-політичних цілей.

Так фахівці з Оксфордського інституту інтернету (Oxford Internet Institute) проаналізувавши контент мереж Facebook і Twitter, дійшли висновку, що у більшості розмов, пов'язаних з політикою, присутні спроби маніпулювання інформацією. При цьому, значна частина маніпулятивних дій продукується безпосередньо ботами, тобто створена автономними програмами, здатними виконувати прості одноманітні завдання [1].

Як відомо, ще на початку 2000-х років розпочалося інтенсивне впровадження техніко-технологічних засобів з елементами штучного інтелекту, зокрема було створено програмне забезпечення Cleverbot (розумний бот). Програма була високо оцінена за результатами тесту Тьюринга. Проте Cleverbot вводить в оману більшість людей, створюючи враження, що вони спілкуються зі справжньою людиною. Система запам'ятовування попередніх бесід дозволяє моделювати наступні розмови для Cleverbot, які створюють ефект живого співрозмовника.

Якісне та кількісне наповнення, спродуковане діями інтернет-ботів, здатне суттєво впливати на формування громадської думки і суспільних відносин. Система «запит-відповідь» у соціальних мережах налаштована так, що на запит інформації отримується найбільш популярна відповідь, яку можна згенерувати, у тому числі через використання інтернет-ботів. Тому можемо стверджувати, що інтернет-боти стають суттєвим агентом впливу на формування політичної думки і культури, що у подальшому призведе до трансформацій у політико-правовій системі держави. Підтвердженням зміни політичних та виборчих вподобань через маніпулювання з інформацією є розслідування, що проводяться нині в Сполучених Штатах Америки, щодо втручання у вибори президента у 2017 році.

У 2016 році компанія Facebook запустила тестову версію системи штучного інтелекту Deep Text у програмі Facebook Messenger для аналізу текстової та візуальної інформації з метою збільшення корисної дії ме-

режі для автоматичної допомоги її користувачу, більш якісної фільтрації спаму та небажаної інформації. Про це компанія оголосила на своїй сторінці [2]. Система здатна до навчання та самовдосконалення. Глибинний аналіз повідомлень користувача дозволяє автоматично вивчити його інтереси, звички та спосіб буття. На основі аналізу текстових повідомлень штучний інтелект здатний передбачати наміри користувача, що дає йому можливість запропонувати теоретично бажані товари, послуги чи засоби та інструменти для здійснення потенційно можливих дій. Серед іншого – це персоналізована реклама товарів, послуг, виклик таксі, продаж-купівля через мережу Інтернет, рекомендація новинного контенту, визначеного відповідно до інтересів користувача, тощо.

Проте, подібна система допомоги та інформаційного захисту від соціальної мережі з часом перетворилася на засіб збору інформації про користувача, елементом стеження за ним, переслідування та нав'язування йому товарів і послуг, що порушує його право на приватність. До того ж, реклама товарів і послуг, якими користувач цікавився раніше, є достатньо нав'язливою, що заповнює значну частину інформаційного простору людини.

Така ситуація створює можливість для маніпулювання індивідуальною свідомістю користувача для отримання матеріального чи суспільно-політичного зиску. Через маніпуляції з інформацією складається ситуація, коли людина при внутрішньому психоаналізі, зокрема, у співставленні «бажане – можливе» починає опиратись на штучно створений образ, а не на реально необхідний (бажаний) для неї. Обираючи нав'язаний товар, послугу чи певний стиль поведінки, людина порушує цілісність власної сутності (особистості), підміняє її структурні елементи. Як наслідок – людина придбає той товар, інформація про який мала найбільшу частку в її інформаційному просторі, а не інший рівноцінний йому. Таким чином, при всіх інформаційних можливостях, людина втрачає одне з головних основоположних прав, закріплених у Конституції України [3] та міжнародних правових актах, зокрема Конвенції про захист прав людини і основоположних свобод [4] – свободу вибору.

Крім того, зважаючи на швидкість саморозвитку, які демонструє штучний інтелект на сьогоднішній день, є побоювання щодо його місця у суспільстві майбутнього. Можливості штучного інтелекту крім питань правового та безпекового характеру ставлять перед науковою спільнотою низку питань філософського характеру. Чи зможемо ми управляти такими новими технологіями через програмно-технологічне обмеження діяльності штучного інтелекту задля використання його потенціалу у вирішенні багатьох світових проблем, як стверджував Ролло Карпентер, за-

сновник розумного бота Cleverbot? Чи не переросте він із технологічного засобу виробництва в учасника суспільних відносин та конкурента для людини? Чи не настав час перегляду правового регулювання суспільних відносин, які здійснюються з використанням технологій штучного інтелекту?

Список використаних джерел:

1. Це Їнь Лі Як боти маніпулюють у політичних інтернет-баталіях // *BBC Monitoring, 22 червня 2017 р*. URL: https://www.bbc.com/ukrainian/features-40374518

2. Introducing DeepText: Facebook's text understanding engine (Ahmad Abdulkader, Aparna Lakshmiratan, Joy Zhang) // Posted on Jun 1, 2016. URL: https://code.fb.com/core-data/introducing-deeptext-facebook-s-text-understanding-engine/

3. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. // База даних Законодавство України / ВР України. URL: http://zakon2.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

4. Конвенція про захист прав людини і основоположних свобод: Конвенція Ради Європи від 04.11.1950. // База даних Законодавство України / ВР України. URL: http://zakon2.rada.gov.ua/laws/show/995_004

Валевський О. Л.
доктор наук з державного управління,
провідний науковий співробітник
Національного інституту
стратегічних досліджень

АКТУАЛЬНІ ЗАВДАННЯ РОЗВИТКУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРІ КУЛЬТУРИ

В Україні про необхідність цифрової трансформації діяльності закладів культури, зокрема музеїв, архівів та бібліотек, ідеться, як мінімум, упродовж останнього десятиріччя. Вимога щодо розвитку інформаційних технологій у сфері культури прописана у багатьох урядових програмах і документах, що визначають державну культурну політику. Серед останніх можна вказати на Програму діяльності уряду (червень 2020 р.) та «Вектори економічного розвитку до 2030 року».

Застаріла матеріально-технічна база та неналежний стан об'єктів культурної спадщини створюють загрозу їх знищення та втрати куль-

турного надбання. За даними Міністерства культури та інформаційної політики України (МКІП), в українських музеях зберігається близько 12 млн об'єктів, що мають культурну цінність. Звісно, переважна більшість з них не експонується і не відома широкому загалу. Забезпечити доступність культурного надбання можна лише через оцифрування, а наразі в Україні майже всі реєстри об'єктів музейних фондів зберігаються у паперовому вигляді. За даними МКІП, в електронному вигляді документацію здійснюють тільки 10–15 % музеїв [1]. Тому актуальним завданням є створення онлайнового реєстру, який би містив вичерпну інформацію про об'єкти спадщини. Також анонсовано реалізацію проєкту Є-Музею, у рамках якого передбачається створення Єдиного порталу культурних цінностей Музейного фонду України.

Окремий напрям цифрової трансформації сфери культури – це забезпечення населення якісними та сучасними бібліотечними послугами.

Згідно з наявними статистичними даними, лише 41 % публічних бібліотек мають комп'ютери, 33 % бібліотечних закладів підключені до інтернету. За експертними висновками, українська мережа бібліотек за рівнем інформатизації та рівнем використання програмного забезпечення на 20-25 років відстає від сучасного світового рівня [2].

На порядку денному залишається реалізація раніше анонсованих проєктів щодо створення у бібліотечній сфері Національної системи централізованої каталогізації та Національної електронної бібліотеки України. Також залишаються багато в чому не реалізованими вимоги Закону України «Про доступ до архівів репресивних органів комуністичного тоталітарного режиму 1917 – 1991 років» у частині вільного доступу до інформації репресивних органів, зберігання та оцифровування носіїв архівної інформації.

Під час воєнної агресії росії застосування інформаційних технологій у сфері культури України стало потужним чинником консолідації суспільства та засобом донесення до світової громадськості масштабів воєнних злочинів рф. Зокрема, слід вказати на реалізацію проєкту Culture Crimes, який надає інформацію про об'єкти інфраструктури культурних закладів та культурної спадщини, що постраждали від воєнних злочинів російської армії. На сьогодні в базі даних зафіксовано понад 500 пошкоджених та зруйнованих об'єктів культурної спадщини і культурних установ України [3].

У цьому контексті слід згадати нещодавню ініціативу країн «Люблінського трикутника» (Польща, Литва, Україна) з оцифрування культурної спадщини в Україні. Ця ініціатива передбачає цифровізацію українських

об'єктів матеріальної та нерухомої культурної спадщини з метою їх збереження, а також створення цифрової платформи для їх популяризації.

Серед проєктів, які підтримуватиме ЮНЕСКО у сфері цифрової трансформації культури, є підтримка створення Національної цифрової платформи культурної спадщини України. Як зазначається МКІП, реалізація проєкту забезпечить, зокрема, можливість надання об'єктам нерухомої спадщини України статусу Enhanced Protection для посиленого їх захисту та автоматичного визнання військовим злочином руйнування окупантами об'єктів культурної спадщини [4].

Воєнна агресія рф на певний час завадила виконанню раніше прийнятих рішень щодо впровадження цифрових технологій у сферу культури України. Водночас численні втрати культурних цінностей унаслідок воєнних дій підтвердили актуальність цифрової трансформації об'єктів спадщини, передусім, з метою їх збереження.

Причини невиконання прийнятих планів щодо цифрової трансформації музеїв, архівів та бібліотек відомі – це чимала вартість інновацій, нестача фінансових ресурсів, відсутність належної матеріально-технічної бази та обладнання для оцифровування документів, а також брак фахівців.

Реалізації цих завдань також заважають як низка технологічних проблем, що пов'язуються із незадовільною матеріально-технічною базою закладів культури, так і економічних: хронічне бюджетне недофінансування, низька оплата праці і, відповідно, неможливість залучення фахівців.

Крім цих відомих перешкод, варто вказати на ще одну – управлінську неспроможність. Її суть полягає в тому, що наразі не сформована єдина цілісна державна політика цифрової трансформації сфери культури.

Нині маємо кілька програмних документів щодо розвитку інформаційних технологій у сфері культури та охорони історичної спадщини, які подекуди непогоджені один з одним. Як наслідок – кожне відомство переймається своєю ділянкою впровадження цифрових технологій. Це призводить до розпорошення обмежених фінансових ресурсів та зменшує ефективність зусиль органів управління у справі цифрової трансформації, коли кожен сектор має власну «стратегію» і опікується тільки нею.

Тому існує нагальна потреба у схваленні узагальненого стратегічного документа державної політики у сфері цифрової трансформації культури, у якому було б визначено концептуальні, технологічні та інституційні засади цього процесу. Отже, на порядку денному стоїть питання визначення шляхів цифрової трансформації культури, які були б викладені в єдиному стратегічному документі.

У цьому плані важливо звернути увагу на те, що запровадження ІТ-технологій у закладах культури не є самоціллю. Загальна мета цифрової трансформації – це створення умов для формування соціокультурної ідентичності, розвитку людини, яка б могла ефективно функціонувати у сучасному світі, що швидко змінюється. Тому ідея створення узагальненої стратегії цифрової трансформації культури – це насамперед створення ідентичності та забезпечення в тому числі й гуманітарної безпеки суспільства.

Наявність такої стратегії, яка в ідеалі мала бути схваленою Верховною Радою України, надала б процесу цифрової трансформації більш системного характеру, сприяла б підвищенню ефективності міжнародної технічної допомоги і, головне – забезпечила б стабільне бюджетне фінансування та консолідовану діяльність органів управління у досягненні загальної мети.

Також наявність законодавчо схваленого стратегічного документа цифрової трансформації стане вагомим чинником у відстоюванні інтересів і потреб культурної сфери перед політиками та управлінським істеблішментом, які часом сприймають їх як непріоритетні. Очевидно, що стратегія цифрової трансформації культури має створюватися із залученням широкого кола представників експертної спільноти, недержавних структур, управлінців, фахівців у сфері інформаційних технологій.

Це завдання набуває особливої актуальності в контексті набуття Україною статусу кандидата на членство в Європейському Союзі, а відтак і вимогою щодо адаптації законодавства України до права Європейського Союзу.

За показником культурного впливу в довоєнному 2021 р., за даними рейтингу Best Countries 2021, Україна посідала 62-ту позицію із 85-ти можливих [5]. Цей показник вказує на рівень впливу країни у сфері креативних індустрій та наскільки її культурний продукт є престижним і впізнаваємим. Зважаючи на певну умовність глобальних рейтингів, тим не менш, такий результат свідчить, що Україні потрібно більш ефективно розвивати культурний потенціал і просувати свої культурні надбання, передусім, за допомогою цифрових технологій.

Цифрова трансформація сфери культури та розвиток цифрових видів мистецтва сприятиме посиленню людського капіталу, підвищуватиме рівень креативності та конкурентоспроможності суспільства, що, у свою чергу, сприятиме появі нових професій, особливо у сфері креативних індустрій. У сукупності це забезпечить розвиток інноваційної культури та інтеграцію України у світовий культурний простір.

Список використаних джерел:

1. МКІП розповіло про діджиталізацію національної спадщини та цифрові культурні проєкти під час війни // URL: https://detector.media/infospace/article/200142/2022-06-15-mkip-rozpovilo-pro-didzhytalizatsiyu-natsionalnoi-spadshchyny-ta-tsyfrovi-kulturni-proiekty-pid-chas-viyny/

2. Бруй О. Відставання на 20 років: цифрова трансформація бібліотек та реальні можливості змін URL:// https://chytomo.com/vidstavannia-na-20-rokiv-tsyfrova-transformatsiia-bibliotek-ta-realni-mozhlyvosti-zmin/

3. Зруйнована культурна спадщина України // URL: https://culturecrimes.mkip.gov.ua

4. МКІП та ЮНЕСКО продовжують співпрацю для захисту культурної спадщини України // https://mkip.gov.ua/news/7382.html

5. Methodology: How the 2022 Best Countries Were Ranked. Cultural Influence URL: https://www.usnews.com/news/best-countries/rankings/influence

Дубняк М. В.
кандидат юридичних наук, старший викладач кафедри інформаційного, господарського та адміністративного права, Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» с.н.с. наукової лабораторії теорії цифрової трансформації і права, Державної наукової установи «Інститут інформації, безпеки і права» НАПрН України ORCID: https://orcid.org/0000-0001-7281-6568

ОБРОБКА ПЕРСОНАЛЬНИХ ДАНИХ ДЛЯ ВИЗНАЧЕННЯ МІСЦЯ ПОСТАЧАННЯ ЕЛЕКТРОННИХ ПОСЛУГ

Збільшення обсягу товарів і послуг, які учасники цифрової економіки здійснюють з використанням мережі Інтернет, обумовлює збільшення обсягу обробки даних, необхідних як для доставки замовлення сторонами угоди, так і виконання податкових зобов'язань.

Розвиток та поширення технологій надання електронних послуг створило для компаній умови, за яких реалізація власного продукту здійснюється незалежно від фізичної присутності компанії на території України.

Надання компаніями нерезидентами електронних послуг для фізичних осіб, які не мають статусу суб'єкта господарювання, не дозволяє ефективно реалізувати правила оподаткування податком на додану вартість (далі – ПДВ). Це призводить до втрат державного бюджету та створює неконкурентне середовище для резидентів-платників. Тим самим, порушуються базові принципи рівності та нейтральності оподаткування платника податків [1].

Для удосконалення порядку оподаткування ПДВ операцій з постачання нерезидентами електронних послуг фізичним особам, врегульовано питання визначення місцезнаходження постачання електронних послуг у Податковому кодексі України, який було доповнено статтею 186.3-1 (*положення статті набрали чинності 03.06.2021, законопроект № 4184 від 02.10.2020).* Ця стаття встановлює, що місцем постачання електронних послуг вважається місцезнаходження отримувача послуг і встановлює перелік відомостей, які можуть враховуватись для визначення місцезнаходження. Зокрема, це:

- інформація про країну встановлення лінії фіксованого зв'язку — провайдера комунікацій, послугами якого користувався одержувач у процесі отримання послуги;
- мобільний код країни SIM-карти, яка використовується під час отримання послуги;
- країна, де розміщуються інші засоби зв'язку, які використані для отримання послуги;
- місцезнаходження пристрою за IP-адресою, що використовувалося отримувачем електронної послуги;
- платіжна адреса фізичної особи – отримувача послуг;
- банківські реквізити, зокрема місце ведення банківського рахунка, використаного для розрахунку за електронні послуги;
- інша комерційно важлива інформація [2].

Але чи відносяться дані про "мобільний код країни SIM-карти" та "IP-адреса пристрою" до персональних даних, що потребують правового захисту, чи обізнаності суб'єкта даних про мету їх збору та обробки? Законодавство України про захист персональних даних давно потребує системного доопрацювання, удосконалення та впровадження європейських стандартів захисту даних. Чинним законодавством не врегульовано питання про обробку персональних даних, отриманих у процесі використання мережі Інтернет та засобів зв'язку.

Комітетами Верховної Ради України напрацьовано декілька законопроектів щодо удосконалення законодавства про захист персональних даних. У цілях нашого дослідження, зупинимось на останньому проекті.

Відповідно до проекту Закону України "Про захист персональних даних" № 8153 від 25.10.2022 "Персональні дані *(далі ПД)* - це будь-яка інформація, що стосується фізичної особи, яку ідентифіковано або може бути ідентифіковано". В даному законопроекті пропонується стаття 17 такого змісту: "Використання технологій відстеження дій суб'єктів персональних даних у електронних комунікаціях та сервісах". Цією статтею, зокрема, буде встановлено заборону відстеження дій суб'єктів персональних даних за допомогою програмного забезпечення, мобільних чи інших застосунків, веб-сайтів, інших технологій електронних комунікацій та сервісів, а також за допомогою пристроїв, які належать чи використовуються суб'єктом персональних даних. Обробка таких даних дозволяється при дотриманні принципів обробки ПД. Зокрема, надання згоди суб'єктом ПД на таку обробку, обробка необхідна для забезпечення функціонування програмного забезпечення, для надання послуги, чи забезпечення безпеки обробки ПД. Контролери і оператори, які здійснюють таку обробку повинні забезпечити, щоб кожний суб'єкт, чиї дані будуть оброблятися, ознайомився з повідомленням про таку обробку до її початку.

Крім того, у разі прийняття законопроекту № 8153, Закон України «Про електронні комунікації» пропонують доповнити статтею 31-2 «Таємниця приватного спілкування», яка передбачає наступне. Спілкуванням є передавання інформації у будь-якій формі від однієї особи до іншої безпосередньо або за допомогою електронних комунікацій будь-якого типу. Таємниця приватного спілкування охоплює, зокрема: 1) зміст спілкування; 2) дані трафіку; 3) дані про місцезнаходження споживача електронних комунікаційних послуг, до яких відносяться будь-які дані, що обробляються при наданні електронних комунікаційних послуг, в тому числі, щодо розташування термінального обладнання; 4) факти та обставини, за яких мало місце припинення або невстановлення з'єднання. Постачальник електронних комунікаційних мереж та/або послуг та інші особи, залучені у процес діяльності засобів електронних комунікацій будь-якого типу, передачу інформації системами електронних комунікацій, повинні зберігати таємницю приватного спілкування після закінчення їх діяльності, на яку поширювалося зобов'язання збереження таємниці [3].

Висновки. Законопроектом № 8153 встановлюється правовий режим захисту даних, які можуть збиратись у зв'язку із особливостями технічного використання мережі Інтернет та засобів зв'язку, саме через те, що комбінації цих даних у процесі обробки можуть забезпечити ідентифікацію фізичної особи. Наразі в процесі обробки жоден суб'єкт персо-

нальних даних не володіє інформацією, про вже зібрані дані про нього, які у поєднанні можуть спричинити ідентифікацію особи. Таким чином, дані про IP-адресу пристрою відносяться до персональних даних, та даних, які підпадатимуть під редакцію п.3. ч.2 нової статті 31-2 «Таємниця приватного спілкування» законопроекту № 8153. Обробка цих даних вимагає дотримання принципів і підстав обробки персональних даних контролером/оператором.

Під час прийняття законопроекту № 4184 від 02.10.2020 «Про внесення змін до Податкового кодексу України... про удосконалення порядку оподаткування податком на додану вартість операцій з постачання нерезидентами електронних послуг фізичним особам» не було запропоновано відповідних змін для чинного законодавства про захист персональних даних, чи Закону України «Про електронну комерцію» який би встановлював обов'язок для суб'єктів електронної комерції повідомляти споживача послуг, про те, що дані про IP-адресу, платіжну адресу, реквізити банківського рахунку, та інші комерційні дані, збираються та обробляються не лише з метою надання послуг електронної комерції, а і з метою визначення місця надання електронних послуг для виконання вимог податкового законодавства.

На нашу думу, у згоді на обробку ПД має чітко зазначатись мета і всі цілі обробки ПД, для того, щоб суб'єкт ПД міг розуміти та оцінити масштаби збору даних про нього і сфери їх використання. При цьому визначення загальної мети обробки, наприклад: «для виконання умов чинного законодавства» без зазначення переліку даних, які можуть бути використані в різних цілях обробки не відповідає сучасним принципам та стандартам у сфері захисту персональних даних.

Список використаних джерел:

1. Пояснювальна записка до законопроекту № 4184 від 02.10.2020 «Про внесення змін до Податкового кодексу України щодо скасування оподаткування доходів, отриманих нерезидентами у вигляді виплати за виробництво та/або розповсюдження реклами та удосконалення порядку оподаткування податком на додану вартість операцій з постачання нерезидентами електронних послуг фізичним особам» https://itd.rada.gov.ua/billInfo/Bills/CardByRn?regNum=4184&conv=9

2. Податковий кодекс України № 2755-VI, редакція від 28.10.2022. https://zakon.rada.gov.ua/laws/show/2755-17#Text

3. Проект Закону України "Про захист персональних даних" № 8153 від 25.10.2022.

Касперський І. П.
кандидат юридичних наук, старший науковий співробітник, доцент доцент спеціальної кафедри Національної академії Служби безпеки України

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ПРИНЦИПІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У ПРОЦЕСАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Питання захисту персональних даних в умовах війни набуває все більшої актуальності, особливо в частині готовності державних структур до захисту величезного обсягу інформації стосовно громадян, яку було зібрано на виконання функцій держави. Важливість захищеності цих масивів підтверджено і тим, що у перші дні повномасштабного вторгнення було прийнято вимушене рішення щодо припинення доступу до державних реєстрів, що ускладнило пошук окупантами підстав до обмеження прав громадян України.

Крім того, необхідність забезпечення європейських стандартів захисту персональних даних випливає не тільки із зовнішньополітичного курсу України на європейську інтеграцію, а і є прямим обов'язком нашої держави виходячи із її міжнародних зобов'язань, що випливають із ратифікації 108-мої Конвенції Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» [1]. Положення названої Конвенції було подвійно імплементовано у національне законодавство: шляхом прийняття окремого Закону про ратифікацію [2] і шляхом закріплення її базових положень у прийнятому у зв'язку із цією ратифікацією Законі України «Про захист персональних даних» [3].

Названими нормативними актами зокрема закріплено необхідність неухильного дотримання принципу функціональної достатності при зборі персональних даних, що означає, що обсяг персональних даних, які збираються конкретним володільцем, не повинен бути надмірним стосовно мети їх збору. Ціль запровадження цього принципу є очевидною – убезпечення громадян від масового витоку всебічних персональних даних та обмеження володільців у зборі персональних даних, необхідність у яких відсутня у зв'язку зі змістом функціональної спрямованості конкретного володільця чи розпорядника даних.

Справжнім викликом забезпеченню даного принципу стало створення в Україні Єдиного державного вебпорталу електронних послуг під назвою «Дія». Згідно із Положенням про Єдиний державний вебпортал

електронних послуг завданнями його запровадження було зокрема надання громадянам електронних публічних послуг, забезпечення доступу до отримання фінансових послуг та забезпечення через електронний кабінет користувача доступу до інформації з національних електронних інформаційних ресурсів [4].

На сьогодні кабінет користувача порталу «Дія» фактично виступає агрегатором досить суттєвого обсягу даних щодо громадян України, які отримуються через портал із загальнодержавних реєстрів персональних даних. Ці ризики помножено на дуже велику кількість користувачів – більше 13 млн. з них користуються мобільним додатком, ця цифра стоїть окремо від такої ж кількості користувачів, що взаємодіють з ресурсом через веб-портал [5].

Попри запевнення міністра цифрової трансформації М. Федорова у тому, що «Дія не збирає та не зберігає особисту інформацію про українців, а лише відображає дані, що містяться у державних реєстрах» [6] ознайомлення зі змістом веб-ресурсу «Дії», на якому з дотриманням вимог чинного законодавства оприлюднено повідомлення про обробку персональних даних, дозволяє зробити висновок про протилежне: все-таки не тільки прізвище, ім'я та по батькові особи, а і серія та номер паспорта, дата народження, зареєстроване або фактичне місце проживання, реєстраційний номер облікової картки платника податків громадянина України а також адреса електронної пошти та номери контактних телефонів таки потрапляють в обробку, яку безпосередньо здійснює розпорядник даних – державне підприємство «Дія» [7].

Потреба в обробці наведених даних є зрозумілою, бо їх наявність дозволяє ідентифікувати конкретного користувача та формувати запит до відповідних державних реєстрів із конкретними пошуковими характеристиками.

Фахове середовище докладно дослідило зміст ресурсів «Дії» і дійшло висновку, що зазначений масив даних – це лише перша частина того, що зберігається в «Дії», насправді ресурс значно масивніший. У ньому є ще два додаткових архіви: один містить фото різних документів користувачів: паспортів, трудових книжок, свідоцтв про шлюб тощо, інший – слабоструктурована база записів з різноманітними даними: як із основною задекларованою для офіційної обробки персональною інформацією, так і з додатковою, наприклад інформація про запит на отримання батьківської допомоги («єМалятко»), заяви на реєстрацію ФОП та квитанції про оплату послуг [8].

Такий стан справ, коли слова міністра розходяться із даними веб-порталу його ж ресурсу, а сам веб-портал лише частково виконує вимоги

законодавства щодо прав суб'єктів персональних даних знати про те, яка інформація про них обробляється, наводить на сумні думки про виправданість довіри наших громадян до державних онлайн-сервісів та електронних реєстрів не користуватись якими на сьогодні неможливо.

Ця картина цілком корелює із результатами такого ж ставлення до захисту персональних даних і суб'єктів приватного права: час від часу медіапростір розбурхують повідомлення про витік інформації з того чи іншого ресурсу, при чому причиною цих повідомлень стають не зізнання володільців і розпорядників даних, а конкретні пропозиції із продажу величезних масивів інформації на чорному ринку [9], пропозиції із надання нелегальних послуг зі збору даних про конкретну особу через месенджери [10], або в кращому випадку звіти правоохоронців щодо їх реакції на витоки [10, 11].

Природно, що активність протиправних елементів кіберспільноти не оминула і ресурсу «Дія». У січні цього року з'явились повідомлення виставлення на продаж на форумі RAID за $ 15 000 особистих даних двох мільйонів громадян, що зберігались сервісом «Дія». Мова йшла про індивідуальні податкові номери, номери телефонів, дані паспортів та банківських карток, а також фото документів. Крім того, на підтвердження джерела даних було одночасно виставлено на продаж закриту інформацію державного підприємства «Дія» та всі файли структури порталу «Дія» [12]. За повідомленнями ІТ- середовища ціна цієї бази даних досягла $ 80 000, після чого посилання на продаж стало недійсним, що вірогідно свідчить про успішну угоду [8].

У відповідь на цю ситуацію згаданий М. Федоров знову заперечив наявність персональних даних на веб-порталі «Дія» і запевнив, що даний витік пов'язаний із базами даних «одного популярного банку». У якості заходів реагування Міністерство цифрової трансформації вирішило запустити у додатку «Дія» найближчим часом послугу «єЗахист», завдяки якій кожен користувач зможе дізнатися про базові правила кібербезпеки, а також в яких реєстрах є інформація про нього [5].

Фахове ІТ- середовище не поділяє оптимізму міністра стверджуючи, що викладені на продаж дані є автентичними, отже витік найімовірніше стався з ресурсу «Дія» [8].

Не вдаючись до технічних подробиць вразливості ресурсу «Дія», які було виявлено після витоку даних, варто зазначити, що найбільшу помилку було допущено з самого початку – з архітектури ресурсу, який має автоматизовані можливості звернення на запит користувача до численних електронних реєстрів. По факту треба вести мову про штучне об'єднання державних реєстрів, що за твердженням правозахисної ор-

ганізації Privacy International, становить серйозну загрозу безпеці даних [15]. Ситуація, коли за одним незмінюваним ідентифікатором користувачу надається доступ до різних за своєю метою збору ресурсів, є прямим порушенням закріплених законодавством України міжнародних принципів обробки персональних даних і ставить під загрозу не тільки конфіденційність, а і цілісність створених за бюджетні кошти величезних масивів необхідної громадянам, суспільству і державі інформації.

Прийнятний вихід з даної ситуації – зламати конфігурацію централізованого доступу, коли до кожного ресурсу чи реєстру користувач міг би звернутися лише окремо, використовуючи при цьому змінювані за своїм наповненням різні засоби надійної ідентифікації. Це може незначно ускладнити лише швидкість отримання доступу до конкретного ресурсу, проте убезпечить від одночасного витоку величезних масивів персональних даних.

Список використаних джерел:

1. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Страсбург, 28 січня 1981 року // Офіційний вісник України від 14.01.2011 — 2011 р., № 1, / № 58, 2010, ст. 1994 /, стор. 701, стаття 85, код акта 54293/2011
2. Закон України «Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних» // Офіційний вісник України від 09.08.2010 — 2010 р., № 58, стор. 46, стаття 1994, код акта 52188/2010
3. Закон України «Про захист персональних даних» // Офіційний вісник України від 09.07.2010 – 2010 р., № 49, стор. 199, стаття 1604
4. Положення про Єдиний державний вебпортал електронних послуг: затв. Постановою Кабінету Міністрів України № 1137 від 04.12.2019 (в ред Постанови Кабінету Міністрів України № 937 від 16.08.2022) // Офіційний вісник України від 06.09.2022 — 2022 р., № 69, стор. 7, стаття 4171, код акта 113366/2022
5. Telegram contact @zedigital message edited Jan 22 at 12:18 URL: https://t.me/zedigital/970
6. Майбутнє — за технологіями, сьогодення — за «Дією»: інтерв'ю з очільником Мінцифри Михайлом Федоровим від 22 листопада 2021р. URL: https://kanaldom.tv/budyashhee-za-tehnologiyami-nastoyashhee-za-diyeyu-intervyu-s-glavoj-minczifry-mihailom-fedorovym/
7. Повідомлення про обробку персональних даних порталу «Дія» URL: https://diia.gov.ua/policy

8. З «Дії» чи ні? Звідки хакери взяли персональні дані 2 млн українців. Розслідування DOU https://dou.ua/lenta/articles/inquiry-about-diia-data-leak/

9. 53 мільйони! В Інтернеті виявлено базу даних усіх українців URL: https://uain.press/news/i-mertvih-i-zhivih-v-interneti-viyavleno-bazu-personalnih-danih-usih-ukrayintsiv-1455854

10. Мінцифри: «Дія» не зливає дані, незаконними телеграм-каналами займається СБУ URL: https://www.pravda.com.ua/news/2020/05/12/7251282/

11. Витік персональних даних: влада розповіла про джерела, обшуки й підозри URL: https://www.pravda.com.ua/news/2020/06/25/7257085/

12. Кіберполіцейські вилучили з незаконного обігу бази персональних даних понад 300 мільйонів осіб URL: https://cyberpolice.gov.ua/news/kiberpoliczejski-vyluchyly-z-nezakonnogo-obigu-bazy-personalnyx-danyx-ponad--miljoniv-osib-7493/

13. Повідомляють про масштабний злив даних користувачів «Дія», Мінцифри це заперечує URL: https://dou.ua/lenta/news/diia-data-leak-2022/

14. Національні ідентифікаційні картки (посвідчення особи). Заява Прайвесі Інтернешнл для Комітету Парламенту Канади з питань громадянства та імміграції від 04.10.2003 // Свобода висловлювань і приватність, 2004, № 1

Величко М. В.
кандидат біологічних наук, старший науковий співробітник, професор Національної академії Служби безпеки України

АКТУАЛЬНІ ПРОБЛЕМИ НОРМАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ ТА ШЛЯХИ ЙОГО ВДОСКОНАЛЕННЯ

У лютому 2017 року в період агресії росії проти нашої держави, за ініціативою України та під час її головування в РБ ООН було внесено на розгляд та ухвалено першу в історії резолюцію РБ ООН 2341 щодо захисту критичної інфраструктури від терористичних атак. На відкритті засідання головуючий Постійний представник України при ООН Во-

лодимир Єльченко, аргументуючи важливість розгляду міжнародною спільнотою питання терористичних викликів критичній інфраструктурі та пошуку ефективних шляхів протидії, наголосив, що це стосується насамперед сфер телекомунікації, промисловості, транспорту, нафто- та газовидобування [1]. Важливість зазначеного підтвердилася 24 лютого цього року, уже після повномасштабної воєнної агресії росії проти України. З першого дня повномасштабного вторгнення росія у повній мірі застосувала проти України усі види атак, включаючи і кібернетичне та інформаційне поле. Одними із пріоритетних об'єктів ураження агресором стали об'єкти критичної інфраструктури, особливо енергетичний сектор економіки держави, проти яких ворог застосовував і далі застосовує не тільки зброю, але й кібератаки, інформаційні диверсії тощо.

Наявне нормативно-правове забезпечення як інформаційної, так і кібернетичної безпеки критичної інфраструктури мирного часу, в умовах воєнного стану потребує прискореного вдосконалення відповідно до нових загроз. На сьогодення правозабезпечення критичної інфраструктури держави здійснюється на основі наступної нормативно-правової бази. Законодавство про критичну інфраструктуру та її захист складають закони України: Конституція України, Закон України «Про національну безпеку України», Закон України «Про критичну інфраструктуру», Закон України «Про захист інформації в інформаційно-комунікаційних системах», Закон України «Основні принципи кібербезпеки України», Закон України «Про основні засади забезпечення кібербезпеки України», Закон України «Про утворення Державної служби захисту критичної інфраструктури та забезпечення національної системи стійкості України» та ін.; постанови Кабінету Міністрів України: Постанова Кабінету Міністрів України № 1109 «Про деякі питання критичної інфраструктури», Постанова Кабінету Міністрів України № 943 «Про деякі питання критичної інфраструктури» (Порядок формування реєстру; Порядок заповнення реєстру), Постанова Кабінету Міністрів України № 1176 «Про затвердження форми заяви на одержання суб'єктом господарювання або уповноваженою ним особою документів дозвільного характеру», Постанова Кабінету Міністрів України «Про деякі питання проведення незалежного аудиту інформаційної безпеки критичної інфраструктури», Постанова Кабінету Міністрів України «Про положення про організаційно-технологічну модель», Постанова Кабінету Міністрів України «Про деякі питання забезпечення функціонування системи реагування на кіберінциденти та кібератаки», Постанова Кабінету Міністрів України «Про затвердження Порядку перевірки стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформа-

ції, вимога щодо захисту якої встановлена законом», Постанова Кабінету Міністрів України «Про здійснення комплексу організаційно-технічних заходів щодо виявлення вразливостей ІС, на яких обробляються державні інформаційні ресурси»; укази Президента України: Указ Президента України № 254, Указ Президента України № 32; стратегії: Стратегія кібербезпеки України; протоколи: Протокол спільних дій суб'єктів кібербезпеки, міжнародні договори України, згода на обов'язковість яких надана Верховною Радою України (Міжнародний стандарт якості ISO/IEC 27001 – регламентує упорядкований підхід для вирішення проблем інформаційної і кібербезпеки), інші чинні відомчі за зазначеним напрямом нормативно-правові акти держави.

Наразі завдання суб'єктів реалізації положень Стратегії кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни» – вживати в межах своєї компетенції заходів щодо посилення адміністративно-правових, у тому числі й контррозвідувального, режимів на об'єктах критичної структури держави [2]. Відсутність на сьогодення завершеного державного реєстру об'єктів критичної інфраструктури з відповідною таксономією їх стратегічного положення та вразливості від атак агресора в умовах воєнного стану ускладнила ситуацію щодо ефективності інформаційного та кіберзахисту критичної інфраструктури.

Станом на початок широкомасштабного вторгнення росії відповідно до попередніх вимог КМУ від 09.10.2020 № 943 та № 1109 «Деякі питання критичної інформаційної інфраструктури» та «Деякі питання критичної інфраструктури», а також листа Секретаря Ради національної безпеки і оборони України від 11.08.2021 № 3420/16-03/2-21, сімдесят п'ять відсотків державних органів надали інформацію про критичну інфраструктуру та критичну інформаційну інфраструктуру. Зазначена робота продовжується.

Вперше у світовій історії на теренах України виник не прогнозований, а реальний новий вид фронту – кіберфронт. Такий стан речей вимагає швидкого оновлення праворегуляторного механізму названої галузі. Прикладом зазначеного є підписання 3 листопада 2022 року Президентом України Закону України від 18.10.2022 № 2684-IX «Про внесення змін до деяких законів України щодо формування та реалізації державної політики у сфері захисту критичної інфраструктури» до Закону України «Про критичну інфраструктуру» та Закону України «Про Державну службу спеціального зв'язку та захисту інформації України». Метою є сприяння реалізації державної політики у сфері критичної інфраструктури та створення умов щодо виконання функцій уповноваженого органу

з питань захисту критичної інфраструктури України у сфері інформаційної та кібербезпеки держави Державною службою спеціального зв'язку та захисту інформації України [3].

Отже, процес удосконалення правової основи захисту критичної інфраструктури держави в умовах воєнного стану є безперервним. Державна система забезпечення захисту та стійкості критичної інфраструктури від інформаційних та кібератак має гарантувати забезпечення населення, суспільства, економіки й держави життєво важливими товарами і послугами на мінімально необхідному рівні упродовж встановленого часу. Основним завданням системи державного управління та регулювання у цій сфері є формування взаємовідносин держави, суспільства та суб'єктів господарювання з метою створення умов, що забезпечать функціонування державної системи захисту критичної інфраструктури; передбачається формування нормативно-правової бази на загальнодержавному, регіональному, галузевому (відомчому) та на місцевому рівнях.

Відповідно, пріоритетними напрямами вдосконалення правової основи діяльності державної системи захисту критичної інфраструктури необхідно визначити:

- вдосконалення ефективності наявної системи державного управління у сфері захисту критичної інфраструктури. Це у свою чергу вимагатиме приведення у відповідність до законодавства ЄС вітчизняної законодавчої та нормативно-правової бази, а також прийняття інституційно-організаційних рішень в частині визначення завдань, повноважень і відповідальності залучених органів державної влади, суб'єктів господарювання та населення;
- забезпечення єдності методологічних засад діяльності суб'єктів системи державного управління у сфері захисту критичної інфраструктури, що передбачає узгодження розробки нормативно-методичних і науково-технологічних інструментів усіх залучених суб'єктів;
- розбудова державно-приватного партнерства для підвищення безпеки та забезпечення стійкості національної критичної інфраструктури, що вимагає чіткого правового врегулювання сфер відповідальності та зобов'язань держави і власників / операторів критичної інфраструктури;
- налагодження системи обміну інформацією: збір, аналіз та обробка інформації щодо загроз і ризиків для критичної інфраструктури, уразливостей та характеристик систем захисту елементів критичної інфраструктури.

Список використаних джерел:

1. Електронний ресурс – режим доступу: https://m.facebook.com/UkraineMFA/posts/enua-ukraine-initiated-the-un-security-council-arria-formula-meeting-on-the-prot/1149392788447973/

2. Указ Президента України від 26 серпня 2021 року № 447/2021 «Стратегія кібербезпеки України. Безпечний кіберпростір – запорука успішного розвитку країни» // Електронний ресурс-режим доступу: https://www.president.gov.ua/documents/4472021-40013

3. Закон України від 18.10.2022 № 2684-IX «Про внесення змін до деяких законів України щодо формування та реалізації державної політики у сфері захисту критичної інфраструктури» // Електронний ресурс-режим доступу: https://radnuk.com.ua/novyny/prezydent-pidpysav-zakon-pro-vnesennia-zmin-do-deiakykh-zakoniv-ukrainy-shchodo-formuvannia-ta-realizatsii-derzhavnoi-polityky-sferi-zakhystu-krytychnoi-infrastruktury/

Єфіменко А. Г.
аспірантка кафедри інтелектуальної власності та інформаційного права навчально-наукового інституту права Київський національний університет імені Тараса Шевченка

«ПРИВАТНЕ ПРАВОСУДДЯ» У КОНТЕКСТІ ВИРІШЕННЯ СПОРІВ ЩОДО ЗАХИСТУ АВТОРСЬКОГО ПРАВА НА ОНЛАЙН-ПЛАТФОРМАХ В РАМКАХ ПРАВА НА СПРАВЕДЛИВИЙ СУД

Цифрові платформи, що надають доступ до великої кількості захищеного авторським правом контенту, стали засобом надання ширшого доступу до великого масиву результатів творчої діяльності і пропонують великі можливості для креативних індустрій щодо розвитку нових бізнес-моделей та комерціалізації об'єктів, що захищаються авторським правом. Однак, незважаючи на те, що вони забезпечують різноманітність і легкість доступу до контенту, такі платформи також створюють виклики та ризики, коли твори завантажується без попереднього дозволу правовласників. Постає питання у обсязі юридичної відповідальності як і користувачів, так і самих платформ. Ця невизначеність впливає на здатність правовласників визначати, чи використовуються як за яких умов використанні твори, що належать їм як первинним або вторинним пра-

вовласникам. Окремим питанням такої невизначеності є забезпечення основоположних прав та свобод користувачів (право на свободу слова, право на інформацію тощо) та авторських прав правовласників.

Українське законодавство наразі не містить спеціального визначення для таких платформ, тому вважаємо необхідним посилатися на статтю 2(6) Директиви (ЕС) 2019/790 про авторське право та суміжні права на єдиному цифровому ринку та внесення змін до директив 96/9/ЕС та 2001/29/ЕС (далі – Директива 2019/790), яка визначає «постачальників послуг щодо обміну контентом онлайн» (далі за текстом – онлайн-платформи) як постачальника послуг інформаційного суспільства, основною або однією з основних цілей якого є зберігання та надання доступу громадськості до великої кількості захищених авторським правом творів або інших захищених об'єктів, завантажених своїх користувачів, які він організовує та просуває з метою отримання прибутку [1].

Онлайн-платформи у своїй діяльності та регулюванні відносин зі своїми користувачами покладаються на Умови надання послуг/Умов використання Спільноти або Стандарти/Рекомендації щодо регулювання та поведінки користувачів та модерації. Ці Умови та Стандарти/Рекомендації не обов'язково відображають зміст конкретної правової системи, але в своїй основі містять законодавство Сполучених Штатів Америки як країни походження більшості онлайн-платформ [2].

Така ситуація призводить до створення наступних викликів: онлайн-платформи, зловживаючи своїм екстериторіальним характером та сферою впливу, створюють власні правові системи та формують порядок вирішення спорів в рамках власних екосистем. По-перше, при здійсненні модерації контенту виникає проблема точності або достовірності такої модерації, тобто система оцінки законного або незаконного походження контенту, а також проблема приватизації правосуддя, що проявляється як у створені дисбалансу між інтересами правовласників та інтересами користувачів, так і формування додаткових вимог до контенту, що можуть підпадати під систему захисту авторським правом, але не будуть відповідати правилам та політикам постачальника та у зв'язку з цим підлягають видаленню. Для оцінки таких викликів та ризиків необхідно звернутися до основоположних процесуальних принципів та проаналізувати їх можливу адаптацію до регулювання системи модерації онлайн-платформами.

Стаття 6 Конвенції про захист прав людини і основоположних свобод (далі – Конвенція) гарантує право на справедливий і публічний розгляд справи упродовж розумного строку незалежним і безстороннім судом, встановленим законом, при визначенні цивільних прав і обов'язків

особи чи при розгляді будь-якого кримінального обвинувачення, що пред'являється особі [3].

Так, відповідно до статті 13 Конвенції, кожен, чиї права та свободи, визнані в цій Конвенції, було порушено, має право на ефективний засіб правового захисту в національному органі, навіть якщо таке порушення було вчинене особами, які здійснювали свої офіційні повноваження [3]. Тобто ефективний спосіб захисту передбачає, в першу чергу, доступ до правосуддя у розумінні наявності належних способів захисту порушених прав.

У 2018 році разом в рамках конференції про Модерацію контенту у Сполучених Штатах, група правозахисних організацій та наукових експертів розробила та запустила набір принципів щодо того, як найкраще забезпечити значущу прозорість та підзвітність інтернет-платформ щодо модерування контенту, створеного користувачами [4].

Також, Принципи Aequitas щодо права на справедливий суд онлайн, що були сформовані у травні 2021 році Інститут цифрових стипендій про сприяння процесу встановлення норм у контексті балансування прав в Інтернеті, таких як свобода слова, захист персональних даних та права інтелектуальної власності тощо. Відповідно до цих принципів права та свободи людини мають лежати в основі регулювання правовідносин на онлайн-платформах, розкривається зміст права на належний розгляд справи на онлайн-платформах, право на представництво та право на апеляцію [5].

У 2019 році генеральний директор YouTube Сьюзен Войчіцкі заявила в дописі в блозі, що компанія почула занепокоєння від творців і що YouTube «досліджує вдосконалення, щоб знайти правильний баланс між власниками авторських прав, творцями та користувачами» [6].

Відповідно до цього звіту, надмірна охорона та захист (як необґрунтоване блокування, так і необґрунтована демонетизація) є цілком реальною проблемою, яка регулярно впливає на права значної кількості завантажувачів.

У зв'язку з цим можна сформувати наступний базис для подальшого розкриття інструментарію для регулювання вирішення спорів щодо порушення авторських прав на онлайн-майданчиках таким чином.

Мають бути забезпечені принципи прозорості, тобто користувачі мають право знати яким чином працює алгоритм (якщо вирішення питання про видалення / не видалення контенту приймає відповідне програмне забезпечення), процедура оскарження такого рішення має бути чітко прописана з фіксацією строків, порядку, а також з залученням кваліфікованої фізичної особи або групи як суб'єкта вирішення спору. Всі учас-

ника процесу також мають бути належним чином проінформовані про порядок надання скарги, вимоги до її змісту та форми, порядок надання зустрічної відповіді або скарги (в залежності від обставин справи). Ці процедурні аспекти по своїй суті мають будуватися на ключових міжнародних актах щодо захисту прав та свобод людини, а також міжнародних договорів у сфері інтелектуальної власності, що наддасть змогу урегулювати поле відносин, що мають екстериторіальний характер. Також важливою складовою урегулювання цього процесу, як вже зазначалося, є необхідність підготовки та підвищення кваліфікації посадових осіб таких онлайн-платформ, що наддасть забезпечити право на належний розгляд справи.

Узагальнюючи, питання «приватизації» правосуддя онлайн-платформами є важливим аспектом не тільки авторського права та системи права інтелектуальної власності як такої, а і основоположних прав та свобод людини. Прикладом початку урегулювання є норми Директиви (ЕС) 2019/790, які покладають на онлайн-платформи додаткові обов'язки в аспекті вирішення спорів щодо порушення авторських прав, але таке регулювання є локальним (в рамках ЄС), точковим та не розкриває весь обсяг необхідних заходів щодо формування підходів саме до процедурних аспектів розгляду таких спорів на платформах.

Список використаних джерел

1. Директива (ЕС) 2019/790 про авторське право та суміжні права на єдиному цифровому ринку та внесення змін до директив 96/9/ЕС та 2001/29/ЕС. Режим доступу: https://eur-lex.europa.eu/eli/dir/2019/790/oj

2. Digital Millennium Copyright Act. Режим доступу: https://www.copyright.gov/legislation/dmca.pdf

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

4. The Santa Clara Principals on Transparency and Accountability in content moderation. Режим доступу: https://santaclaraprinciples.org/

5. Aequitas principles on due process online. Режим доступу: https://aequitas.online/

6. Copyright Transparency Report. Режим доступу: https://blog.youtube/news-and-events/access-all-balanced-ecosystem-and-powerful-tools/

Литвинова Л. А.
кандидатка наук із соціальних комунікацій, завідувачка сектору з охорони інтелектуальної власності Національної бібліотеки України імені В. І. Вернадського

КОНЦЕПЦІЯ ДИРЕКТИВИ ПРО АВТОРСЬКЕ ПРАВО ТА СУМІЖНІ ПРАВА НА ЄДИНОМУ ЦИФРОВОМУ РИНКУ ЩОДО УСТАНОВ КУЛЬТУРНОЇ СПАДЩИНИ ЄС

За останні кілька років Європейський Союз прийняв приблизно п'ятнадцять директив щодо здійснення авторських прав і доступу до інформації та культурної спадщини. Кульмінацією законодавчої діяльності стала Директива 2019/790/ЄС про авторське право та суміжні права на єдиному цифровому ринку (Директива DSM), яку було прийнято 17 травня 2019 року після дуже довгого та трудомісткого законодавчого процесу [1]. Директива DSM не тільки доповнює існуючу структуру законодавчої бази ЄС з авторського права, а й оновлює її у певних вузьких галузях – досліджень, інновацій, освіти та збереження культурної спадщини (п. 4 та п. 5 Преамбули Директиви DSM) – шляхом перетворення деяких факультативних винятків з авторського права на обов'язкові. Зокрема, Розділ II Директиви DSM вводить чотири нові та обов'язкові винятки і обмеження авторського права, що стосуються установ культурної спадщини, а саме: ст. ст. 3-6 вводять обмеження виняткових прав правовласників для адаптації правової бази до цифрового використання творів: інтелектуальний аналіз тексту та даних доступних творів у комерційних та некомерційних дослідницьких цілях, інтелектуальний аналіз тексту та даних для інших цілей, цифрове використання творів у навчальних і освітніх цілях та збереження культурної спадщини. Окрім того, у ст. 8 встановлюється новий механізм ліцензування творів, що вийшли з комерційного обігу. Тобто, всього Директива DSM запроваджує п'ять нових обов'язкових винятків, які принесуть позитивні зміни установам культурної спадщини.

Установа культурної спадщини (cultural heritage institution – CHI) визначається ст. 2(3) Директиви DSM як «загальнодоступна бібліотека або музей, архів або установа зі збереження кіно– або аудіоспадщини». Цікаво, що це визначення частково збігається з визначенням дослідницької організації (ст. 2(1)), але це не викликає жодних практичних проблем, оскільки існує безліч установ, які в своїй діяльності працюють в обох напрямках. Головне, щоб основною метою установи було проведення

наукових досліджень або здійснення освітньої діяльності, що включає також проведення наукових досліджень. Виходячи з цього, національна бібліотека може одночасно бути установою культурної спадщини, дослідницькою установою і навіть освітньою установою. Таким чином, чи буде національна бібліотека в певній державі дійсно мати право на вищезгадані винятки, залежатиме від її ролі, передбаченої національним законодавством.

Директива DSM запроваджує не один, а два нові винятки для інтелектуального аналізу тексту та даних (text and data mining – TDM) (ст. 3 і ст. 4), які мають бути реалізовано всіма державами–членами ЄС. Перший виняток дозволяє оптимально використовувати інтелектуальний аналіз тексту та даних для наукових досліджень науково-дослідними організаціями та установами культурної спадщини, а саме відтворювати твори та інші об'єкти, що охороняються авторським правом (крім програмного забезпечення), а також добувати вміст баз даних. Умовою застосування цього винятку є отримання цими організаціями законного доступу до перерахованих об'єктів. Наприклад, у разі підписки, отриманої дослідницькими організаціями або установами культурної спадщини, особи, прикріплені до них та охоплені цими підписками, повинні вважатися такими, що мають законний доступ. Законний доступ також має охоплювати доступ до контенту, який знаходиться у відкритому доступі в Інтернеті. Відповідно до цього винятку установи культурної спадщини можуть надсилати текстові повідомлення та аналізувати дані про всі твори, що знаходяться в їх колекціях, якщо це відбувається з метою наукових досліджень.

Виняток чи обмеження відповідно до ст. 4 дозволяє будь–якому користувачеві (включаючи установи культурної спадщини) відтворювати твори та інші об'єкти, що охороняються авторським правом, а також добувати вміст баз даних для проведення інтелектуального аналізу текстів та даних з будь-якою метою, що сприятиме розвитку аналітики даних та штучного інтелекту в ЄС. Цей виняток стосується лише тих матеріалів, які доступні на законних підставах і щодо яких правовласники прямо не заборонили таке використання.

Разом ці два винятки надають установам культурної спадщини широкі можливості для інтелектуального аналізу текстів та даних. У тих випадках, коли правовласники зарезервували свої права і не можуть покладатися на загальний виняток, запроваджений у ст. 4, вони можуть повернутись до конкретного винятку щодо наукових досліджень у ст. 3. Важливо розуміти, що такий виняток для наукових досліджень застосовується не тільки в ситуації, коли установа культурної спадщини про-

водить дослідження, а й коли вона дозволяє стороннім дослідникам проводити свої дослідження.

Наступний виняток дозволяє некомерційне цифрове використання творів та інших об'єктів, що охороняються авторським правом, з єдиною метою ілюстрації для навчання під відповідальність освітніх установ і має супроводжуватися вказівкою джерела, у тому числі імені автора (ст. 5). Допускається як очна, так і дистанційна діяльність, але остання може здійснюватися тільки через захищене електронне середовище, доступне тільки для викладацького складу, студентів та учнів закладів освіти. Оскільки, сфера дії ст. 5 обмежена онлайн-навчанням, тому на практиці вона, швидше за все, застосовуватиметься до цифрових форматів або трансляції аналогових матеріалів. Тобто, заклади освіти можуть з повною правовою визначеністю надавати навчальний контент дистанційним студентам та учням в інших державах–членах ЄС через своє безпечне електронне середовище, наприклад, інтранет університету або віртуальне навчальне середовище школи. Установи культурної спадщини можуть отримати зиск від цього винятку запропонувавши навчання у партнерстві зі школами, коледжами чи університетами.

Однією з цілей Директиви DSM є уніфікація правил, які застосовуються до цифрового збереження, щодо сприяння створення транскордонних мереж з об'єднання ресурсів та досвіду по всій Європі. Установи культурної спадщини держави–члена ЄС, які не мають технічних засобів або їм не вистачає експертних знань в оцифруванні, можуть «покладатися на третіх осіб, які діють від їхнього імені та під їхню відповідальність, включаючи тих, які базуються в інших державах–членах, для виготовлення копій» (п. 28 Преамбули). Таке доповнення забезпечує можливість спільного використання обладнання для оцифрування через транскордонні мережі оцифрування та дозволяє залучати зовнішніх підрядників під час створення резервних копій. Для збереження фондів установ культурної спадщини виняток згідно зі ст. 6 дозволяє робити резервні копії творів та інших об'єктів, що постійно перебувають у їх колекціях, та вільно конвертувати формати таких резервних копій. Немає жодних обмежень щодо формату або засобу відтворення. Тобто, установи культурної спадщини повинні мати можливість робити копії у будь-якому форматі, на будь-якому носії та з використанням будь-якої технології. Відповідно до цієї статті установам культурної спадщини дозволяється ігнорувати умови контракту, де прописано, що їм не дозволяється робити копії для збереження, крім того вони можуть виконувати національні процедури для усунення або обходу заходів технічного захисту.

З точки зору установ культурної спадщини найважливішою зміною, внесеною Директивою DSM, є положення, які дозволяють їм надавати твори з їхніх колекцій, що вийшли з комерційного обігу (out of commerce works – OOCW). Відповідно до ст. 8 Директиви DSM установи культурної спадщини повинні докласти розумних зусиль, щоб визначити, чи є робота доступною по звичайних каналах торгівлі чи ні. За цим положенням можуть використовуватися лише матеріали, які постійно перебувають в колекції установи, а виняток стосується лише прав та типів матеріалів, щодо яких жодна організація зі збору платежів відповідно до свого мандату не може видати ліцензії (ст. 8 (2). Цей так званий «резервний» виняток дозволяє установам культурної спадщини розміщувати такі твори на некомерційних веб–сайтах.

Якщо винятки, введені ст. 6, підходять для створення резервних копій об'єктів постійної колекції, але про надання до них доступу в Інтернеті мови не йде, то ст. 8 частково усуває цю прогалину. Вона зобов'язує всі держави–члени ЄС створити механізм, відповідно до якого установам культурної спадщини дозволяється відтворювати, розповсюджувати, оприлюднювати та робити доступними в Інтернеті всі твори зі своєї колекції, що вийшли з комерційного обігу, за умови укладання ліцензії із організацією колективного управління (ст. 8 (1)).

Щоб дати можливість правовласникам заборонити установам культурної спадщини надавати доступ до своїх творів, останні мають публікувати інформацію про твори, що вишли з комерційного обігу, на «загальнодоступному єдиному онлайн–порталі», яким керуватиме Відомство інтелектуальної власності Європейського Союзу (EUIPO), за шість місяців до того, як вони зроблять твори доступними в Інтернеті (ст. 10(1)). Після закінчення шестимісячного періоду твори можуть бути розміщені на вебсайтах установ культурної спадщини з некомерційною метою або відповідно до умов виданої ліцензії, погодженої між установою та організацією колективного управління, або як виняток. У будь–якому разі установа культурної спадщини не несе ризику бути притягнутою до відповідальності за порушення авторських прав.

Як бачимо, Директива DSM, прийнята в 2019 році, розглядає деякі питання авторського права, з якими стикається сектор культурної спадщини, а саме, освіта, збереження культурної спадщини, наукові дослідження та інновації. Розглянуті вище винятки, введені Директивою DSM, є істотним поліпшенням становища дослідницьких, освітніх установ та установ культурної спадщини і, відповідно, мільйонів їх користувачів.

Список використаних джерел:

1. Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0790&from=EN#d1e822-92-1https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019L0790&from=EN.

Горлинський В. В.
кандидат філософських наук, доцент, доцент кафедри, Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»
Горлинський Б. В.
кандидат технічних наук, начальник управління Адміністрації Держспецзв'язку,
Романенко В. П.
кандидат технічних наук, доцент, завідувач кафедри, Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

ІНСТИТУЦІЙНО-ПРАВОВІ АСПЕКТИ КОНСТИТУЮВАННЯ НАЦІОНАЛЬНОГО КІБЕРПРОСТОРУ УКРАЇНИ

Яскравим проявом цифрової трансформації сучасного суспільства є конституювання національного кіберпростору України. В умовах ескалації воєнної експансії російської федерації, що супроводжується перенесенням бойових дій у кіберпростір, питання його надійного захисту з боку держави, стає чинником її виживання.

Питання значущості захисту національного кіберпростору у забезпеченні національної безпеки обґрунтовано у працях А. Вакалюка, С. Гахова, Ю. Даника, І. Діордіци, Д. Дубова, О. Звездової, О. Корнейки, М. Ожевана, О. Потія, С. Рибки, Ю. Щиголя Ю. Яковенки та ін. Але, поряд з теоретичними здобутками, залишаються питання, що потребують поглиблення і конкретизації, розкриття яких, дозволить покращити

рівень захисту національного кіберпростору. Одним з таких актуальних питань, постає розробка і обґрунтування принципових теоретико-правових положень побудови національного кіберпростору, уточнення знань про його змістовний бік як умови контролювання і надійного захисту. Але підґрунтям визначення теоретичних засад конституювання кіберпростору є сукупність факторів, що зумовлюють його формування, інституалізацію, визначають межі національного кіберпростору в структурі глобального інформаційного простору. *Отже, метою роботи є визначення чинників і ознак конституювання національного кіберпростору як теоретичного підґрунтя з'ясування системних засад його структурного змісту, контрольованості та захисту*.

Не зважаючи на різноманітні варіації визначення кіберпростору, що пропонуються в дослідженнях, з погляду на сутність поняття, кіберпростір розглядається як цифрове комунікативне середовище. Поряд з цим, серед аспектів, що підкреслюють певний бік конституювання кіберпростору, дослідники відокремлюють техніко-технологічний, соціальний, правовий, комерційний, геополітичний тощо [1].

Змістовним визначенням, що застосовується як технічний стандарт ISO/IEC 27032 в країнах Європейському Союзу та НАТО, є констатація кіберпростору, як середовища існування, отриманого у результаті взаємодії людей, програмного забезпечення і послуг в Інтернет за допомогою технологічних пристроїв і мереж, підключених до них, яке не існує у будь-якій фізичній формі. В даному визначенні, поряд з техніко-технологічною, підкреслено соціальну і віртуальну ознаки кіберпростору. Але з погляду на сферу охоплення, це визначення можна розглядати як таке, що стосується, перш за все, глобального виміру кіберпростору.

Більш конкретним і прийнятим до застосування в правовому полі нашої держави як стандарту, вважається визначення, що міститься в Законі України «Про основні засади кібербезпеки України». «Кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних» [2]. Однак, поняття кіберпростору, наведене у Законі, не відокремлюється певними ознаками від глобального інформаційного та глобального кіберпростору. Постає питання відповідності контролюючих і безпекових функцій держави, щодо глобальних, суспільних, недержавних і національних інформаційних і телекомунікаційних систем. Такими ознаками для національного кіберпростору авторами пропонується вважати державну юрисдикцію і при-

належність засобів організації кіберпростору, державним інституціям, а також, підконтрольність недержавних і суспільних суб'єктів державним органам влади. Іншими, додатковими ознаками відокремлення національного кіберпростору від інформаційного можна вважати: способи захисту кіберпростору – криптографічний, технічний та засоби організації та контролю кіберпростору, а саме організаційний, техніко-технологічний і нормативний, організація яких ґрунтується на національній системі нормативно-правових актів; юридичну відповідальність суб'єктів за організацію технічного і криптографічного захисту інформації та інформаційно-комунікаційних систем; застосування національних інформаційно-комунікаційних систем і електронних засобів зв'язку, на які розповсюджується юрисдикція держави; державна значущість інформації, яка підлягає криптографічному і технічному захисту, систем електронних комунікацій, управління технологічними процесами, електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та технологічних системах національного, або державного призначення.

Наведені теоретичні положення дозволяють конкретизувати сутність і сформулювати визначення національного кіберпростору. *За своєю сутністю, національний кіберпростір являє собою цифрове комунікативне середовище на функціонування якого поширюється юрисдикція держави.* Якщо поглибити визначення за конкретними ознаками, то це – *середовище функціонування електронних комунікаційних мереж загального користування державної форми власності та/або інших форм власності, підконтрольних державним органам влади, із застосуванням ресурсів національної інформаційної інфраструктури з метою забезпечення інформаційних, комунікаційних і управлінських інтересів людини, суспільства і держави*.

Аналіз наукових праць дозволив визначити фактори, що впливають на процес конституювання національного кіберпростору а саме: системний характер процесів, що розгортаються в сучасному глобальному кіберпросторі, його конкретних секторах і на національному рівні; концептуальні зміни у підходах до розуміння змісту кібербезпеки і розширення функцій з її забезпечення; швидкий розвиток інформаційних технологій та їх перехід на квантову основу, що потребує врахування завдань з захисту кіберпростору постквантового періоду; загрози, що виникають із конвергенції інформаційних технологій з новітніми технологіями; необхідність реагування на кібератаки, спрямовані на державні установи і структури національної безпеки; спроби деструктивного інформаційно-психологічного впливу на особовий склад сектору безпе-

ки і оборони; курс України на євроатлантичну інтеграцію, узгодження національної системи стандартів кібербезпеки з стандартами НАТО і формування нової нормативної бази; сучасні глобальні зміни, що супроводжуються підвищенням ризикогенності професійної діяльності; вступ людства в період підвищеного соціального, екологічного і технологічного ризика; виклики ґендерної політики щодо досягнення ґендерної рівності у сфері безпеки і оборони України і міжнародні вимоги до гендерної політики держави, стосовно гендерного інтегрування [3]. Наведений перелік актуальних чинників не є остаточним адже зосереджує увагу на ключових моментах сьогодення, що передбачає можливість подальшого обговорення і доопрацювання цього питання в наукових колективах.

Отже, розробка і обґрунтування принципових теоретико-правових положень побудови національного кіберпростору, уточнення знань про його змістовний бік як умови контролювання і надійного захисту, постає одним з актуальних питань, що має теоретичну і практичну значущість для надійного захисту інформаційного простору українського суспільства, особливо в умовах воєнного стану. Подальша розробка науково-теоретичних, правових і організаційних питань захисту національного кіберпростору, є одним з важливих завдань наукової спільноти на шляху забезпечення національної безпеки України.

Список використаних джерел:

1. Гахов С. О. «Кіберпростір як основна категорія науки кібернетика», Сучасний захист інформації. Державний університет телекомунікацій, № 1. с. 53-57, 2017. [Електронний ресурс]. URL: http://journals.dut.edu.ua/index.php/dataprotect/article/view/1412. Дата звернення: Трав. 21, 2022.

2. Про основні засади кібербезпеки України. Закон від 05.10.2017. № 2163-VIII-ВР. База даних «Законодавство України» / ВР України. URL: http://zakon.rada. gov.ua/laws/show/2163-19 (дата оновлення: 17.09.2022).

3. Горлинський В. В., Горлинський Б. В. Аналіз ключових чинників формування системи компетентностей фахівців у галузі кібербезпеки // Information Technology and Security. July-December 2021. Vol. 9. Iss. 2. P. 219–231. URL: https://doi.org/10.20535/2411-1031.2021.9.2.249976.

Ісмайлов К. Ю.
кандидат юридичних наук, доцент,
начальник 5-го відділу 3-го управління
інформаційних технологій та
програмування Департаменту
кіберполіції Національної поліції
України

ДЕЯКІ ІНСТРУМЕНТИ ПОШУКУ ТА ФІКСАЦІЇ ОПЕРАТИВНОЇ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТ

Сьогодні поряд з традиційними методами та засобами отримання оперативної інформації співробітниками правоохоронних органів в карай ефективним стає пошук і аналіз інформації на підставі відкритих джерел (Open Source Intelligence – OSINT), а також її аналіз за допомогою моделі поліцейської діяльності, побудована навколо оцінки та управління ризиками (Intelligence-led policing – ILP) [1].

Актуалізується зазначене питання тим, що зараз спостерігається недостатня обізнаність співробітників правоохоронних органів у питаннях застосування онлайн-інструментів пошуку та фіксації інформації особливо правоохоронцями, містом роботи яких є невеликі міста та селища. Така ситуація стала наслідком практично відсутністю в навчальних планах та навчальних програмах дисциплін закладів вищої освіти із специфічними умовами навчання та повністю відсутність в цивільних закладах вищої освіти тем з новітніх засобів та прийомів пошуку, аналізу та фіксування поліцейськими оперативнозначущої інформації.

Слід відмітити, що здатність використовувати поліцейськими інформаційні технології потрібно не лише співробітникам спеціальним підрозділам таким як, кіберполіції, оперативно-технічного забезпечення або кримінального аналізу, а й усім без винятку суб'єктам оперативно-розшукової діяльності, слідчим та навіть дільничним інспекторам поліції (поліцейським офіцерам громади). Дореч, останнім зараз необхідно реагувати на такі явища як кібербулінг, секстінг, грумінг та інше, що не можливо забезпечити на якісному рівні без відповідних знань у сфері інформаційних технологій.

Отже, перед початком здійснення пошуку оперативно значущої інформації в мережі співробітник повинен захистити себе, тобто необхідно дотримуватися таких правил:

1. Використовувати перевірений VPN-сервіс
2. Інформація в аккаунтах соціальних мереж, месенджерах та інших профілях повинна бути легендована.

3. Пристрій, з якого проводиться моніторинг не повинен містити особисту інформацію співробітника.

Одним з сучасних та вкрай ефективним з таких засобів є застосування чат-ботів в месенджері Telegram [2, с. 258]. Чат-бот – це комп'ютерна програма, розроблена на основі нейромереж та технологій машинного навчання, яка веде розмову за допомогою слухових або текстових методівhttps://uk.wikipedia.org/wiki/%D0%A7%D0%B0%D1%82-%D0%B1%D0%BE%D1%82 – cite_note-1. Чат-боти використовуються в системах діалогу для різних практичних цілей, включаючи обслуговування клієнтів або отримання інформації. Деякі чат-боти використовують складні системи обробки людської мови, але більшість використовує простіші системи [3]. Використання чат-ботів відбувається та саме вони створюються для громадянського суспільства. Але за допомогою чат-ботів правоохоронці можуть отримувати інформацію про суб'єкта, його зв'язки або об'єкт посягання практично миттєво. Треба відмітити що при їх використанні не потрібно додатково встановлювати додатки або програми, витрачати оперативну пам'ять пристрою та отримувати додатковий дозвіл. З недоліків використання чат-ботів є неофіційний характер отриманої інформації, іноді платний контент та те, що бот необхідно знайти та перевірити його на спроможність виконувати необхідну функцію, що в реаліях роботи правоохоронця дуже складно зробити [3].

Щодо запровадження чат-ботів у месенджерах, то тут треба виділити саме месенджер Telegram, тому що саме в ньому найефективніше реалізована функція чат-ботів, яка виконує багато функцій в сфері бізнесу, ЗМІ, розваг, навчання, фінансовій сфері та інших.

Наведемо деякі чат-боти в Telegram, за допомогою яких кожен співробітник правоохоронних органів в декілька кликів зможе отримати потрібну йому інформацію:

@OpenDataUABot;
@UAFind_bot;
@info_baza_bot;
@Getcontact_bot;
@QuickOSINT_bot;
@userbox_boxbot;
@UniversalSearchRobot

Окрім наведених чат-ботів співробітникам правоохоронних органів можуть використовувати такий інструмент як Hunchly, який автоматично відстежує URL-адресу, часові позначки та хеш кожної сторінки, яку відвідує особа під час моніторингу мережі. Hunchly фіксує всі веб-сторінки у форматі MHTML, який містить заголовки з інформацією, що описує

саму сторінку, мітку часу, коли сам браузер захопив сторінку, а також містить увесь текст, стилі CSS і зображення, які містяться на сторінці. Що значно краще, ніж PDF або знімки екрана, оскільки всі посилання зберігаються, макет загалом точніший і всі метадані зберігаються, включаючи метадані в захоплених зображеннях. Варто зазначити, що запис MHTML на 100% обробляється Google Chrome. Hunchly просто дає вказівку Chrome виконати захоплення, а потім витягує результат для зберігання та аналізу.

Також правоохоронці можуть використовувати інформаційну панель мультимодальної аналітики сервісу InVID, яка представляє собою платформу для візуального пошуку та дослідження інформації для виявлення та відстеження нових історій на багатьох платформах соціальних медіа, включаючи учасників (осіб, організацій) і відносини між ними. Інформаційна панель використовує технологію кількох скоординованих переглядів для настільної версії та кросплатформену програму HTML5 для доступу до аналітичних функцій за допомогою смартфонів та інших мобільних пристроїв. Механізми синхронізації інформаційної панелі в реальному часі дозволяють відстежувати інформаційні потоки в контекстуальному інформаційному просторі InVID. Це включатиме можливість відображати зображення та відеозміст і використовувати мініатюри для представлення пов'язаних історій і кластерів змісту, таким чином інтегруючи візуальний вміст у існуючі робочі процеси веб-аналітики та спільного створення знань. Програма InVID підтримує:

– виявлення історій у соціальних мережах,
– ідентифікація вартого новин відео на основі історії,
– автоматичне вилучення та індексування метаданих,
– дослідження та візуалізація контенту,
– географічний розподіл нових історій,
– вбудоване відтворення на рівні відео та фрагментів,
– перевірка вибраних відео (за допомогою Додатка перевірки),
– автоматизована звітність PDF.

Начальне зображення показує поточний прототип інформаційної панелі, який включає графік візуалізації потоку історій для виявлення кластерів документів, відсортований список головних історій, включаючи мініатюру зображення та головну статтю, а також віджет відтворення відео.

Співробітникам також не варто нехтувати інформацією з загальнодоступних інформаційних чат-ботів. Що саме мається на увазі? Так, в чат-ботах представлені основні інформаційні канали всіх країн, у тому числі України, такі як «1+1», «Інтер», «ICTV», «НТН», «5 канал» вони

ж є в соціальних мережах, але офіційні сторінки доступ до висвітлювання своєї інформації в ЗМІ або в соціальних мережах національно-налаштованих або інших противоправних груп видаляються адміністрацією соціальних мереж, а технологія чат-ботів дозволяє безперешкодно цілодобово нав'язувати свою думку, висвітлювати дії або призивати до неправомірної поведінки інших людей. Тому сучасний працівник правоохоронних органів повинен використовувати інформації, яку поширюють в інформаційних чат-ботів.

Список використаних джерел:

1. Керована розвідкою поліцейська діяльність. URL: http://surl.li/dqgsn

2. Ісмайлов К. Ю., Сіфоров О. І., Лефтеров Л. В. Основні прийоми пошуку та аналізу інформації на підставі відкритих джерел. *Міжнародна та національна безпека: теоретичні та прикладні аспекти:* матер. III Міжнар. наук.-практ. конф., 15 бер. 2019 р. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2019. С. 258-261.

3. Ісмайлов К. Ю., Берназ П. В. Деякі особливості застосування правоохоронцями чат-ботів в месенджері Telegram для виявлення оперативнозначущої інформації. *Міжнародна науково-практична конференція Експлуатація як складова торгівлі людьми: виміри, тенденції та шляхи протидії*. ЛьДУВС. 2019 С. 43-46.

4. Чат-бот. URL: http://surl.li/dqgtc

Гангал А. В.
кандидат філософських наук,
доцент спеціальної кафедри
№ 4 Національного технічного
університету України «Київський
політехнічний інститут імені Ігоря
Сікорського»
Волошина Н. М.
кандидат філософських наук,
доцент, доцент спеціальної кафедри
№ 4 Національного технічного
університету України «Київський
політехнічний інститут імені Ігоря
Сікорського»

ДЕСТРУКТИВНА СОЦІАЛЬНА ІНЖЕНЕРІЯ – ЗАГРОЗА БЕЗПЕЦІ СУСПІЛЬСТВА У ТРЕТЬОМУ ТИСЯЧОЛІТТІ

Сьогодні кожна людина пов'язана з комп'ютером, зареєстрована хоча б в одній соціальній мережі. Соціальні мережі притягують людей, так як в сучасному світі всі люди спілкуються, обмінюються інформацією, знайомляться, частина людей придумує для себе віртуальний світ, в якому вони можуть бути безстрашними, популярними за допомогою чого відмовляються від реальності. Проблема, що пов'язана з безпекою персональних даних є сьогодні найбільш актуальною і водночас складною.

Сьогодні як ніколи, постає проблема свідомого використання інформаційних потоків або ресурсів з метою впливу на свідомість особистості, груп людей або всього суспільства, але на нашу думку, слід зазначити що суспільство, яке стало широко використовувати телекомунікації і глобальні комп'ютерні мережі, не може передбачити можливості використання цих технологій.

Словосполучення «соціальна інженерія» чітко відображає суть поняття, що являє собою сукупність підходів і методів, які орієнтовані на цілеспрямовану зміну сталих соціальних процесів, організаційних структур, що визначають людську поведінку, використовуючи психологічні особливості людей: зацікавленість, довіра, звички тощо і забезпечують контроль за ними.

Інформаційна війна на сучасному етапі розглядається, як процес маніпулювання інформацією або інформаційними потоками даних, яким довіряє об'єкт впливу (без відома об'єкту) з метою прийняття рішення проти інтересів держави, установи або особистості. Так само і соціальна

інженерія є особливим родом маніпулювання інформацією або інформаційними потоками, через виконання дій або розголошення конфіденційної інформації, зміни цілісності даних. Отже, інформаційна війна включає в себе деструктивні методи і способи соціальної інженерії.

Проведений аналіз наукових джерел засвідчує, що поняття деструктивної соціальної інженерії – відсутнє. На нашу думку, соціальна інженерія – це наука, об'єктом якої є вивчення людської природи, і як наслідок, подальшим конструюванням соціального середовища на мікро і макро рівні, з метою вирішення соціальних проблем і адаптації соціальних систем до умов, що змінюються. Але якщо соціальна інженерія застосовується для маніпулювання інформацією або інформаційними потоками за допомогою деструктивних методів і способів вона є деструктивною соціальною інженерією.

Слід зазначити, що сьогодні дослідники і фахівці, особливо у галузі кібербезпеки, використовують поняття соціальний інжиніринг, хоча поняття інжиніринг має інше змістовне значення (інжиніринг (англ. engineering) – набір способів та методів, які компанія, підприємство, фірма використовує для проектування власної діяльності). Соціальний інжиніринг – це метод несанкціонованого доступу до інформації або систем зберігання інформації без використання технічних засобів. Основна мета – це отримання доступу до захищених систем з метою крадіжки інформації, паролів, даних, тощо [3]. В ролі об'єкта атаки вибирається особистість, що і є деструктивною соціальною інженерією, але у вузькому розумінні.

Метою деструктивної соціальної інженерії є спонукання особистості (групи, соціуму) виконувати певні дії, які вони за звичайних умов ніколи б не вчинили. Наприклад, розголошувати власну конфіденційну інформацію, переходити на невідомі сайти, здійснювати дії за сумнівними інтернет-посиланнями, використовувати програмні продукти, що здійснюють крадіжку особистої інформації.

Деструктивну соціальну інженерію можна представляти як метод керування діями індивіда без використання технічних засобів, що ґрунтується на використанні слабкостей людського фактору. Вона побудована на використанні некомпетентності, непрофесіоналізму або недбалості персоналу для отримання доступу до інформації, доводячи, що найслабкішою ланкою системи залишається особистість. З іншого боку, деструктивну соціальну інженерію часто розглядають, як незаконний метод отримання інформації, тому сьогодні її активно використовують в Інтернеті для отримання закритої інформації або інформації, що має достатню цінність. Тоді методи несанкціонованого доступу до інформації

можна умовно поділити на категорії, коли використовують методи деструктивної соціальної інженерії та ті, що, в певній мірі, існують без них.

Основоположником деструктивної соціальної інженерії є Кевін Митник. Його можна вважати родоначальником даної науки, так як саме він популяризував її в першому десятилітті XXI століття. Сам Кевін раніше був хакером, який здійснював незаконне проникнення у найрізноманітніші бази даних. Він стверджував, що фактор людини є самим уразливим місцем системи будь-якого рівня складності та організації.

Якщо говорити про деструктивні методи соціальної інженерії, то можна сказати, що вони були вже відомі дуже давно. Проте донести всю важливість їх значення і особливості застосування зміг саме Кевін Митник.

Як зазначає Лаптєв С. О.: «Соціальна інженерія (як вже зазначалось деструктивна) – це такий нетехнічний тип стратегії кібератак, який базується на взаємодії між людьми та маніпуляціях таким чином, щоб людина порушила стандартні правила кібербезпеки. Для таких атак не потрібно бути хакером і знати купу технічної інформації, тому зловмисники активно використовують дану тактику. Легше обманом отримати бажане, ніж зламувати програмне забезпечення, наприклад, людина за власним бажанням передає вам свій пароль, аніж ви спробуєте зламати його. Проте соціальна інженерія вимагає від зловмисника гарної підготовки, що зазвичай має на меті збір інформації про жертву, аби точно знати, як саме можна отримати бажану інформацію» [2, С. 46].

Загальна система деструктивної соціальної інженерії базується на тому факті, що саме особистість чи соціальна група та їх свідомість (системний адміністратор, помічник керівника, співробітники, адресати пошти або телефонного виклику тощо), є найслабшою ланкою будь-якої інформаційної системи. Таким чином, всі дії злочинців, які використовують деструктивний інформаційно-психологічний вплив, спрямований безпосередньо на користувача, як на найвразливіше місце в системі інформаційної безпеки.

Основні напрями деструктивної соціальної інженерії: несанкціонований доступ до персональних даних; проникнення до інфраструктури організації для дестабілізації основних вузлів інформаційної системи та її мережі; загальна дестабілізація роботи організації, а також подальше цілковите руйнування її авторитету і її структури; фінансово-економічне шахрайство; вилучення конфіденційних відомостей; отримання конфіденційної інформації; отримання інформації про перспективні плани і проекти організації; отримання інформації про співробітників, їх персональні дані для їх подальшої дискредитації [1].

Сьогодні кібершахраї, хакери, злочинці використовують особливі методи деструктивної соціальної інженерії, які розраховані на різні аспекти психології особистості. На основі деструктивних впливів і їх чинників можна визначити основні області застосування методів деструктивної соціальної інженерії:

1) обман співробітника (системного адміністратора, любого співробітника, адресата пошти або телефонного виклику);

2) використання можливостей відкритих каналів телекомунікацій (телефон, електронна пошта, фальшиві інтернет-сайти, служба миттєвого обміну SMS, соціальні мережі);

3) проникнення на територію;

4) з'ясування і отримання телефонних номерів, паролів, відомостей;

5) розвідка (військова, політична, економічна, промислова, науково-технічна);

6) злочинна діяльність, зокрема:

шахрайство – заволодіння чужим майном або придбанням права на майно шляхом обману чи зловживання довірою;

рейдерство – протиправне заволодіння майном підприємства, установи, організації тощо;

викрадення – під викраденням розуміють корисливого злочинця чи групу злочинів, пов'язаних з протиправною оборуткою чужого майна на користь злочинця чи інших осіб (крадіжка, грабіж, розбій тощо);

вимагання – вимога передачі чужого майна чи права на майно або вчинення будь-яких дій майнового характеру з погрозою насильства над потерпілим чи його близькими родичами, обмеження прав, свобод або законних інтересів цих осіб, пошкодження чи знищення їхнього майна або майна, що перебуває в їхньому володінні чи під охороною, або розголошення відомостей, які потерпілий чи його близькі родичі бажають зберегти в таємниці;

7) дестабілізаційна діяльність;

8) правоохоронна діяльність (оперативне впровадження).

Висновок. Розвинені варіанти деструктивної соціальної інженерії – це витончена галузева політика професійних команд шахраїв і технічних фахівців різних профілів, які завдяки знанням, досвіду і навіть творчій уяві, можуть змінювати існуючі елементи і конструювати нові соціальні структури. Сьогодні, на перші місця серед загроз інформаційної безпеки, ставляться методи деструктивної соціальної інженерії, а ряд вчених стверджує, якщо деструктивна соціальна інженерія візьме на озброєння технології машинного навчання і штучного інтелекту, то людство отримає загрозу, яку можна порівняти з глобальним потеплінням і ядерною зброєю.

Тому питання протидії деструктивній соціальній інженерії – є мега актуальним, яке потребує не тільки правового регулювання, а й постійного вдосконалення методів її виявлення і контролю, не слід також забувати про посилення відповідальності за її застосування.

Список використаних джерел:

1. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. В. Б. Толубка. Київ: ДУТ, 2015. 288 с.

2. Лаптєв С. О. Удосконалений метод захисту персональних даних від атак за допомогою алгоритмів соціальної інженерії. *Кібербезпека: освіта, наука, техніка.* № 4 (16), 2022. С. 45–622.

3. Холод О. М. Формування концепцій соціального інжинірингу. DOI: 10.5281/zenodo.1069551.

Андрієнко О. В.
кандидат психологічних наук, адвокат, Заступник директора з правових питань ДП «ССМ» (Publicis Groupe Ukraine), Член Секретаріату Громадської ради при Комітеті Верховної Ради України з гуманітарної та інформаційної політики

РЕКЛАМА У ЦИФРОВОМУ ПРОСТОРІ: ПРИКЛАДНІ ПРОБЛЕМИ ГАРМОНІЗАЦІЇ ЗАКОНОДАВСТВА УКРАЇНИ З ВИМОГАМИ ЄВРОПЕЙСКОГО СОЮЗУ

Нещодавно KFC викликало хвилю обурення рекламною розсилкою, котра була автоматично згенерована у Німеччині і пропонувала курку до роковин початку Голокосту [1]. Тож законодавство членів Європейського Союзу (далі – ЄС) наразі не убезпечує від таких інцидентів. Водночас Україна як кандидат на вступ до ЄС зобов'язалася адаптувати до його вимог правове поле, зокрема, у сфері реклами.

Існує потенційно нескінченна кількість предметів правового регулювання, які залишаються поза межами теоретичних досліджень фундаментальних для права питань. Їх законодавче регулювання є синтетичним за своєю природою, оскільки не лише вбирає низку фундаментальних розробок з дотичних питань, але й пропонує новаторські рішення

як відповідь на розвиток економічної та соціальної реальності, котрі у подальшому стають підґрунтям для нових теоретичних пошуків, – і цикл замикається. При цьому йдеться про **конструювання оптимального законодавства** («поясу Золотоволоски»), тобто про достатній для стабілізації суспільних відносин ступінь регулювання: не занадто слабкий (щоб захистити ці відносини від хаосу та сваволі окремих їх суб'єктів) і водночас не надмірний (щоб регулювання не паралізувало розвиток таких відносин). Водночас, з огляду на **принцип голографічності розвитку будь-якої реальності**, спроба оптимально врегулювати конкретний предмет відображує у мініатюрі весь спектр проблем, притаманних для правової системи в цілому. Таким прикладом є правове регулювання реклами, яка нечасто стає предметом теоретичних досліджень, проте постійно присутня у нашому інформаційному полі, особливо у цифровому світі.

Будь-яке законодавче регулювання суспільних відносин можна розглядати як колапсування хвилі потенційно нескінченної кількості ймовірностей розвитку реального світу до обмеженого набору правових норм (дискретних часток мовою фізики). Ці норми, з одного боку, обмежують межі розгортання реальності суспільних відносин, а з іншого – стають підвалинами для її подальшого розвитку. Водночас, ці норми можуть бути кодифікованими (врегульовані окремим законом чи кодексом), а можуть бути хаотично імплементовані до широкого спектру нормативних актів. Очевидно, що **акт кодифікації – це результат визнання на рівні суб'єктів колективної свідомості важливості конкретного сегменту суспільних відносин**. Тому перше питання, яке підлягає розв'язанню: **чи має предмет нормативного регулювання достатній ступінь критичності**, щоб присвятити йому окремий нормативний акт. Те, що, на відміну від багатьох країн, відносини у сфері реклами з 1996 року врегульовані в Україні окремим законом, вказує на визнання цього питання критичним для нас, зокрема, з огляду на високу вразливість суспільства до публічних повідомлень (зависоку чутливість до впливу та низьку критичність мислення, чи контрсугестію у термінології Б. Ф. Поршнєва), брак медіаграмотності, а також недостатній наразі розвиток ефективних механізмів спів- та саморегулювання. **Цифрова трансформація суспільства експоненційно підсилює ці проблеми**, зокрема через **гіперперсоналізацію рекламного впливу**.

Будь-яке **правове регулювання розгортається у багатовимірному просторі**. Передусім, це **координати, які задаються різними суб'єктами нормотворчості**: 1) суверенною законодавчою владою держави; 2) міжнародними та наднаціональними суб'єктами різного масш-

табу, зокрема, на рівні ЄС; 3) ключовими гравцями на ринку, зокрема, платформами спільного доступу до інформації на кшталт Facebook, TikTok, Twitter, YouTube тощо, котрі мають власні правила, які, належачи за своєю природою до м'якого права (soft law), часто бувають набагато жорсткішими за акти національного законодавства (hard law).

Важливу роль відіграє **часова координата**. Перед Україною стоїть завдання гармонізувати своє законодавство, зокрема, із директивами ЄС. Проте на рівні ЄС наразі існує **чимало суперечливих норм, прийнятих у різний період й в умовах різної технологічної реальності**. Так, прийнята у 2010 році Директиві про аудіовізуальні медіа послуги [2] містить норми, які суперечать Європейській конвенції про транскордонне телебачення [3] із далекого 1998 року, превалюючи над ними (зокрема, щодо квоти реклами на телебаченні). Більше того, стрімкість технологічного розвитку та становлення Метавсесвіту робить актуальним питанням, з якою періодичністю законодавство повинно оновлюватися, особливо з огляду на об'єктивну інертність законотворчого процесу у будь-якій державі чи міждержавному об'єднанні. Сама необхідність регулярного перегляду не ставиться під сумнів. Проте чи повинен такий перегляд прив'язуватися до запланованих дат, чи орієнтуватися на швидкість накопичення інновацій та практики їх застосування, чи гармонійно поєднувати обидва підходи, – питання відкрите.

Доступність цифрового контенту з будь-якої точки світу спонукає **переосмислювати суто географічні координати застосовності національного законодавства**, адже реклама українського рекламодавця може бути показана українському споживачеві, який наразі вимушено перебуває у Польщі чи Великобританії і de jure набув статусу податкового резидента відповідної країни. Це спонукає до формування комплексних критеріїв за сукупністю ознак, як це відбулося з визначенням місця надання послуг для застосування так званого «податку на Гугл» [5]. Водночас, така гнучкість призводить до необхідності **компромісів із принципом правової визначеності й створює алюзію на принцип невизначеності** Гейзенберга, коли можливо або чітко врегулювати вкрай вузьке коло суспільних відносин, або ж встановити лише загальні принципи регулювання широкого кола, яке до того ж постійно розвивається і розширюється.

Крім того, з огляду на стрімкість технологічних та соціальних трансформацій **сама класифікація суспільних відносин у сфері цифрової реклами поки є живою і постійно мінливою сутністю**, яка, фактично, піддається довільному поділу на сфери за низкою критеріїв:

– ***за видом цифрових ресурсів***: в онлайн-медіа, на платформах спільного доступу до інформації (у тому числі, відео), на маркетплейсах, у пошукових системах, на власних веб-сторінках компаній, у месенджерах тощо;
– ***за суб'єктом її створення, модерації та розповсюдження***: створювана/ модерована/ розміщена рекламодавцем; рекламним агентством; користувачем (зокрема, користувацький контент, який може охоплювати широку аудиторію, як у випадку блогерів та інфлюенсерів); рекламодавцем, який підтримує і поширює користувацький контент;
– ***за використовуваною технологією розміщення***: 1) із застосуванням планування та розміщення «руками» людини або ж 2) із використанням різноманітних ідентифікаторів (таких як «реп'яшки» – cookies), профілювання, автоматизованих систем видачі повідомлень та відповідей на пошукові запити, спам-розсилок, ботів, Programmatic (програм автоматизованої закупівлі на рекламних біржах персоналізованих показів реклами) тощо. Застосування другої групи технологій ґрунтується на використанні великих даних, методах машинного та глибокого навчання, штучного інтелекту. Саме ця група несе найбільше ризиків, оскільки може призводити до гіперперсоналізованого впливу на окремого користувача, введення його в оману, а також порушувати вимоги щодо захисту персональних даних. Такий вплив за умови самоусуненням людини із процесу масової комунікації призводить до етично та потенційно правових негативних наслідків (як у прикладі з KFC чи реклами послуг з організації власного поховання, яка у відповідь на запит, як організувати святкування власного ювілею, переслідує людей, котрі перейшли певну вікову межу,).

Остання теза виводить на перший план **питання про межі застосування штучного інтелекту як для генерування та поширення реклами**, так і **для моніторингу порушень у рекламній сфері** (багато платформ вже використовують відповідні алгоритми для виявлення порушення прав інтелектуальної власності, а також реклами, яка містить мову ненависті, неетичний контент тощо), а також **власне для творення нормативного регулювання**.

Допомога технологій штучного інтелекту може виявитися надзвичайно помічної для творчого переосмислення низки питань, зокрема:

1) щодо **можливих заходів відповідальності**, вийшовши за межі її традиційних форм таких як визнання реклами недостовірною, приписи, заборони та фінансові санкції. Скажімо, моделювання впливу дій з боку

державних органів на репутацію недобросовісних рекламодавців може бути суттєвим важелем впливу, особливо для публічних компаній;

2) щодо **розробки нових засобів захисту прав фізичних осіб**, зокрема, про право на захист від спаму (що вже закріплено у статті 120 Закону «Про електронні комунікації») та право на забуття;

3) щодо **кола тих, до кого може бути застосована відповідальність**, розширюючи його за межі рекламодавця та рекламорозповсюджувача та включаючи платформи розміщення реклами, блогерів, а в деяких випадках – кінцевих користувачів (зокрема, при оцінці ступеню відповідальності споживання ними медіа-контенту) та по мірі появи – повністю віртуальних суб'єктів, які функціонують з використанням штучного інтелекту.

Тож ми повертаємося до зростаючої ролі спільного регулювання та саморегулювання, які неможливі без **постійного розвитку** (зокрема, через більдунг та підвищення медіаграмотності) **індивідуальних та колективних суб'єктів різного рівня та природи**: споживачів, рекламодавців, законотворців, правозастосовців, народу як цілого, європейської та світової спільноти як людських колективних агентів, а також штучного інтелекту як нашого спільного дітища.

Список використаних джерел:

1. Бінлі Алекс. KFC запропонувала «насолодитися хрумкою куркою» в пам'ять про погром євреїв. Скандал у Німеччині. – BBS News 10.11.2022. – https://www.bbc.com/ukrainian/news-63591944 – Дата доступу 22.11.2022.

2. Директива Європейського Парламенту та Ради Європи 2010/13/ЄС від 10.03.2010 про аудіовізуальні медіа послуги. – https://cedem.org.ua/library/dyrektyva-yevropejskogo-parlamentu-ta-rady-yees-2010-13/ – Дата доступу 22.11.2022.

3. Європейська конвенція про транскордонне телебачення від 05.05.1998. – https://zakon.rada.gov.ua/laws/show/994_444#Text.

4. Закон України № 1525-IX «Про внесення змін до Податкового кодексу України щодо скасування оподаткування доходів, отриманих нерезидентами у вигляді виплати за виробництво та/або розповсюдження реклами та удосконалення порядку оподаткування податком на додану вартість операцій з постачання нерезидентами електронних послуг фізичним особам». – https://zakon.rada.gov.ua/laws/show/1525-20#Text.

Брайчевський С. М.
кандидат фізико-математичних наук провідний науковий співробітник Державної наукової установи «Інститут інформації, безпеки і права» НАПрН України

РЕГІОНАЛЬНА СПЕЦИФІКА ПРАВОВОГО РЕГУЛЮВАННЯ В СФЕРІ СОЦІАЛЬНИХ КОМУНІКАЦІЙ В ОСОБЛИВИХ УМОВАХ

Невпинний прогрес в галузі інформаційних технологій неминуче призводить до кардинальних змін в багатьох сферах нашого життя, в тому числі в сфері соціальних комунікацій. Особливої актуальності вони набувають в контексті цифрової трансформації [1] українського суспільства. В першу чергу це означає суттєве зростання впливу використання цифрових технологій в усьому, що так чи інакше пов'язане з генерацією, обробкою та зберіганням інформації.

Очевидно, що виключно важливу роль в цьому плані відіграють генерація і споживання публічної інформації [2], оскільки без неї неможливо реалізувати повноцінні соціальні комунікації. За своєю природою публічна інформація завжди тісно пов'язана з особливостями місцевих суспільних процесів, адже в першу чергу саме вона відбиває їх свідоме сприйняття населенням. Підкреслимо, що соціальні комунікації набувають характерних особливостей в умовах проведення реформи децентралізації [3]. Головна причина цього полягає в несинхронізованій діяльності багатьох незалежних агентів інформаційних процесів. В першу чергу йдеться про організації та фізичних осіб, які приймають участь в формуванні публічної інформації.

Важливість (і складність) проблеми значно зростає в особливих умовах, під якими будемо розуміти війну, природні катаклізми тощо. У випадку виникнення таких умов суттєво зростає регіональна специфіка, викликана впливом зовнішніх чинників, різних в різних місцях. Тоді ситуації (а отже і особливості регулювання суспільних процесів) в різних регіонах можуть кардинально відрізнятись між собою, а отже може зростати рівень фактичної автономії як в системі прийняття рішень на різних рівнях, так і в інформаційних процесах, пов'язаних з цими рішеннями [4]. Ця обставина, в свою чергу, породжує регіональну специфіку правового регулювання. В тому числі необхідно враховувати роботу тимчасових органів (військові адміністрації, комісії з питань надзвичайних ситуацій тощо), що мають додаткові повноваження щодо правового

регулювання на місцевому рівні. Яскравим прикладом можуть служити відмінності між прифронтовою зоною та глибоким тилом. І, звичайно, ця специфіка позначається на комунікативних процесах, оскільки вони завжди прив'язані до місцевої ситуації.

В результаті поєднання зазначених чинників процес соціальних комунікацій втрачає цілісність, оскільки базові комунікативні механізми неминуче зазнають фрагментації на регіональній основі. Отже, виникає потреба компенсації цього негативного ефекту. Вона залежить в тому числі і від ефективності правового регулювання в даній сфері. А це, в свою чергу, зумовлює актуальність вивчення специфіки правового регулювання соціальних комунікацій на регіональному рівні в особливих умовах.

З сучасної точки зору соціальні комунікації являють собою складне явище, що містить ряд компонентів різної природи [5-6]. Але для нас важливо те, що в їхній основі завжди лежить процес обміну інформацією в різноманітних формах, в тому числі електронних. І тією мірою, як в наше життя впроваджуються нові інформаційні технології, вони починають грати все більшу роль в комунікативних процесах.

А тому і правове регулювання в сфері соціальних комунікацій все більше передбачає активне застосування цифрових технологій. І очевидно, що воно може бути успішним лише за умови наявності ефективної автоматизованої системи накопичення, опрацювання і поширення правової інформації. Нагадаємо, що за визначенням правова інформація – це «будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо» [7].

Правова інформація як така має досить складну структуру. Ця складність, в першу чергу, зумовлюється характером її джерел [7]. Отже, машинна обробка таких складних за своєю структурою масивів даних, яка забезпечує правильне інтерпретування [8], є непростою та відповідальною справою, що породжує низку проблем концептуального і технічного характеру.

З іншого боку, соціальні комунікації є вкрай динамічними, і тому відповідне правове регулювання вимагає постійної адаптації до поточних змін актуальності тем спілкування. Важливо, що ці зміни мають більший вплив на суспільні процеси на регіональному рівні, ніж на центральному. В умовах децентралізації [3] зазначений чинник значно посилюється за рахунок відсутності достатньої синхронізації в процесах генерації правової інформації на різних рівнях адміністративно-територіального устрою України, що виникає в першу чергу внаслідок перерозподілу по-

вноважень між центром і регіонами, а також між різними органами місцевого самоврядування [10, 11].

В особливих умовах ситуація стає значно складнішою через те, що в різних регіонах (внаслідок породжених різною обстановкою характерних особливостей соціальних комунікацій), відповідно виникає необхідність окремого правового регулювання шляхом генерації на місцевому рівні правових норм, що відбивають наявну регіональну специфіку. Тому має бути забезпечена ефективна система доступу до всього комплексу правових норм, що діють в даному місці. При чому (в умовах постійного зростання ролі інформаційних технологій) цей доступ належним чином повинен допускати використання сучасних автоматизованих засобів накопичення, зберігання та обробки інформації.

Ми вже обговорювали загальні питання структури правової інформації в умовах децентралізації [12]. Було показано, що важливим чинником є уніфікація структури правової інформації [13-14]. Метою в даному випадку є досягнення можливості отримувати і обробляти правову інформацію в різних регіонах і на різних рівнях стандартними інструментальними засобами. Також розглядалися [4] деякі загальні методи вдосконалення механізмів надання нормативно-правової інформації в особливих умовах на регіональному рівні. Ключову роль, на нашу думку, має відігравати створення інтегрованих масивів даних, які природним чином поєднають регіональну генерацію правових норм з універсальним доступом до них на загальнодержавному рівні. Врахування цих питань може виявитися корисним при створенні автоматизованих систем, призначених для інформаційного супроводу процесів правового регулювання в сфері соціальних комунікацій.

Оскільки соціальні комунікації є надзвичайно складним явищем, розробка таких систем становить окрему нетривіальну задачу, вирішувати яку повинні професійні колективи кваліфікованих фахівців в різних галузях сучасної науки.

Список використаних джерел:

1. Цифрова трансформація. URL: https://www.kmu.gov.ua/diyalnist/mizhnarodna-dopomoga/coordination/cifrova-transformaciya (дата звернення 10.11.2022)

2. Закон України «Про доступ до публічної інформації» (Відомості Верховної Ради України (ВВР), 2011, № 32, ст. 314) URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення 10.11.2022)

3. Офіційний український державний сайт «Децентралізація влади». URL: https://decentralization.gov.ua/ (дата звернення 10.11.2022)

4. Брайчевський С. М. Проблема надання нормативно-правової інформації в особливих умовах. «Інформація і право». 2022. № 2 (41). С. 28-36. URL: http://ippi.org.ua/braichevskii-sm-problema-nadannya-normativno-pravovoi-informatsii-v-osoblivikh-umovakh-s-28-36 (дата звернення 10.11.2022)

5. Різун В. В. Начерки до методології досліджень соціальних комунікацій. Психолінгвістика. 2012. Вип. 10. С. 305-314. URL: http://nbuv.gov.ua/UJRN/psling_2012_10_44 (дата звернення 14.11.2022)

6. Холод О. М. Соціальні комунікації: соціо- і психолінгвістичний аналіз. 2011. Львів: ПАІС/ 2011. 288 с. URL: http://194.44.152.155/elib/local/sk784391.pdf (дата звернення 14.11.2022)

7. Закон України «Про інформацію». (https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2938-17#Text) (дата звернення 16.11.2022)

8. ISO/IEC 2382:2015, Information technology. Vocabulary. *Part 1: Terms and definitions* https://www.iso.org/standard/63598.html (дата звернення 16.11.2022)

9. Офіційний український державний сайт «Децентралізація влади». https://decentralization.gov.ua/ (дата звернення 16.11.2022)

10. Концепція реформування місцевого самоврядування та територіальної організації влади в Україні .https://zakon.rada.gov.ua/laws/show/333-2014-%D1%80#Text (дата звернення 16.11.2022)

11. Нестерович В. Ф. Децентралізація як конституційний принцип здійснення публічної влади на регіональному та місцевому рівнях. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2019. № 3. С. 47–54. https://visnik.dduvs.in.ua/wp-content/uploads/2019/12/3-19-ua/10.pdf (дата звернення 16.11.2022)

12. Брайчевський С. М. Уніфікація структури правової інформації в умовах децентралізації. Матеріали Першої «Парламентський контроль в умовах децентралізації державної влади та цифрової трансформації в Україні: стан та проблеми» 30 березня 2021 року. Київ. С. 40-43. URL: http://ippi.org.ua/sites/default/files/zbirnik_tez_konferenciyi__30.03.2021_0.pdf (дата звернення 21.11.2022)

13. Опришко В. Ф. Міжнародне економічне право і процес. К., *Парламентське вид-во*, 2014. 518 с.

14. Уніфікація в праві. *Юридична енциклопедія* https://leksika.com.ua/15731028/legal/unifikatsiya_v_pravi (дата звернення 21.11.2022)

Андрощук Г. О.
кандидат економічних наук, доцент,
головний науковий співробітник
Науково-дослідного інституту
інтелектуальної власності НАПрН
України

ЦИФРОВЕ ПІРАТСТВО ТА КОНТРАФАКЦІЯ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ: АНАЛІЗ СТАНУ, ТЕНДЕНЦІЇ, МЕХАНІЗМИ ПРОТИДІЇ

Компанія International Data Corporation (IDC) оприлюднила прогноз щодо глобальної IT-галузі: йдеться про витрати на цифрову трансформацію організацій, продуктів та бізнес-практик. У ситуації, що склалася, і в умовах пандемії, що продовжується, багато корпорацій та організацій змушені переглянути модель роботи: перенесли навантаження у хмару та оптимізували витрати. За оцінками у 2021 р. витрати у сфері цифрової трансформації становили приблизно $1,36 трлн. У поточному році очікується зростання на 17,6%, а глобальні витрати піднімуться до $1,8 трлн. у вигляді глобальних витрат на цифрову трансформацію підприємств. І понад 60% світового ВВП буде оцифровано із зростанням у кожній галузі, зумовленому цифровими пропозиціями, операціями та відносинами [1]. Нині більше половини (3,9 млрд) світового населення підключено до Інтернету, який є найбільш відкритим глобальним інформаційним суспільством. Нові технології є каталізаторами змін, пропонуючи підприємствам надзвичайно широкі можливості. Технології штучного інтелекту (ШІ), розширена реальність і квантові обчислення стають наступним набором нових технологій, які викличуть стрибкоподібні зміни, що дозволять підприємствам переформатувати цілі галузі. Визначальною в цифровій економіці стає роль інтелектуальної власності (ІВ). Роль ІВ та цифрової інфраструктури обороту прав ІВ стає ключовим чинником, що визначатиме зростання національних економік і, як результат – вплив країни в світі. Передумови для цього створені розвитком глобальних цифрових мереж, понад 70% трафіку яких становить рух об'єктів ІВ. Про зростання ролі сфери ІВ в глобальному вимірі свідчить останній Звіт Всесвітньої організації інтелектуальної власності – World Intellectual Property Report 2022 (WIPR). За 35 років потроїлася кількість інновацій, пов'язаних із комп'ютерною технікою та суміжними галузями (ІКТ), на цей сектор припадає майже чверть всіх патентів, а щорічні темпи зростання становили 8%. Нова революція у сфері інновацій пов'язана із цифровізацією, яка призводить до трансформації ці-

лих галузей. Кількість цифрових інновацій зросла в чотири рази. На цей сектор припадає 12% усіх патентних заявок, а щорічні темпи зростання патентної активності становлять 13% [2].

В Угоді про асоціацію між Україною та ЄС у ч. 1 ст. 250 розрізняються терміни «контрафактні товари» і «піратські товари». Контрафактними товарами є: і) товари, зокрема, упаковка, що містить без дозволу торговельну марку, ідентичну торговельній марці, зареєстрованій належним чином стосовно такої самої групи товарів, які за суттєвими ознаками не можуть бути відрізнені від товарів із зазначеною торговельною маркою та таким чином порушують права власника торговельної марки; іі) будь-який символ торговельної марки (логотип, маркування, наклейка, брошура, інструкція з користування або гарантійний документ). Навіть при окремому представленні, за таких самих умов, як і товари, зазначені в підпункті (і); ііі) пакувальні матеріали, що містять торговельні марки контрафактних товарів, представлені окремо, за таких самих умов, як і товари, зазначені в підпункті (і). До піратських відносяться товари, які є копіями або містять копії, вироблені без згоди власника або особи, належним чином уповноваженої представляти інтереси власника в країні виробництва в питаннях авторського права та суміжних прав або права на промисловий зразок, незалежно від того, чи зареєстровані вони в національному законодавстві, чи ні [3].

Нещодавно Відомство інтелектуальної власності ЄС (EUIPO) оприлюднило дослідження порушень авторського права (музика, фільми та телебачення) в Інтернеті в ЄС: тенденції та причини [4]. Дослідження охоплює період з січня 2017 по грудень 2020 р. для телевізійних програм, музики та фільмів у 27 країнах-членах ЄС та Великобританії. В рамках дослідження, зокрема, виявлено, що рівень цифрового піратства, виміряний як середня кількість запитів від інтернет-користувачів до вебсайтів-порушників за місяць, зменшився на 34% у 2020 р. порівняно з попереднім роком. Наведемо ключові висновки дослідження EUIPO: У період з 2017 по 2020 рік загальний доступ до піратського контенту скоротився вдвічі. Найпомітніше скорочення в музиці – 81%, далі йдуть кіно (68%) та телебачення (41%). В середньому інтернет-користувач в ЄС отримував доступ до піратського контенту 5,9 разів на місяць у 2020 році. Пандемія COVID-19 мала лише тимчасовий вплив навесні 2020 р., коли піратство фільмів зросло. Влітку 2020 р. тенденція до зниження відновилася. Потокове передавання було найпоширенішим методом доступу, на нього припадало близько 80% усього доступу. Відмінності між державами-членами ЄС досліджувалися за допомогою економетричного аналізу. Такі фактори як нерівність доходів збільшують піратство, а до-

ступ до легальних пропозицій та обізнаність про такі пропозиції, як правило, зменшують піратство. Основні дані для цього дослідження отримані в результаті відстеження трафіку на піратських веб-сайтах, отриманих від MUSO, лондонської компанії, яка надає статистику піратської діяльності. Для порівняння трафіку та його аналізу використовувалися додаткові дані: економічні змінні, такі як дохід душу населення; частка молоді у населенні; легальна цифрова пропозиція: інтернет та мовні платформи; сприйняття, поінформованості та поведінки щодо піратства. Ці дані були отримані від Євростату, Європейської аудіовізуальної обсерваторії та, для даних про сприйняття та відношення споживачів, від дослідження сприйняття IB EUIPO. Проте час вносить свої корективи. Аналіз нових досліджень показує, що рівень піратства збільшується. Нові дані, нещодавно надані трекінговою компанією MUSO, показують, що кількість відвідувань піратських сайтів збільшилася майже на 30% порівняно з минулим роком [5]. Видавнича категорія зростає особливо сильно. США, як і раніше, є притулком для більшості піратів в абсолютному вираженні. Попри зростаючу доступність легальних варіантів, онлайн-піратство залишається неприборканим. Щодня піратськими сайтами та сервісами користуються мільйони людей по всьому світу. Нові дані, опубліковані MUSO, показують, що піратські сайти залишаються дуже актуальними: люди не мають проблем з їх пошуком, трафік на ці сайти стрімко зростає. Так, у першому кварталі 2022 р. кількість відвідувань піратських сайтів збільшилася більш ніж на 29% порівняно з попереднім роком, що відповідає 52,5 млрд. відвідувань. Майже половина цього трафіку (48%) припадає на контент, пов'язаний із телебаченням, видавнича справа посідає друге місце (27%), за нею йдуть фільми (12%), музика (7%) та програмне забезпечення (6%). Зростання трафіку помітне для всіх типів піратства, але виділяється категорія публікацій. Порівняно з першим кварталом 2021 р. кількість відвідувань цієї категорії різко зросла. Програмне піратство відстає, але ця категорія продовжує зростати. **Америка попереду.** США – це країна, яка відправляє на піратські сайти найбільше відвідувачів. З понад 5,7 млрд «відвідувань» за перші три місяці року на США припадає понад 10% всього піратського трафіку. Зі збільшенням на 39% порівняно з минулим роком зростання піратської аудиторії перевищує середній світовий показник. Далі йдуть Росія та Індія з трохи більш ніж 3 млрд відвідувань піратських сайтів, за ними йдуть Китай та Франція з 1,8 та 1,7 млрд відвідувань відповідно. Найбільшим медіасектором, на який припадало 46.6% усього трафіку, що йде на піратські web-сайти, є телевізійний контент. Протягом перших восьми місяців 2022 р. було визначено деякі помітні тенденції в даних

MUSO про піратство в розрізі різних галузей. Так із січня по серпень 2022 р. експерти MUSO зафіксували 141.7 млрд відвідувань піратських сайтів для всіх галузей, що на 21.9% більше, ніж за аналогічний період 2021 року. Аналіз за секторами медіа індустрії показує, що найбільшим сектором був телевізійний, який охоплює телебачення, аніме, прямі трансляції спортивних програм та інші прямі трансляції. Серед цих медіасекторів телевізійний контент склав 46.6% всього трафіку на піратські web-сайти. Порівнюючи дані вимірювань по кожному із секторів, що мали місце з січня по серпень 2022 р. із даними за аналогічний період 2021 р., MUSO зазначає, що піратство зросло в усіх галузевих секторах. Причому піратський кінотрафік показує найбільше зростання на 49.1%. Музичний сектор демонструє найнижчі показники зростання – 3.87%. Аналіз ситуації в розрізі методів доставлення неліцензійного контенту свідчить, що 53.9 % трафіку припадає на неліцензовані потокові сайти порівняно із 46.1% трафіку на сайти завантаження (включаючи торенти та кіберблокери). Щоб отримати точнішу картину тенденцій в розрізі способів доставляння, необхідно проаналізувати кожен медіасектор. На потокові трансляції припадає 95.1% трафіку телевізійного контенту, тоді як на завантаження припадає 99% трафіку публікацій і 100% трафіку піратського програмного забезпечення. Аналіз рівня піратства в географічному розрізі свідчить, що в період від січня по серпень 2022 р. на США припадало 10.9% піратства, що на 87.3% вище, ніж в Росії, яка посідає друге місце. Найвищі серед країн Європи показники піратства має Франція (5 місце), за нею йде Велика Британія (7 місце). Україна у глобальному рейтингу займає 14 місце [6].

Проблема цифрового піратства досить гостро стоїть в Україні. Згідно з результатами дослідження практики споживання цифрового контенту в Інтернеті, проведеного на запит Асоціації компанією GfK в червні 2020 р., більшість українців використовують одночасно і легальні, і піратські ресурси – 75% для фільмів та серіалів та 80% для музики. Водночас, близько двох третин опитаних користувачів, які завантажував файли за останні 6 місяці, використовували для цього нелегальні ресурси [7]. За даними Центру досліджень соціальних комунікацій НБУ рівень комп'ютерного піратства в Україні становить 86%, в той час як середній рівень у світі — всього 42%. А у дослідженні Суспільного про розвиток піратства в Україні зазначається, що сумарна аудиторія двох найбільших сайтів, де можна безкоштовно завантажити mp3-файл з майже будь-якою піснею світу, становить близько 21 млн користувачів з України. І це тільки (за січень 2020 р.) [8]. В Офісі ефективного регулювання BRDO розробили законопроєкт, покликаний запобігти цифровому піратству і за-

хистити контент від шахрайського доступу до нього шляхом використання спеціальних пристроїв [9]. Законопроєкт визначає механізми захисту від несанкціонованого доступу до цифрових послуг телебачення та радіомовлення, які користувачі отримують за окрему плату. Він запобігає цифровому піратству і наближає українське законодавство до європейського, як того вимагає Угода про асоціацію України з ЄС. Мінекономіки доопрацювало законопроєкт, розділивши його на два проєкти закону – № 5870 і № 5871, які були зареєстровані у Верховній Раді 27 серпня 2021 року. «В Україні сьогодні дуже легко не платити за цифровий контент, оскільки законодавство не передбачає заборону виробництва, продажу і використання незаконних пристроїв умовного доступу», – відзначили в BRDO. В Європі послуги доступу до цифрового контенту захищаються окремою Директивою 98/84 / ЄС ще з 1998 року. Через піратство тільки українська книжкова галузь щорічно втрачає $30 млн.

Організація економічного співробітництва та розвитку (ОЕСР) у дослідженні «Економічні наслідки контрафакції та піратства» відзначила, що саме Інтернет надав порушникам прав ІВ новий та потужний засіб для продажу своєї продукції, припускаючи, що значна частка контрафактних товарів розповсюджується через Інтернет [10]. Стрімкий розвиток Всесвітньої мережі Інтернет загострив проблему контрафакції, створивши для порушників права ІВ додаткові та спрощені канали у кіберпросторі для просування, реклами, пропозиції та продажу контрафактної продукції споживачам. Інтернет-піратство та крадіжка авторської власності у сучасному світі має широке поширення. Особливо це стосується країн, де рівень інтернет-культури не надто високий. Європейська комісія опублікувала звіт із захисту прав інтелектуальної власності у світі. Найпроблемнішою країною виявився Китай — йому надали пріоритет 1. Україна потрапила до списку країн з пріоритетом 2, до якого також входять Індія, Туреччина, Індонезія та Росія. Пріоритет 2 означає «серйозні системні проблеми в галузі охорони та захисту прав ІВ, заподіяння значної шкоди бізнесу ЄС, порівняно з попереднім роком, прогрес відсутній або мінімальний». Україна залишалась однією з чотирьох основних транзитних країн для потрапляння контрафакту на ринок ЄС. [11]. Онлайн-піратство залишається серйозною проблемою для нашої країни. На думку Єврокомісії, нинішнє законодавство у сфері захисту ІВ в Україні є дуже слабким. Через це в нашій країні постійно з'являються сайти з викраденим контентом.

У березні 2022 р. Обсерваторія ЄС опублікувала Звіт про оцінку загрози злочинів у сфері інтелектуальної власності за 2022 р. (Intellectual Property Crime Threat Assessment 2022 Report), в якому викладені резуль-

тати спільного дослідження Відомства з інтелектуальної власності Європейського Союзу (EUIPO) та Європолу [12]. https://www.europol.europa.eu/cms/sites/default/files/documents/Report. Intellectual property crime threat assessment 2022_2.pdf Цей звіт показує, що виробництво і продаж контрафакту є дуже прибутковою діяльністю для злочинців і залучених злочинних мереж. Отримані результати наголошують на важливості рішення про те, щоб знову зробити злочини проти ІВ правоохоронним пріоритетом у боротьбі з організованою злочинністю, і ще більше посилити заклики до скоординованих дій усіх країн світу. У звіті підкреслюється, що ця остання березнева оцінка, проведена спільно EUIPO та Європолом, підтверджує, що злочини проти ІВ становлять як загрозу здоров'ю і безпеці споживачів та завдають шкоди економіці. Зокрема, імпорт контрафактних та піратських товарів у 2019 р. становив 119 мільярдів євро, що складає 5,8 % усіх товарів, що надходять до ЄС. Хоча більшість контрафактних товарів, що поширюються в ЄС, виробляються за межами ЄС, є ознаки, що виробництво підроблених і неякісних товарів все частіше відбувається в межах членів держави. Часте вилучення фальсифікованих пакувальних матеріалів та напівфабрикатів на кордоні однозначно вказують на наявність виробничих потужностей в ЄС – одні для часткового збирання та інші, що виконують повний виробничий цикл. Розповсюдження підроблених та неякісних товарів онлайн та офлайн було ключовою злочинною діяльністю під час пандемії. Криза охорони здоров'я, викликана COVID-19, підкреслила той факт, що злочинні організації не визнають кордонів і використовують найменшу слабкість або недолік в координації спільних протизлочинних зусиль для зміцнення своїх позицій. «Оцінка загрози з боку особливо небезпечних форм організованої злочинності 2021» (Serious and Organised Crime Threat Assessment, SOCTA) чітко визначає злочини проти ІВ, як одну із загроз серйозної та організованої злочинності, з якою стикається ЄС. У звіті зазначається, що щоб ефективно боротися з цією злочинною загрозою, уряди повинні розуміти природу та масштаб цієї загрози. Ця доповідь допомагає тим, хто бере участь у боротьбі зі злочинами проти ІВ, оцінити цю злочинну діяльність. Партнерство між Європолом та EUIPO продовжує та посилює оперативну відповідь держав-членів на злочини проти ІВ, особливо у складні часи пандемії COVID-19.

Стан в Україні. Український альянс по боротьбі з підробками та піратством (UAACP) провів анкетування-опитування громадської думки. Отримані результати свідчать, що в Україні доросле населення та школярі у 80% випадків не замислюються над питанням чи оригінальний товар вони купують, лише 15% дорослих та молоді впевнені, що ніколи не ку-

пували підробок. Аудиторія студентів більш схильна до покупки контрафактного товару, молодь не цікавить якість товару, яка їх, здебільшого, задовольняє, а приваблює дешевизна підробок. Студентська спільнота у 50% випадках купувала підроблені товари свідомо, а 25% студентів будуть і надалі купувати підробки, тому що нічого поганого у цьому не вбачають, а грошей завжди не вистачає [13]. https://www.europol.europa.eu/cms/sites/default/files/documents/Report. Intellectual property crime threat assessment 2022_2.pdfЯк бачимо українська молодь більш схильна до придбання підробок і така ситуація загрожує безпеці України. В умовах військового стану усім українцям необхідно більш уважно підходити до питання придбання підробок, з огляду на економічне підґрунтя цього негативного явища. Варто нагадати, що контрафакт — це не тільки питання моралі і порушення прав ІВ, це злочин, який генерує швидкі неконтрольовані державою грошові потоки, які з великою вірогідністю можуть бути спрямовані на потреби ворога для фінансування військових злочинів проти нашої держави!

Висновки. З 23 червня 2022 р. Україні надано статус кандидата у члени Євросоюзу. Крім відкриття перспектив це накладає численні обов'язки з удосконалення системи захисту прав ІВ. Потребує значно глибших структурних змін, ніж цього вимагала Угода про асоціацію України з ЄС, нормативне регулювання цієї сфери. Також потрібно створити регламенти й політики митного контролю, гармонізовані з ЄС. Через різке зростання онлайн-продажів спостерігається помітне зростання продажів контрафактної продукції, незважаючи на різні рішення, доступні для боротьби з нею. Загалом щороку на різних онлайн-платформах продаватиметься контрафактна продукція на суму понад 1,7 трлн доларів – і ця оцінка Міжнародної коаліції по боротьбі з контрафакцією була складена ще у 2015 році. Продаж контрафакту призводить до втрати мільйонів робочих місць та втраченого прибутку і на сьогодні є найбільшим у світі злочинним підприємством. Очікується, що до 2024 р. лише у США обсяг продажу контрафакту в електронній торгівлі зросте до 6 трлн доларів [14].https://www.europol.europa.eu/cms/sites/default/files/documents/Report. Intellectual property crime threat assessment 2022_2.pdf Захист прав ІВ в умовах воєнного стану є вкрай важливим, оскільки це міжнародні зобов'язання України щодо вступу в ЄС та життєва необхідність захисту економічних інтересів України. Держава, яка не захищає права ІВ, фактично підтримує тіньовий бізнес (чим завдає збитків чесному бізнесу, який платить податки), фінансує організовану злочинність та воєнних злочинців. Забезпечити ефективний захист від контрафакту можна, лише

об'єднавши зусилля митних, правоохоронних, експертних, судових органів, правовласників, усіх зацікавлених осіб. Адже обмін інформацією між ними та координація спільних дій мають важливе значення для запобігання, виявлення, контролю, розслідування та судового переслідування правопорушників.

Список використаних джерел:

1. Затраты на цифровую трансформацию в 2022 году достигнут $1,8 трлн в мировом масштабе. URL: https://bin.ua/news/interesting/it/277540-zatraty-na-cifrovuyu-transformaciyu-v-2022-godu.html

2. World Intellectual Property Report 2022 The Direction of Innovation. URL: https://www.wipo.int/wipr/en/2022/

3. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державамичленами, з іншої сторони. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text

4. ONLINE COPYRIGHT INFRINGEMENT IN THE EUROPEAN UNION MUSIC, FILMS AND TV (2017-2020), TRENDS AND DRIVERS. URL: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/online-copyright-infringement-in-eu/2021_online_copyright_infringement_in_eu_en.pdf

5. Pirate Site Traffic Surges With Help From Manga Boom. URL: https://torrentfreak.com/pirate-site-traffic-surges-with-help-from-manga-boom-220503/

6. Борис Скуратівський Дослідження: Сполучені Штати та Росія – лідери по медіапіратсву. Україна – на 14 місці. URL https://mediasat.info/uk/2022/10/13/doslidzhennya-spolucheni-shtati-ta-rosiya-lideri-po-telepiratsvu-ukraina-na-14-misci/

7. Бізнес закликає українців користуватися легальним контентом в Інтернеті URL https://eba.com.ua/biznes-zaklykaye-ukrayintsiv-korystuvatysya-legalnym-kontentom-v-interneti/

8. Чуловська О. Вкрасти, щоб прочитати: чому в Україні процвітає книжкове піратство і як з ним боротися? URL: https://www.readmodo.com/piratstvo/

9. У BRDO хочуть зайнятися боротьбою з піратством в Україні. URL: https://biz.nv.ua/ukr/tech/borotba-z-piratstvom-u-brdo-pidgotuvali-zakonoproekt-novini-ukrajini-50181964.html

10. The Economic Impact of Counterfeiting and Piracy – OECD, 2008. URL: https://www.oecd.org/sti/ind/theeconomicimpactofcounterfeitingandpiracy.htm

11. Олексій Турчак. В Украине очень высокий уровень интернет-пиратства: отчет Еврокомиссии URL:. https://informator.ua/ru/v-ukraine-ochen-vysokij-uroven-internet-piratstva-otchet-evrokomissii

12. Intellectual Property Crime Threat Assessment 2022 Report. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Report.%20Intellectual%20property%20crime%20threat%20assessment%202022_2.pdf.

13. До «Всесвітнього дня боротьби з підробками» EUIPO розмістило інформацію щодо нових тенденцій в поведінці молодих європейців стосовно підроблених товарів та онлайн-піратства. URL: http://pakharenko.ua/do-vsesvitnogo-dnya-borotbi-z-pidrobkami-euipo-rozmistilo-informaciyu-shhodo-novix-tendencij-v-povedinci-molodix-yevropejciv-stosovno-pidroblenix-tovariv-ta-onlajn-piratstva/.

14. Samuel Baird, Noel Paterson How Some Brands are Successfully – and Cost-Effectively – Combating Online Counterfeiters. URL: https://www.ipwatchdog.com/2022/10/13/brands-successfully-cost-effectively-combating-online-counterfeiters/id=152088/.

Андрощук Г. О.
кандидат економічних наук, доцент,
головний науковий співробітник
Науково-дослідного інституту
інтелектуальної власності НАПрН
України
ORCID: 0000-0003-0781-9740
Работягова Л. І.
провідний науковий співробітник
Науково-дослідного інституту
інтелектуальної власності НАПрН
України
ID ORCID 0000-0002-5450-1607

ПАТЕНТНИЙ ТРОЛІНГ В ЦИФРОВІЙ ЕКОНОМІЦІ

За даними Всесвітнього економічного форуму частка цифрової економіки у загальносвітовій економіці перевищує 20% і стрімко зростає, більше 60% світових компаній працює над впровадженням своєї стратегії digital-трансформації. Однак застосування цифрових технологій та мобільних пристроїв в багатьох державах опинились під загрозою через

активізацію діяльності у цій сфері «непрактикуючих осіб» (NPE – non-practicingentity) або патентних тролів. На відміну від діючих компаній, які використовують свої патенти для виробництва та продажу свого продукту, патентні тролі часто задешево купують патенти у компаній-банкрутів і не використовують їх у виробництві, а лише стягують плату за ліцензування з інших підприємств та осіб, які, як їм здається, порушують патент, яким вони володіють.

Загальна стратегія патентних тролів полягає у тому, щоб зв'язатися з компаніями та пригрозити їм майбутньою судовою справою. Далі може бути кілька варіантів розвитку подій: 1) підприємець погоджується сплачувати ліцензійні платежі володільцю патенту (тобто патентному тролю) або домовляється про одноразову виплату суми (так званого штрафу), яку він вимагає; 2) підприємець не погоджується сплачувати за ліцензію, починається судова справа, патентний троль та підприємець укладають мирову угоду; 3) суд виносить своє рішення, зобов'язуючи підприємця платити ліцензійні платежі або не задовольняє позов непрактикуючої особи; 4) суд визнає недійсним (анулює) патент, який належить патентному тролю.

Варто зазначити, що сам по собі процес відкриття судової справи в багатьох випадках може тривати роками і коштувати кілька мільйонів доларів. Як результат, більшість компаній погоджуються вирішити цю проблему без витрат на судові процеси. Однак така угода може бути не найкращим рішенням, хоча це і може здатися на перший погляд вигідним. Патентні тролі, можуть продовжувати надсилати претензії у майбутньому, перетворивши короткострокову економічну перевагу одноразової виплати для підприємців у довгострокові постійні платежі.

США найбільше страждають від такого явища як патентний тролінг. Щороку патентними тролями близько $80 млрд виводиться з економіки США. Крім того, через їх діяльність суттєво зменшуються витрати на НДДКР, зокрема, на 48% у великих компаніях та на 19% – у малих. Наприклад, за статистикою RPX Corporation – американського постачальника послуг з управління патентного ризику по всьому світу, середній щорічний темп зростання кількості судових процесів з боку непрактикуючих осіб складає 20%. Це стосується перш за все сфери високих технологій, у якій 84% усіх поданих позовів за рік належать патентним тролям. Вражає також і кількість компаній, що постраждали від патентного тролінгу – на 2014 рік це вже понад 10000 американських підприємств [1].

Велику кількість патентних тролів у США пояснюють наявністю в американській судовій системі аспектів, які зазвичай називають «підтримкою тролів», а саме:

– високу вартість судочинства;
– правила розподілу витрат у суді (обидві сторони несуть свої витрати);
– сплату непередбачених гонорарів для адвокатів, яка стимулює продовження судових процесів;
– високу суму збитків та ризик потрійних збитків у разі визнання судом «навмисного порушення прав людини»;
– позицію американських судів та присяжних щодо патентоздатності винаходів;
– низьку якість експертизи, що створює невизначеність щодо обсягу правової охорони винаходу;
– загальне формулювання положень закону щодо патентоздатності програмного забезпечення та бізнес-методів [2].

Патентний тролінг у державах-членах ЄС є не таким поширеним явищем, як у США. Проте, ситуація наразі змінюється. Так відповідно до доповіді Darts-ip – провідної глобальної організації, яка займається аналітикою з інтелектуальній власності, у 2018 році, кількість судових позовів від патентних тролів у державах-членах ЄС суттєво зросла, зокрема, у період з 2007 до 2017 року майже втричі – з 65 до 173 за рік. Найбільше постраждала IT-індустрія, на неї припадає близько 75% усіх випадків. Звіт також показує, що це стосується не лише великих компаній – майже чверть усіх відповідачів є малі та середні підприємства [3]. Таку ситуацію пов'язують з тим, що американські непрактикуючі особи почали частіше працювати на європейському ринку. Експерти та всесвітньо відомі компанії, які працюють в ЄС, вважають, що Європейська комісія недостатньо займається проблемою патентного тролінгу та вимагають пришвидши створення єдиної патентної системи в ЄС.

Створення єдиної патентної системи в ЄС нерозривно пов'язано зі запровадженням Єдиного патентного суду (далі – ЄПС). Так, Регламент ЄС № 1257/2012 Європейського Парламенту та Ради від 17 грудня 2012 р. про впровадження посиленої співпраці у сфері створення єдиної патентної охорони та Регламент ЄС № 1260/2012 Європейського Парламенту та Ради від 17 грудня 2012 р. про впровадження посиленої співпраці у сфері створення єдиної патентної охорони щодо застосовних механізмів перекладу, які встановлюють єдину патентну охорону, набули чинності 20 січня 2013 р., але вони будуть застосовуватися лише від дати набрання чинності Угодою про ЄПС, тобто з першого дня четвертого місяця після здачі на зберігання 13-го документа про ратифікацію або приєднання держав-членів, які беруть участь, за умови, що серед них присутні три держави-члена (Німеччина, Франція та Італія).

Очікується, що після нещодавнього завершення необхідних ратифікаційних процедур державами-членами ЄС, які беруть участь (наразі їх 17), єдина патентна система запрацює навесні 2023 року. Створення єдиної патентної системи привнесе дві головні зміни:

1. Можливість звертатися до Європейського патентного відомства для отримання єдиного патенту, який буде діяти в усіх державах-членах ЄС, що беруть участь, як єдиний охоронний документ з єдиною дією без необхідності його визнання в кожній державі-члені. При цьому єдиний патент буде співіснувати з національними патентами і європейським патентом.

2. Наявність міжнародного ЄПС, наділеного виключною юрисдикцією щодо розгляду всіх справ про порушення та визнання недійсними європейських і єдиних патентів, а також справ про порушення і дійсність свідоцтв додаткової охорони, виданих для продукту, на який поширюється такий патент, та європейських патентних заявок. Його ухвали та рішення поки будуть виконуватись в державах-членах ЄС, що ратифікували Угоду про ЄПС.

Створення ЄПС забезпечить найкращі умови для всіх сторін, які беруть участь у патентних спорах у ЄС, а саме:

для володільців патентів ЄПС запропонує більш надійне забезпечення дотримання чинних патентів із загальноєвропейськими наслідками щодо прийнятих рішень, судових заборон та відшкодування збитків;

для третіх осіб та громадськості ЄПС забезпечить централізовану процедуру визнання патентів недійсними, яка може здійснюватися у будь-який час протягом усього строку дії патенту, незалежно від процедури заперечення, яка здійснюється в Європейському патентному відомстві.

Критики нової патентної системи стурбовані тим, що не повністю враховані всі наслідки її впровадження, зокрема для малого та середнього бізнесу. Так, можливість отримання судової заборони в масштабах всього ЄС до розгляду питання про дійсність патенту може зіграти на руку патентним тролям. Однак відповідно до ст.62(2) Угоди про ЄПС Суд не виносить попередні судові заборони автоматично, а на власний розсуд зважує інтереси сторін і, зокрема, бере до уваги потенційні збитки для будь-якої зі сторін внаслідок винесення або відмови в судовій забороні. Якщо володілець патенту (патентний троль) не займається практичною діяльністю, це відіграватиме роль у такій оцінці не на його користь.

Що стосується однієї з можливостей ЄПС припинити дію патенту за допомогою єдиної процедури одночасно на території всіх 17 держав-членів ЄС, якою можуть скористатися патентні тролі, то слід зазначити,

що в состав колегій ЄПС входять судді з юридичною освітою, і судді з технічною освітою, до яких висувають наступні вимоги: мати університетський диплом в будь-якій технічній галузі; високий фаховий рівень у цій галузі а також достатні знання в галузі цивільного та цивільно-процесуального права для вирішення патентних спорів.

Такий склад колегій ЄПС дозволить гармонізувати матеріальне патентне право стосовно обсягу та обмежень прав, що надаються патентом, а також засобів правового захисту у разі порушення патентних прав, забезпечить для судового провадження більш прості, швидкі та ефективні судові процедури, зокрема, щодо визнання недійсними патентів на програмне забезпечення, та патентів на винаходи, реалізовані на комп'ютері, володільцями яких дуже часто є патентні тролі. Крім того, на відміну від США, у Європі судові витрати лягають на сторону, яка програла. Такий підхід створює додаткові ризики для патентних тролів у разі поразки в судовому процесі.

Список використаної літератури:

1. Harward Business Review: The Evidence Is In: PatentTrolls DoHurt Innovation. URL:https://hbr.org/2014/07/the-evidence-is-in-patent-trolls-do-hurt-innovation

2. Андрощук Г. О., Работягова Л. І. Реформа патентної системи США: аналіз змін // Наука, технології, інновації. 2017. № 4. С.71-80.

3. Patent trolls arein creasingly targeting Europe's innovators. URL: https://guests.blogactiv.eu/2018/06/21/%E2%80%A8patent-trolls-are-increasingly-targeting-europes-innovators/

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

ПРОБЛЕМА ВИЗНАЧЕННЯ ЗМІСТУ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ ВАЛІДАТОРІВ БЛОКЧЕЙН-ТРАНЗАКЦІЙ

Технологія блокчейн з кожним роком набуває все більшого поширення та глобального транскордонного застосування. Провідні країни світу збільшують інвестування в проєкти пов'язані із технологіями розподілених реєстрів, і це приносить свої результати. Проте незважаючи на

кількість переваг, які дають останні, перед світовою спільнотою постала гостра необхідність у вирішенні значної кількості правових проблем, котрі породжує та котрі супроводжують цю технологію.

Однією із основних проблем правового регулювання суспільних відносин у сфері застосування технології блокчейн, яка потребує першочергового вирішення – є проблема визначення змісту юридичної відповідальності учасників блокчейн мережі. [1]

Враховуючи підвищений суспільний інтерес до криптовалют та криптоактивів вказану вище проблему ми будемо розглядати на їхньому прикладі. Тобто це дослідження стосуватиметься саме відкритого (публічного) блокчейну, який по-суті за своєю природою вже є саморегулюючою системою, яка враховуючи її складний технологічний характер не завжди може піддаватись правовому регулюванню.

Дослідивши одиничні моделі визначення змісту юридичної відповідальності розробників вихідного програмного коду блокчейн-проєктів, [1] ми можемо встановити особливості настання відповідальності валідаторів транзакцій (учасників блокчейн мережі, котрі проводять перевірку відповідності транзакцій, яка передує механізму консенсусу, найчастіше Proof-of-work (PoW) та Proof-of-stake (PoS), які таким чином генерують нові блоки в існуючий ланцюжок). [2] Під поняттям відповідності блокчейн-транзакції необхідно розуміти дотримання: а) правового режиму, де вона здійснена (чи не суперечить остання законодавству щодо відмивання коштів, фінансування тероризму, дотримання міжнародних економічних санкцій, оплати товарів виведених із цивільного обороту чи оплати незаконних послуг, шахрайства тощо); б) внутрішніх правил блокчейн мережі (наприклад, використання криптовалютних систем для нелегальної комунікації, злому закритих ключів, атаки на мережу тощо). [3]

Враховуючи особливості технології блокчейн, варто звернути увагу, що валідатори блокчейн-транзакцій можуть виступати, і як звичайні валідатори, котрі лише генерують нові блоки, так і як розробники програмного коду механізму проведення перевірки (протоколу), при цьому, як одні, так і інші можуть діяти одноосібно або колегіально.

Перевірка блоків є одним із ключових факторів, що забезпечує функціональність блокчейну. Без узгодження перевірених транзакцій неможливо досягнути консенсусу. Але, окрім користі, валідатори інколи завдають істотної шкоди учасникам блокчейн мережі. Так у останніх є можливість підтверджувати невідповідні транзакції та вчиняти різні атаки на механізм консенсусу. Часто валідатори володіючи 51% потужностей мережі можуть блокувати вже досягнутий консенсус між сторонами угоди

та створювати альтернативні блокчейни і проводити подвійне списання коштів за виконання транзакцій. [2]

У такому випадку шкода завдається як ініціаторам угоди, так і іншим учасникам блокчейн мережі (за рахунок зменшення вартості криптоактивів). За таких обставин, постає питання про притягнення винних осіб до відповідальності. Якщо говорити про відповідальність валідаторів за ініціювання угод з подвійним списанням або підтвердження невідповідних транзакцій, то саме юридична відповідальність буде найбільшим стимулом утриматись від вчинення таких дій. Однак, якщо говорити про атаку не блокчейн мережу, то основним інструментом її саморегулюючого захисту є протокол. І якщо юридична відповідальність замінить собою механізм саморегулювання, то це, *по-перше*, порушить основний принцип DLT, *по-друге*, значно знизить безпеку мережі, оскільки розробники втратять стимул створювати нові протоколи та покращувати вже існуючі. [3]

Таким чином, ми розглянемо правові основи для відповідальності валідаторів блокчейн транзакцій за погодження невідповідних угод, котрі здійснюються іншими учасниками блокчейн мережі та за безпосереднє ініціювання таких протиправних транзакцій, адже це є дуже важливим елементом в побудові системи правового регулювання застосування технології блокчейн.

У широкому розумінні можна сказати, що існує три умови настання юридичної відповідальності за вищевказані діяння:

1) наявність правової основи (бази);

2) наявність причинно-наслідкового зв'язку між діянням, яке спричинило шкоду з правовою основою для відповідальності;

3) наявність факту завдання матеріальних збитків чи репутаційних ризиків у разі порушення механізму консенсусу або фізичної шкоди у випадку втручання в роботу фізичних пристроїв, які керуються застосунками Інтернету речей.

Коли мова йде про притягнення до юридичної відповідальності валідаторів, які ініціюють невідповідні блокчейн-транзакції, то зробити це значно простіше ніж притягнути до відповідальності тих осіб, які погоджують протиправні угоди. [3] Оскільки валідатори отримують винагороду за свою діяльність, то коло їх обов'язків чітко визначене самою блокчейн мережею. Тому якщо валідатори, які не є розробниками протоколів ініціюють вчинення невідповідних транзакцій, то можна визначити безпосередню ступінь вини таких осіб. Натомість, якщо протиправні діяння всередині блокчейн мережі здійснюється за рахунок протоколів, то в такому випадку необхідно робити перевірку на відповідність вихід-

ного програмного коду самого протоколу, але відповідальність в такому випадку буде нести не та особа, яка цей код розробила, а та яка його запустила, [4] що ще раз підтверджує нашу тезу про те, що цей елемент саморегуляції блокчейн мережі набагато складніше піддати правовому регулюванню.

Також дискусійним є питання, чи з'являються у валідаторів, які виступають у ролі розробників механізму перевірки блокчейн-транзакцій фідуціарні обов'язки перед іншими користувачами мережі (частіше за все, перед ініціаторами угод). З одного боку, умисне невиконання програмного коду транзакцій, або ухилення від переходу на оновлену версію вихідного програмного коду, який може принести користь іншим користувачам є прикладами порушення таких обов'язків. Також до них можна віднести зобов'язання відхиляти пропозиції «хардфорку», який має на меті завдання шкоди іншим користувачам блокчейн-мережі та виконання завідомо хибного програмного коду націленого на перевірку «пустих» блоків. [5] Проте, це лише припущення, оскільки обсяг фідуціарних обов'язків валідаторів без встановлення чітких правових засад їх визначення залишається відкритим. Скоріше за все лише судова практика допоможе вирішити цю проблему.

Правовою основою для притягнення валідаторів блокчейн-транзакцій, які за власною ініціативою здійснюють вплив на консенсус між сторонами угоди може стати кримінальне, фінансове та антимонопольне законодавство. Зміна ланцюжка блоків з метою блокування вже досягнутого консенсусу між сторонами контракту з точки зору кримінального права може вважатись шахрайством. Так само можна говорити про крадіжку, якщо валідатори створять альтернативний блокчейн та проведуть подвійне списання криптовалют за транзакцією. Фінансове законодавство може встановити підстави для юридичної відповідальності валідаторів за навмисне маніпулювання цінами на криптоактиви або деривативи. У випадку, якщо деякі валідатори об'єднаються з метою зловживання домінуючим становищем, то відповідальність за це може передбачатись антимонопольним законодавством. [5]

Натомість, як вже сказано вище, притягнути валідаторів, які підтверджують невідповідні транзакції до юридичної відповідальності значно важче, особливо, коли вони діють дійсно децентралізовано. Не рідко за таких обставин відсутні докази, хто саме записав протиправну транзакцію в блок, відтак відсутній причинно-наслідковий зв'язок між діянням та правовою основою для відповідальності, до того ж постає питання визначення ступеня вини в завданні матеріальних збитків, оскільки валідатор лише підтверджує транзакцію ініційовану іншими учасниками

блокчейн мережі. При цьому, якщо в одній юрисдикції певні транзакції суперечать закону, це не означає, що їх не можливо вчинити в іншій юрисдикції, тому в такому випадку юридична відповідальність не гарантує того, що якщо один валідатор відмовився підтверджувати протиправну транзакцію, то цього не зробить інший. Саме тому, це питання необхідно вирішувати на міжнародному рівні. [3]

Отже, підсумовуючи вищесказане, можна дійти висновку, що проблема визначення змісту юридичної відповідальності валідаторів блокчейн-транзакцій є вкрай актуальною, адже останні виконують одну з провідних функцій у діяльності блокчейн мережі. На сьогодні дійсно існують деякі перепони в притягненні окремих категорій валідаторів блокчейн-транзакцій до юридичної відповідальності, особливо коли це стосується елементів саморегуляції системи, проте це не означає, що проблема взагалі не підлягає вирішенню. У публічному блокчейні це питання можна вирішувати лише шляхом поєднання зовнішніх правових механізмів (там, де це можливо) з внутрішніми саморегулюючими процесами мережі, таким чином досягаючи компромісу між децентралізацією системи та правовим регулюванням з боку держави. У приватному ж блокчейні, ця проблема вирішується значно простіше, так, валідаторів блокчейн-транзакцій можна за аналогією з криптовалютними біржами та іншими постачальниками віртуальних активів зобов'язати дотримуватись певних правил (у тому числі ставити ЕЦП на схвалені ними угоди), так само цих суб'єктів можна зобов'язати реєструватись у відповідних державних органах, або взагалі зробити цю діяльність ліцензійною.

Список використаних джерел:

1. Васько В. А. Проблема визначення змісту юридичної відповідальності розробників відкритого вихідного коду блокчейн-проєктів. 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.

2. Proof of Work (PoW) проти Proof of Stake (PoS). URL: bit.ly/3ES2j

3. Østbye Peder. Who is Liable for Non-Compliant Cryptocurrency Transactions: Should Transaction Validators be Held Liable? URL: bit.ly/3ERKL6U.

4. Felipe Herrera. Who is the data controller on the blockchain? URL: bit.ly/3TYPc4i.

5. Østbye, Peder, Who is Liable if a Cryptocurrency Protocol Fails? URL: bit.ly/3i6bbZX.

Заславська Л. В.
науковий співробітник Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України»

ЕЛЕКТРОННІ БІБЛІОТЕКИ ЯК СКЛАДОВА НАЦІОНАЛЬНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ УКРАЇНИ

Стрімкий розвиток суспільства, цифрова трансформація та поширення інформаційних (цифрових) технологій сприяють кардинальним змінам суспільних відносин в усіх сферах життєдіяльності людини та суспільства. Зазначене також стосується цифровізації бібліотечної справи та подальшому розвитку електронних бібліотечних ресурсів (е-бібліотек).

Бібліотеки України є базовим елементом культурної, наукової, освітньої, інформаційної інфраструктури держави. Вони важливі для розвитку інформаційної та мовної культури суспільства, патріотичного, правового та екологічного виховання, формування стійкого інтересу до вивчення та розуміння національної історії та культури. Бібліотеки сприяють розбудові читаючої, мислячої та освіченої нації, спроможної практично втілювати набуті знання і досвід у розбудову незалежної України.

Кабінет Міністрів України ухвалив Розпорядження № 219-р від 23 березня 2016 р. «Про схвалення Стратегії розвитку бібліотечної справи на період до 2025 року «Якісні зміни бібліотек для забезпечення сталого розвитку України». [1]

Метою Стратегії є визначення ключових проблем розвитку бібліотечної справи в Україні, пріоритетів діяльності сучасних бібліотек у забезпеченні сталого розвитку України, напрямів, завдань та основних дій, спрямованих на їх реалізацію.

Бібліотечна справа потребує вжиття низки комплексу системних організаційних, структурних і технологічних змін згідно із сучасними загальносвітовими тенденціями.

На сьогодні бібліотечна мережа в Україні нараховує близько 40 тис. бібліотек державної та комунальної власності, відомчого підпорядкування. Вона складається з мережі публічних (у тому числі спеціалізованих для дітей, юнацтва), технічних, сільськогосподарських, медичних, академічних, освітянських бібліотек та бібліотек вищих навчальних закладів, а також бібліотек для сліпих.

Різноманітні потреби населення в інформації, освіті, культурі нині забезпечують 15987 публічних бібліотек (з них 13253 – у сільській міс-

цевості). Кожен третій мешканець України (понад 13,7 млн.) є користувачем публічних бібліотек. Бібліотечний фонд публічних бібліотек універсальної тематики становить близько 235 млн. одиниць. Водночас, доступ до Інтернету має лише 3,3 тис. (21 %) бібліотек, а загальна кількість комп'ютеризованих робочих місць у публічних бібліотеках сягає 16 тис. (в середньому *один комп'ютер на одну бібліотеку*) [1].

Сучасний швидкий темп розвитку людства майже зовсім не залишає часу на перебування, читання та знаходження інформації в приміщеннях бібліотек. Реальність така, що майже усі верстви населення перебувають в цифровому інформаційному просторі. Будь-яку інформацію сучасна людина черпає з інтернет-простору. І якщо доросла людина, в міру своєї освіченості та обізнаності вже може певним чином «фільтрувати» той чи інший контент, то діти та підлітки вразливі до різних інтернет-загроз. Звичайне читання книги для дітей не таке цікаве як різні ролики в інтернет-просторі, які можуть нести спотворену та недостовірну інформацію. Було б досить не погано, якби наприклад вводячи запит на певне слово чи термін в пошукових сервісах, ми мали змогу не лише на його тлумачення у вікіпедії, а й посилання на єдину ***Національну електронну бібліотеку***. Саме її створення і передбачене *Стратегією розвитку бібліотечної справи на період до 2025 року* "*Якісні зміни бібліотек для забезпечення сталого розвитку України*" [1].

Основні задачі електронної бібліотеки – інтеграція інформаційних ресурсів та ефективна навігація в них.

Інтеграція інформаційних ресурсів – це їхнє об'єднання з метою використання різної інформації зі збереженням її властивостей, особливостей представлення і можливостей її обробляти. Цифрове об'єднання бібліотечних інформаційних ресурсів може відбуватися як фізично, так і віртуально. Але при цьому таке об'єднання повинно забезпечувати користувачу сприйняття необхідної інформації як єдиного інформаційного простору: електронна бібліотека повинна забезпечити роботу з електронними базами даних та високу ефективність інформаційних пошуків.

Ефективна навігація в електронній бібліотеці – це можливість користувача знаходити інформацію, яка його цікавить, в усьому доступному інформаційному просторі з найбільшою повнотою і точністю при найменших витратах зусиль [2].

Основні функції електронної бібліотеки відповідають функціям сучасної традиційної бібліотеки, проте вони модифіковані, оскільки ґрунтуються на широкому використанні сучасних інформаційних технологій, які фахівці окреслюють так:

– *кумулятивна* – формування інформаційних ресурсів в електронній формі з використанням різних форматів;
– *меморіальна* – зберігання впродовж тривалого часу в електронній формі інформаційних ресурсів, що містять відомості про історію і культуру, що забезпечує формування соціальної пам'яті суспільства;
– *комунікаційна* – надання доступу користувачам до баз знань;
– *інформаційна* – задоволення інформаційних потреб різних категорій користувачів;
– *довідкова* – пошук достовірних фактографічних та бібліографічних даних;
– *освітня* – інформаційний супровід освітніх, науково-дослідних, виробничих процесів;
– *культурна (просвітницька)* – за допомогою інноваційних технологій введення в науковий обіг, поширення серед користувачів інформації про документи, які складають історичну та культурну цінність;
– *когнітивна* – управління знаннями та продукування нового знання, його аналітико-синтетичне опрацювання з використанням новітніх інформаційних технологій;
– *соціальна* – надання користувачеві можливості дистанційного освоєння знань, ознайомлення з алгоритмами інформаційного пошуку на основі інноваційних інструментів, які забезпечують ефективне орієнтування в інформаційному просторі, такий підхід спонукає його до участі у соціокомунікативних процесах;
– *науково-дослідницька* – інформаційна підтримка наукових досліджень та проведення власних наукових розвідок.

Основним призначенням електронних бібліотек є надання читачам повних текстів документів і функціональних можливостей роботи з ними в поєднанні з інформацією, поданою в інших форматах, наприклад, файлів, що містять зображення, звук, анімацію, відео. Саме можливість накопичувати і надавати доступ до документів різного формату є вагомою перевагою електронних бібліотек. Сьогодні активно діє безліч електронних бібліотек, що містять інформаційні ресурси різних напрямів, обсягу і якості, доступні користувачам через глобальну мережу Інтернет [3].

Національна бібліотека України імені В. І. Вернадського (НБУВ) у 2013 р. на Конгресі українознавців презентувала новий проект – *«Електронна бібліотека «Україніка» – зведеного бібліографічного та електронного ресурсу усієї документальної спадщини України* з організацією доступу до науково-довідкових, бібліографічних і текстових ресурсів,

репрезентації оригіналів документів у цифровому форматі з широкими можливостями представлення на сайтах бібліотек, архівів, наукових установ у глобальній світовій мережі.

Започаткована НБУВ «Україніка» має передусім науковий, академічний, характер. Її головне призначення – слугувати якомога більш повною інформаційною базою для розвитку вітчизняної науки, вищої освіти, задоволення потреб закладів культури, органів державного управління, політикуму. Мета проекту – акумулювати у цифровому форматі твори усіма мовами, незалежно від місця видання, про український народ, територію України та про всі народи, які жили або живуть на цій території. Це дозволило надати користувачам електронної бібліотеки знання про Україну, її народ, його історію, традиції та культуру, розбудовану політичну націю, сформовану нею державу; матеріали про природне, географічне середовище, демографічний, економічний, соціальний, освітній, науковий потенціал України, здобутки української нації, її місце у світовому цивілізаційному розвитку.

Основними джерелами поповнення електронної бібліотеки є електронні ресурси НБУВ, вільнодоступні мережеві електронні ресурси, українознавчі сайти та веб-ресурси наукових установ, культурних закладів, оцифровані видання із фондів НБУВ та інших бібліотек, авторські електронні версії видань. Наразі триває наповнення електронної бібліотеки [3].

В Україні також існують інші електронні бібліотеки, як наприклад:

1) Електронна бібліотека «Культура України» створена за ініціативи Національної бібліотеки України ім. Ярослава Мудрого.

2) Електронна бібліотека «Diasporiana» (http://diasporiana.org.ua/) – проект зі збереження інтелектуальної спадщини української еміграції, заснований у 2011 р.

3) EXLIBRIS: українська електронна бібліотека: історія, публіцистика, художня література» (http://exlibris.org.ua/).

4) LIBRARIA – електронна бібліотека компанії Архівні інформаційні системи (АІС), що здійснюється у співпраці з бібліотеками, архівами та науковими інституціями в Україні та за її межами, та ін. [3].

Хоча варто визнати, що кожна із цих установ реалізує окремо власні проекти оцифрування рідкісних документів та створює різноманітні бази даних, електронні бібліотеки тощо. І якщо подивитись статистику користування цими ресурсами, то вона буде дуже великою. Але зовсім не йдеться про злагодженість дій та об'єднання зусиль.

Портал «Дія» теж має свій проект «Цифрова трансформація бібліотек та книговидавничої справи (е-Книга)», що має бути реалізований до

29 грудня 2022 року [4]. Він передбачає впровадження автоматизованої бібліотечної інформаційної системи, української цифрової бібліотеки, автоматизацію подання документів для отримання грантової підтримки, ведення електронного каталогу з інформацією про доступні книжки на національному ринку. Один із її підпроектів «Українська цифрова бібліотека» – це платформа, де будуть зібрані сучасні книжки українських та іноземних авторів (переклади), підручники для школярів в форматі epub, забезпечений доступ до них через мобільний застосунок на смартфоні (для індивідуального користування) та через веб-інтерфейс (для бібліотек).

Проте питання створення єдиної Національної електронної бібліотеки залишається й досі відкритим, мабуть через велику кількість питань та проблем, що постають у створенні такої бібліотеки. Це насамперед:

- *технічне забезпечення* (серверні потужності, техніка для оцифрування);
- *стандарти* (цифрових об'єктів, обміну даними, правила каталогізації);
- *програмне забезпечення*;
- *довготривале збереження* (файлів оцифрованих об'єктів, можливість доступу до файлів в довгостроковій перспективі);
- *низка правових питань* (переведенню в електронну форму підлягають об'єкти, які не охороняються авторським правом, на які закінчився строк охорони авторського права та на які поширюється дія нормативно-правових актів із питань авторського права та суміжних прав (у разі надання відповідного дозволу автором або особою, яка володіє авторськими правами), запозичення електронних документів, вироблених іншими особами або організаціями, здійснюється на договірній основі з дотриманням норм чинного законодавства та з урахуванням взаємних інтересів).

Те, що проекти цифрової трансформації бібліотек та бібліотечної справи визначені як пріоритетні та увійшли до стратегічних державних документів, вселяє надію. Хочеться вірити, що ми все ж будемо спроможні реалізувати плани, й те, що вже давно працює практично в кожній цивілізованій країні, ми теж зробимо.

Бо найголовніше, на що треба зважати всім сторонам, які включені в процеси цифрової трансформації, що сучасні ІТ в бібліотеках і професійно впроваджені та діючі національні проєкти не є самоціллю. Вони не для того, щоб відзвітувати, не для того, щоб просто бути, бо вони є у інших. Це не данина моді. Це потрібно, щоб бібліотеки просто могли нормально працювати і виконувати своє суспільне призначення з більшою

користю та витратою менших ресурсів. Щоб кожен, кому це необхідно, швидко, легко та зручно знайшов серед всього масиву інформації, яку пропонують бібліотеки, те, що йому потрібно, і міг цим скористатися [5].

Це потрібно перш за все для досягнення таких ***основних цілей цифровізації бібліотечної справи***:

- інтеграції культури Українського народу у європейський та світовий інформаційний простір, зміцнення культурних зв'язків і формування позитивного іміджу України у світі;
- забезпечення рівних можливостей безкоштовного доступу користувачів до надбань української культури і мистецтва за допомогою Інтернет мережі;
- надання користувачам якісно нових можливостей роботи з інтегрованим інформаційним ресурсом бібліотек, музеїв та інших закладів культури в єдиній точці доступу;
- створення електронних копій друкованих документів для збереження культурної спадщини, що знаходиться у фондах бібліотек та інших закладів культури та запобігання фізичного зносу документів;
- підвищення ефективності використання документів, розкриття фондів бібліотек, музеїв, архівів та інших закладів культури з питань культури і мистецтв;
- створення можливості працювати одночасно з одним і тим же виданням різним користувачам.

Список використаних джерел:

1. Розпорядження № 219-р від 23 березня 2016 р. Документ 219-2016-р, чинний, поточна редакція — Прийняття від 23.03.2016. [Електронний ресурс] Режим доступу: https://zakon.rada.gov.ua/laws/show/219-2016-%D1%80#Text

2. Вікіпедія. Електронна бібліотека. [Електронний ресурс] Режим доступу: https://uk.wikipedia.org/wiki/%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0_%D0%B1%D1%96%D0%B1%D0%BB%D1%96%D0%BE%D1%82%D0%B5%D0%BA%D0%B0 Дата звернення 04.11.2022 р.

3. Електронні бібліотеки України як джерелознавча база наукових досліджень. Кізян Ольга Іванівна [Електронний ресурс] Режим доступу: https://library.vn.ua/Konf2019/texts/6_1.htm Дата звернення 04.11.2022 р.

4. Портал «Дія». Проєкти цифрової трансформації. [Електронний ресурс] Режим доступу: https://plan2.diia.gov.ua/projects. Дата звернення 04.11.2022 р.

5. Відставання на 20 років: цифрова трансформація бібліотек та реальні можливості змін. Оксана Бруй. [Електронний ресурс] Режим доступу: https://chytomo.com/vidstavannia-na-20-rokiv-tsyfrova-transformatsiia-bibliotek-ta-realni-mozhlyvosti-zmin/ Дата звернення 04.11.2022 р.

Petriaiev O.
https://orcid.org/0000-0001-6561-2647

THE USE OF SOCIAL AND DIGITAL TRANSFORMATION IN THE ZONE OF GEOPOLITICAL INTERESTS

In the conditions of the fourth technological revolution, there is a trend of social transformations that lead to social and geopolitical changes. Consider this trend on the example of the Republic of Turkey.

After the collapse of the Ottoman Empire and the First World War, Turkey was in search of its new place in the political arena of the world. Its new leader, Mustafa Kemal Ataturk, realizing that by the beginning of the 20th century, in the conditions of European industrialization, the territory of the former Ottoman Empire was still in a patriarchal society, undertook a number of state reforms in order to modernize political, economic and social life. After the Second World War, in the conditions of the Cold War between the North Atlantic military bloc and the Warsaw Pact bloc, Turkey joined the former, thereby securing its southern borders from the spread of communism, and providing the West with a corridor to the Middle East.

After the end of the Cold War, Turkey launched the processes of its resuscitation as a strong regional state. In the conditions of the opened markets of the former republics of the Soviet Union, the Republic of Turkey managed to develop its economy and strengthen its industrial potential. The historical chance of revival that was given to Turkey made it possible to expand its zone of influence in the territories that were once part of the Ottoman Empire. Turkey has used hard, soft and smart power as tools of geopolitical influence on the zones of its interests.

The Caucasus, Central Asia, the Balkans, North Africa and the Middle East became the zones of strategic interests of the Turkish Republic. The strategy was to develop relations with new states that were close to Turkey in ethno-religious sense. The only country from the region of the Caucasus and Central Asia, which was excluded from the influence of Turkey due to historical and social reasons, was Armenia. Thus, by the new millennium,

Turkey was to become a center of attraction for those close to it in religion, ethnicity, language and spirit of the new independent countries [1].

After the Justice and Development Party came to power in 2002, elements of the ideology of the times of the Ottoman Empire and historical revisionism were clearly manifested in the political life of Turkey. In place of the internal secular policy pursued by the Turkish leader Mustafa Kemal Ataturk, the process of returning to Islam began in the country, which began to penetrate into the political and social life of the country. Foreign policy has also changed; it became more aggressive; the country took an active part in military operations in Libya, Iraq, Syria and Afghanistan.

The new ideology of the Turkish Republic in the 21st century was Neo-Ottomanism and Erdoganism. Turkish researcher Mehdiev E. T. defines the concept of Neo-Ottomanism as a strategic course aimed at returning the «Ottoman past» taking into account modern realities. This ideology is based on four principles: blood, Ottoman thinking, soil and language. The main task of the ideology is the complete rejection of the ideology of Kemalism, the formation of a new Ottoman thinking and the construction of a supra-Turkish identity through the application of the mechanism of humanitarian and economic policy. Also, military methods can be used. The ultimate goal of neo-Ottomanism is to make Turkey a new supra-regional leader [2].

The ideology of Erdoganism, is based on the charisma of the leader of Turkey, Tayyip Recep Erdogan, his populist policy and the return to the religious origins of Turkey in order to make the Republic of Turkey the center of the Islamic world.

Thus, during the reign of Erdogan, Turkey has become not only a strong military state, but also an intermediary for the transportation of energy and food from the Caucasus, the Russian Federation, Ukraine and the Middle East to European countries.

The Republic of Turkey is also actively using propaganda. For example, between 2011 and 2015, Turkey filmed five seasons of the Magnificent Century series about the reign of Suleiman the Magnificent. The series were shown in 58 countries. Despite the initial criticism, the series played the role of an informational policy of glorifying the former greatness of the Ottoman Empire, and created interest in the modern Republic of Turkey [3].

Thus, the Republic of Turkey, using political, economic, military and informational methods of influence, as well as the ideology of Neo-Ottomanism, is building a new structure of domination in the region of the former Ottoman Empire and Turkestan.

References:

1. Уразова Е. И. Экономическая активность Турции в Кавказко-Центральноазиатском регионе. Турция в условиях новых внутренний и внешних реалий: сборник статей. М.: 2010. с. 156-170.
2. Мехдиев Э. Т. «НЕООСМАНИЗМ» В РЕГИОНАЛЬНОЙ ПОЛИТИКЕ ТУРЦИИ. Вестник МГИМО-Университета. 2016;(2(47)). с. 32-39.
3. Великолепный век. URL: https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%BB%D0%B8%D0%BA%D0%BE%D0%BB%D0%B5%D0%BF%D0%BD%D1%8B%D0%B9_%D0%B2%D0%B5%D0%BA (20.11.2022)

Сердечна А. Ю.
старший викладач кафедри
кримінального права та кримінології
Національної академії Служби безпеки
України

ДОСВІД УДОСКОНАЛЕННЯ КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВІЙНИ

На сьогоднішній день Україна протистоїть найсерйознішому за роки своєї незалежності виклику у сфері забезпечення державної безпеки – повномасштабна війна, яку розв'язала рф проти України, вимагає рішучих та ефективних заходів, направлених на захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки, та вироблення нових підходів до виявлення відповідних загроз, їх попередження і припинення.

В Стратегії інформаційної безпеки, затвердженої Указом Президента України 28 грудня 2021 року № 685/2021, інформаційну безпеку визначено як «складову частину національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціо-

нованне розповсюдження, використання й порушення цілісності інформації з обмеженим доступом».

Інформаційну безпеку складають найрізноманітніші відносини, що містять своїм невід'ємним компонентом інформаційну складову, на яку вказує низка термінів, що використовуються законодавцем у побудові кримінально-правових норм та які визначають відносини у сфері забезпечення інформаційної безпеки. Це такі уживані в законі слова та сполучення, що характеризують предмет злочину, як: «відомості», «дані», «таємниця», «документи», «матеріали», «носій», , «комп'ютерні мережі», «засоби зв'язку» тощо. На ознаки протиправного діяння, що посягає на інформаційну безпеку, вказують такі терміни: «розголошення», «розповсюдження», «завідомо неправдиве повідомлення», «втрата», «привласнення», «заклик», «фальсифікація» тощо [1, с.278–282].

Стратегічною ціллю № 1 вказаної Стратегії визначено протидію дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави. При цьому серед основних заходів, направлених на її досягнення, зазначено створення системи протидії дезінформації та інформаційним операціям, а також посилення відповідальності за поширення недостовірної інформації (дезінформації).

Оскільки збройна агресія рф проти України супроводжується інформаційними кампаніями, інформаційно-психологічними та спеціальними операціями, поширенням колаборційної діяльності на захоплених окупантом територіях, які підривають національну безпеку України та становлять безпосередню загрозу державному суверенітету, територіальній цілісності, конституційному ладу та іншим національним інтересам України, для запобігання цьому до Кримінального Кодексу України було внесено зміни, якими встановлено кримінальну відповідальність за вищевказаними протиаправні діяння.

Так Кримінальний кодекс України доповнено наступними статтями:

ст. 111^1 – «Колаборційна діяльність». Нею охоплюється значна кількість складів кримінальних правопорушень щодо співпраці з державою-агресором. Обєктивна сторона вказаного злочину має декілька форм, а саме: а) публічне заперечення здійснення збройної агресії проти України, встановлення та утвердження тимчасової окупації частини території України; б) публічні заклики до підтримки рішень та/або дій держави-агресора, збройних формувань та/або окупаційної адміністрації держави-агресора; співпраці з державою-агресором, збройними формуваннями та/або окупаційною адміністрацією держави-агресора, невизнання

поширення державного суверенітету України на тимчасово окуповані території України.

ст. 111^2 – «Пособництво державі-агресору». Законодавець визначив пособництвом умисні дії, спрямовані на допомогу державі-агресору, збройним формуванням та/або окупаційній адміністрації держави-агресора, з метою завдання шкоди Україні шляхом: реалізації чи підтримки рішень та/або їх дій; добровільного збору, підготовки та/або передачі матеріальних ресурсів чи інших активів їх представникам.

ст. 114^2 – «Несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану». Кримінально караним за вказаною статтею визнається: а) виключно «поширення» інформації; б) вичерпний перелік якої наведено у ч. 1 та ч. 2 розглядуваної кримінально-правової заборони; в) поширення не обов'язково має бути публічним.

ст. 436^2 – «Виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників». Обєктивна сторона вказаного злочину має такі форми: а) виправдовування збройної агресії РФ проти України, розпочатої у 2014 році; тимчасової окупації частини території України; б) визнання правомірною збройної агресії РФ проти України, розпочатої у 2014 році; тимчасової окупації частини території України; в) заперечення збройної агресії РФ проти України, розпочатої у 2014 році; тимчасової окупації частини території України; г) представлення збройної агресії РФ проти України як внутрішнього громадянського конфлікту; д) глорифікація: осіб, які здійснювали збройну агресію РФ проти України, розпочату у 2014 році, представників збройних формувань РФ, іррегулярних незаконних збройних формувань, озброєних банд та груп найманців, створених, підпорядкованих, керованих та фінансованих РФ, представників окупаційної адміністрації РФ, яку складають її державні органи і структури, функціонально відповідальні за управління тимчасово окупованими територіями України, представників підконтрольних РФ самопроголошених органів, які узурпували виконання владних функцій на тимчасово окупованих територіях України.

Безумовно, таке реагування законодавця на перманентні та небажані факти несанкціонованого поширення різноманітної інформації, і як наслідок, встановлення за це кримінальної відповідальності, є надзвичайно важливими для запобігання та припинення протиправної діяльності, направленої на підрив національної безпеки, та становить загрозу національним інтересам України.

Водночас серед науковців, практиків та в експертному середовищі триває дискусія щодо меж криміналізації колабораціонізму та інших недоліків у законодавстві. Про ці недоліки говорять як правозахисники, так і представники органів влади. Практика свідчить про те, що застосування положень ст. 111-1 КК України ускладнило розмежування правопорушень, передбачених ст.ст.111 («Державна зрада»), 111-1 («Колабораційна діяльність»), 111-2 («Пособництво державі-агресору») і 436-2 («Виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників») КК України. Так, наприклад, в диспозиції ст. 111-2 КК України йдеться про колабораційну діяльність в окремих формах, які вже передбачено статтею 111-1 КК України.

Задля усунення широкого тлумачення та протиріч, до Верховної Ради України подані декілька законопроектів щодо удосконалення відповідальності за колабораційну діяльність та суміжні кримінальні правопорушення та відповідно внесення змін до Кримінального та Кримінального процесуального кодексів України.

Список використаних джерел:

1. Дзюба Ю. П. Інформаційна безпека в системі міжгалузевих зв'язків кримінального права / Ю. П. Дзюба // Наука кримінального права в системі міждисциплінарних зв'зків : матеріали міжнар. наук.-практ. конф., 9-10 жовт. 2014 р. – Харків, 2014. – С. 278–282. – Режим доступу: http://dspace.nlu.edu.ua/ handle/123456789/7076

Погорілий М. І.
студент Національної академії Служби безпеки України, Науковий керівник: доктор військових наук, проф. Шемаєв В. М.

СОЦІАЛЬНІ МЕРЕЖІ РФ VK.COM ТА CHATROULETTE.COM – ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ

З початку відновлення незалежності української держави синьо-жовтий стяг мирної України, в результаті агресивних дій нашого східного сусіда, на жаль, перетворюється на червоно-чорний.

Крім прямого фізичного протиборства, яке почалося у 2003 році з російсько-українського конфлікту навколо острова Тузла, та відкрито

продовжилося у 2014 році воєнною агресією російської федерації (далі – рф) шляхом повної анексії Автономної республіки Крим (далі – АРК) України, рф паралельно веде проти нашої держави інформаційно-психологічну війну.

Психологічна війна використовує пропаганду та різні види інформації задля впливу на думки, емоції, погляди та поведінку супротивника. Якщо подивитися на інформаційний простір, то ми можемо побачити: коли ідея перемагає, за нею йдуть люди – військові, цивільні, спостерігачі та виборці, які поділятимуть таке бачення реальності. Якщо ж ідеї програють в інфопросторі, то фізичну битву можна програти ще до її початку.

Відтак, російські служби спеціального призначення у цій війні широко використовують інформаційну зброю, при чому для впливу не тільки на свідомість українців, а й на населення власної країни, з метою нав'язування ідей дискредитуючих Україну. При застосуванні терміну «інформаційна зброя», ми розуміємо донесення інформації у такий спосіб, який змінює сприйняття та думки щодо ситуації, спричиняє переосмислення мотивацій жертви, і, як наслідок — втрату або навпаки появу бажань воювати чи протистояти.

Направленість інформаційної зброї може впливати на конкретні фрейми-мішені знань, до повних епістемологічних спотворень — змінювати організацію, структурні методи та обґрунтованість знань. Окремі дослідники інформаційного впливу зазначають, що окрім зброї, інформація теж може бути мішенню і бути перетворена у дезінформацію.

Одним з різновидів інструментарію інформаційної зброї російської федерації у війнах проти своїх сусідів та зокрема України, є соціальні мережі. З поміж інших, у своєму дослідженні ми виділяємо такі ресурси:

1. Vk.com (більш відомий як «ВКонтакті») — російська соціальна мережа, яка належить однойменній компанії (колишній Mail.ru Group). Засновник Дуров Павло Валерійович 1984 року народження. Найбільш популярна у Росії, Білорусі, Казахстані та Узбекистані [1].
2. Chatroulette.com (більш відомий як «Чат рулетка») — російський веб-сайт, який дозволяє «анонімно» спілкуватися за допомогою відео та текстового чату. Відвідувач веб-сайту потрапляє на випадково обраного незнайомця і починає з ним онлайн-чат. Навесні 2010 року відвідуваність сайту досягала 1,5 млн осіб на день. Веб-сайт належить російському його засновнику — програмісту Андрію Терновському 1995 року народження [2].

Обидва веб-сайти повністю підконтрольний російським спецслужбам. У нашій державі, вищевказані веб-сайти заборонені та заблокова-

ні для використання на території України Указами Президента України від 15 травня 2017 року № 133/2017 [3] та від 14 травня 2020 року № 184/2020 [4].

Загроза національній безпеці України, яку несе у собі «ВКонтакті» обумовлена тим, що у період від заснування у 2006 року і до анексії російською федерацією Автономної республіки Крим України 2014 року, його користувачами було близько 9 млн. українців. Багато хто з наших громадян добровільно вказували на сторінках своїх профілів детальну особисту інформацію, таку як: прізвище, ім'я, по батькові; дату та місце народження; адресу проживання; дані про освіту (освітні заклади); дані про кар'єру (місця роботи та посади); сімейний статус (усі родинні зв'язки); мову спілкування; контакти (номери телефонів, адреси електронної пошти та посилання на профілі в інших соціальних мережах); особисті фотографії (у т.ч. з місць відпочинку та відмітками друзів).

У листопаді 2013 року в Україні розпочалася Революція гідності, на той момент веб-сайт vk.com ще належав його засновнику Дурову П. В. У грудні 2013 року федеральна служба безпеки (далі – фсб) рф почала вимагати від нього надати їм особисті дані організаторів груп Євромайдану. Згодом, Дуров П. В. був змушений залишити посаду генерального директора компанії та продати свою частку власності особам, афілійованим зі спецслужбами рф.

У 2014 році після нападу рф на Україну, американська компанія з кібербезпеки CrowdStrike виявила, що російські хакери, пов'язані з групою APT28, поширили через для застосунок «ВКонтакті» на платформі операційної системи Android шкідливий вірус. Він проник в програмне забезпечення українських артилеристів (в розрахунковий засіб для наведення гаубиць) та дозволив росіянам визначати місце розташування української артилерії, з метою подальшого завдання по них удару російськими силами. Експерти з кібербезпеки вважають, що соцмережі представляють ще більшу небезпеку, ніж пропаганда, ставши стартовими майданчиками для хакерських атак [5].

Таким чином фсб рф отримали широку базу персональних даних багатьох росіян, білорусів, казахів, узбеків, вірменів, азербайджанців, грузинів, та на жаль, близько 9 млн. українців, яка тепер використовуються як інструмент інформаційної війни проти України шляхом застосування при проведенні інформаційно-психологічних операцій.

Відповідно до Настанови Збройних сил США 3-13 «Інформаційні операції» (Joint publication 3-13 «Information operations») від 2006 року спеціальні інформаційні операції (далі – СІО) – це інтегроване застосування ключових можливостей електромагнітних засобів,

комп'ютерних мереж, психологічних операцій, військового мистецтва та безпекових операцій разом із спеціальною підтримкою та відповідними можливостями з метою впливу, руйнування, завдання шкоди, захоплення процесу ухвалення рішень (людиною чи технічними засобами) [6].

З початком повномасштабного наступу збройних сил російської федерації (далі – зс рф) на територію України від 24 лютого 2022 року, українська інформаційна спільнота, зокрема блогери, почали національний спротив на інформаційному фронті. Застосовуючи веб-сайт chatroulette.com, вони сатирично спілкуються з росіянами, котрі підтримують збройну агресію рф проти України, висміюючи їх низький інтелектуальний рівень, соціальний статус та рівень життя в цілому. Багато українців (не тільки цивільні, а й військовослужбовці) теж почали використовувати даний сервіс для тролінгу росіян. Така діяльність беззаперечно позитивно впливає на укріплення свідомості наших громадян, протидіючи російській пропаганді, але разом з тим й несе серйозну загрозу національній інформаційній безпеці України.

За допомогою вищенаведених соціальних мереж спецслужби рф здійснюють розвідку в мережі Інтернет. Open source intelligence (OSINT) – розвідка на основі аналізу відкритих джерел інформації) – одна з форм процесу організації та управління збором розвідувальних даних (Intelligence Collection Management), що включає їх пошук і відбір із публічних загальнодоступних джерел, добування та аналіз інформації, формування розвідувального документу для прийняття відповідного рішення [8, 7].

При використанні сервісу «Чат рулетки» (навіть при застосуванні мереж, захищених засобами VPN), ворог отримує в своє розпорядження IP-адресу користувача, дані про фактичне місце перебування суб'єкта та номер телефону який використовується для підключення до мережі Інтернет. За номером телефону підтягуються й персональні дані суб'єкта, які раніше були розміщені у соціальні мережі «ВКонтакті».

На веб-сайті «Чат рулетка» працюють невеликі групи висококласних політтехнологів, спічрайтерів та іміджмейкерів (як за приклад можна взяти «блогера» Артема Кузьмина, який поширює СІО за допомогою популярного відеохостингу youtube.com), що створюють і обігрують заданий сценарій. Групи відповідних фахівців спецслужб рф виконують СІО, підключаючись до чатів з українцями, надаючи їм персональні дані жертви, демонструючи з екрану телефону їх особисті фотографії (колись завантажені у соціальну мережу «ВКонтакті»). Такі СІО спрямовані на дестабілізацію психологічного стану українців, створення емоцій страху,

зниження бойового духу військових, та як наслідок — зниження бажань воювати чи протистояти загарбникам.

Загроза національній безпеці України полягає не лише в тому, що такий великий об'єм особистої інформації добровільно надається ворогові громадянами України. Основну загрозу становить підключення до сервісу «Чат рулетки» військовослужбовців Збройних Сил України (далі – ЗСУ) та інших підрозділів Сил оборони України, які в цей момент перебувають на бойових позиціях або в інших місцях дислокації військових та скупчення бойової техніки. На жаль така ситуація нерідко зустрічається на просторах даного веб-сайту.

Таким чином ворогом збирається таємна інформація про місця розташування підрозділів Сил оборони України, яка використовується для подальшого ураження наших позицій.

Вважаємо за необхідне додатково розробити та видати відповідний Наказ Генерального штабу Збройних Сил України, який передбачатиме сувору заборону військовослужбовцям підрозділів Сил оборони України підключення до російських веб-сайтів, зокрема до chatroulette.com, з метою забезпечення національної інформаційної безпеки України.

Список використаних джерел:

1. Електронна енциклопедія Wikipedia. Україномовна версія [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/VK.

2. Електронна енциклопедія Wikipedia. Україномовна версія [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Chatroulette.com.

3. Указ Президента України № 133/2017 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)».

4. Указ Президента України № 184/2020 «Про рішення Ради національної безпеки і оборони України від 14 травня 2020 року «Про застосування, скасування і внесення змін до персональних спеціальних економічних та інших обмежувальних заходів (санкцій)».

5. Т. Гроув Київ бачить ризики в російських соціальних мережах / Т. Гроув // The Wall Street Journal. — 2017. — трав. – Режим доступу: https://www.wsj.com/articles/russian-social-media-seen-as-threat-to-ukraine-and-to-cybersecurity-1496055606.

6. Joint publication: 3-13. Information operation, 2006 [Електронний ресурс]. – Режим доступу : http://www.acqnotes.com/Attachments/Joint%20Publication%203-13%20Information%20Operations%2013%20Feb%2006.pdf.

7. Електронна енциклопедія Wikipedia. Англомовна версія [Електронний ресурс]. – Режим доступу: http://en.wikipedia.org/wiki/Open-source_intelligence.

8. Електронна енциклопедія Wikipedia. Англомовна версія [Електронний ресурс]. – Режим доступу: http://en.wikipedia.org/ wiki/ Intelligence_collection_management.

9. Указ Президента України № 56/2022 «Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки».

10. Указ Президента України № 447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України».

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

СИСТЕМНІ ОСНОВИ РЕГУЛЮВАННЯ СОЦІАЛЬНО-ПРАВОВИХ ВІДНОСИН В ДИНАМІЧНИХ УМОВАХ РОЗВИТКУ ЕЛЕКТРОННОГО УРЯДУВАННЯ

Успішний розвиток суспільства визначається гармонійними та раціональними відносинами між окремими його суб'єктами, які в цілому можуть бути визначені як соціальні структури. Під соціальними структурами в цьому випадку слід розуміти сукупність соціальних трудових колективів, соціально – демографічних угрупувань, територіальних поєднань й етнічних спільнот, пов'язаних між собою відносно сталими стосунками. Останнього часу роль соціальних структур [1] в процесах розвитку управління господарством країни розширюється з точки зору практичного використання – визначаються їх види, типи та кластери, формуються відповідні чинники для їх класифікації. З іншого боку формування соціально – правових відносин в рамках системного підходу до моделювання процесів їх функціонування між соціальними структурами дає можливість інтегрува-

ти виділені специфічні підсистеми в загальну систему законодавства країни.

Тоді відносини між виділеними соціальними структурами можливо визначити в опису відповідної системи, в якій окремі соціальні структури виступають в якості специфічних підсистем. В залежності від критерію опису системи взаємодії між соціальними структурами можливо побудувати специфічні графи за різними критеріями пріоритетності – за господарчими відносинами, регіональним підпорядкуванням та інше [2]. Але в будь – якому разі відносини між елементами системи, тобто соціальними структурами, регулюються певними нормативно – правовими відносинами. Тому виникає задача розробки теоретичних основ функціонування системи динамічного розвитку соціальних структур в умовах раціонального правового забезпечення їх діяльності.

Для успішного функціонування та динамічного розвитку системи регулювання соціально – правових відносин необхідно вирішення нових задач та удосконалення на їх основі принципів як власної надійної роботи окремих соціальних структур, так і міжструктурної взаємодії з іншими структурами, тобто виділеними елементами окресленої системи.

В такому разі першою задачею є визначення раціональної структури правових документів, що відповідають найкращим умовам діяльності окремих соціальних структур, коли коло правових документів інших сполучених структур виступають як обмеження та крайові умови. При цьому першочергова увага приділяється збереженню принципів функціонування соціальних структур держави в умовах розвитку процесів правового управління в умовах електронного урядування.

Далі в процесах проектування системи регулювання соціально – правових відносин в умовах електронного урядування [3] створюються блоки міжструктурних досліджень зв'язків у використанні нормативно – правових документів. Такі дослідження у будь – якому випадку базуються на даних накопиченої інформації про використання нормативно – правових документів, а банки даних такої інформації базуються на обробці документів за лексико – графічними підходами. Мета таких досліджень перш за все полягає у формуванні шляхів швидкого електронного доступу до необхідних нормативно – правових документів за глобальним критерієм діяльності чи нагальних проблемних питань певної соціальної структури до документів інших соціальних структур. Але, з іншого боку, накопичення даних про використання нормативно – правових документів, що використовуються в діяльності сполучених соціальних структур, є основою для обґрунтування деяких їх положень, змін або скасування.

Практично задача про дослідження міжструктурного використання правових документів для окремих соціальних структур розповсюджується на реалізацію загального підходу до обґрунтування доцільності створення нових правових документів (законів, державних стандартів, галузевих нормативів та ін.), що відповідають динамічним умовам розвитку цієї соціальної структури, як елемента всієї системи, чи регулювання (пристосування) вже існуючих документів до поточних умов. В цьому випадку вивчаються потоки інформаційного обміну користування правовими та нормативними документами в рамках всієї системи регулювання соціально – правовими відносинами країни. Реалізація такої задачі здійснюється із використанням теорії графів, яка визначає правила побудови графів відносин що – до використання нормативних документів між окремими соціальними структурами та методів сітьового моделювання, які дають змогу визначити критичні (напружені, тобто найбільш інтенсивні) шляхи використання окремих нормативно – правових документів. Такий підхід дає змогу визначити ряд важливих параметрів певної структури системи регулювання нормативно – правових відносин, наприклад, час доступу до корисної інформації та витрати ресурсів для цього.

Проектування складеної за певним критерієм системи електронного урядування для підтримання раціонального функціонування правових відносин в діяльності соціальних структур базується на принципах побудови можливого використання та оцінки ефективності нормативно – правових документів, які використовуються і для проектування парних соціальних структур. Звичайно, функціонування такої розгалуженої інформаційно – нормативної системи вимагає попереднього опрацювання та створення відповідних документів, наприклад, ідентифікаторів правових документів, розробки критеріїв оцінки ефективності використання документів. В цілому система регулювання соціально – правових відносин в рамках електронного урядування уявляє собою досить складну структуру, а тому її проектування та подальший розвиток можливий в рамках певного критеріального обмеження. Наприклад, це може бути галузева підсистема, підсистема надання певних соціальних послуг, підсистема міжнародної співпраці в рамках певних двомовностей та ін.

В цілому розвиток підходу до регулювання соціально – правових відносин на основі принципів системного моделювання відносин між соціальними структурами суспільства дозволяє вирішити ряд нагальних задач, а саме:

– визначити раціональну структуру правових документів, що відповідають найкращим умовам функціонування окремих соціальних структур;

– бгрунтувати механізм реорганізації системи правових документів в динамічних умовах розвитку соціальних відносин суспільства та електронного урядування;
– підвищити надійність та практичну цінність правових документів, а також оперативність їх використання, а також інші задачі.

Список використаних джерел:

1. Прокопенко Т. О. Теорія систем та прийняття управлінських рішень : Черкас. держ. технол. ун-т. – Черкаси : ЧДТУ, 2018. – 187 с

2. Козловець М. А. Соціальна структура українського суспільства в контексті постсоціалістичних трансформацій. «Вісник НЮУ імені Ярослава Мудрого». Серія: Філософія, філософія права, політологія, соціологія, 4(35), 41–57. https://doi.org/10.21564/2075-7190.35.119623

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

НАУКОВЕ ВИДАННЯ

СОЦІАЛЬНА І ЦИФРОВА ТРАНСФОРМАЦІЯ: ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ

МАТЕРІАЛИ
II ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

КИЇВ, 25 ЛИСТОПАДА 2022 РОКУ

Науковий керівник конференції
О. А. Баранов

Упорядники:
В. М. Фурашев, С. О. Дорогих, М. В. Дубняк

Підписано до друку 29.12.2022.
Формат 60x84/16. Ум-друк. арк. 6,28.
Наклад 100 прим. Зам. № 2212-13.

Видавець ПП «Фенікс»
(Свідоцтво суб'єкта видавничої справи ДК № 1044 від 17.09.02).
Україна, м. Одеса, 65009, вул. Зоопаркова, 25.
e-mail: fenix-izd@ukr.net
www.feniksbooks.com

Виготовлювач ТОВ «7БЦ»
03067, м. Київ, вул. Олекси Тихого, 84
e-mail: 7bc@ukr.net, тел: (044) 592-00-80
Свідоцтво суб'єкта видавничої справи ДК №5329 від 11.04.2017