

Національна академія правових наук України
Науково-дослідний інститут інтелектуальної власності

**ПИТАННЯ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ**

Збірник наукових праць

**ІНТЕЛЕКТУАЛЬНА ВЛАСНІСТЬ
В ЦИФРОВІЙ ЕКОНОМІЦІ**

Випуск вісімнадцятий

**Київ
Інтерсервіс
2021**

*Рекомендовано вченою радою Науково-дослідного
інституту інтелектуальної власності НАПрН України
(протокол № 11 від 15 грудня 2020 р.)*

Р е д а к ц і й н а к о л е г і я :

О. П. Орлюк, доктор юридичних наук, професор, академік НАПрН України (*голова редколегії*); **О. Б. Бутнік-Сіверський**, доктор економічних наук, професор, академік АТН України, академік УАН (*головний редактор з економічних наук*); **О. Ф. Дорошенко**, кандидат юридичних наук (*відповідальний секретар*); **Г. О. Андросюк**, кандидат економічних наук, доцент, **Ю. Е. Атаманова**, доктор юридичних наук; **М. К. Гальянич**, доктор юридичних наук, професор, член-кореспондент НАПрН України, **К. О. Горська**, доктор наук з соціальних комунікацій; **В. С. Дроб'язко**, кандидат філологічних наук; **Н. М. Мироненко**, доктор юридичних наук, професор, член-кореспондент НАПрН України; **А. С. Штефан**, доктор юридичних наук

ПЗ5 Питання інтелектуальної власності : зб. наук. праць /
за ред. к.е.н. Г. О. Андросюка; НДІ ІВ НАПрН України.
Випуск 18. К. : Інтерсервіс, 2021. 168 с.

ISBN 978-966-999-133-1

Збірник присвячено організаційно-правовим та економічним аспектам інтелектуальної власності в цифровій економіці. Наукові статті, що увійшли до збірника, відображають відповідні напрацювання фахівців НДІ інтелектуальної власності, отриманих за результатами досліджень, проведених у 2020 році та круглого столу «Legal Tech (юридичні технології) в інтелектуальній власності : стан та тенденції», проведеного 10 грудня 2020 року.

Для науковців, аспірантів і практичних працівників сфери інтелектуальної власності.

УДК 347.(77+78)

Друкується в авторській редакції

*Відповідальність за зміст матеріалів несуть їх автори.
Редакційна колегія не завжди поділяє
точку зору авторів*

ISBN 978-966-999-133-1

© Науково-дослідний інститут інтелектуальної
власності НАПрН України, 2021
© Колектив авторів, 2021

ЗМІСТ

Від редакційної колегії	5
Бутнік-Сіверський О. Б., Андрощук Г. О. Цифрова економіка — оподаткування електронних послуг: зарубіжний досвід та стан в Україні	8
Андрощук Г. О. Система забезпечення цифрових доказів існування інтелектуальних активів: WIPO PROOF	25
Андрощук Г. О., Работягова Л. І. Винаходи, реалізовані на комп'ютері: керівні принципи і практика ЄПВ	33
Арсирій А. Системи електронного правосуддя: запровадження проєкту «Електронний суд»	47
Бакурова А. В., Пасічник М. С., Терещенко Е. В., Філей Ю. В. Продукційна модель прийняття рішень на прикладі призначення судом покарання за крадіжку	53
Бочарова Н. В. Проблема гуманізації інтелектуальної власності в умовах інформаційного суспільства	64
Буров О. Ю. Кібербезпека в мережах прийняття рішень: стан і тенденції (досвід США)	72
Васильєв О. В., Чьочь В. В. Тенденції розвитку патентно-інформаційних систем для забезпечення патентних досліджень	82
Кваша Т. К., Андрощук Г. О. Патентний ландшафт як інструмент аналітики інтелектуальної власності (на прикладі аналізу сфери військових технологій)	94
Кислий Т. Ф. Legal Tech проти кіберсквотингу: міжнародний досвід та українські реалії доменних спорів	106

Коноваленко В. В.

Електронна система підтримки прийняття рішень
«Knowledge to royalty converter»: від послуг до роялті 120

Лавренчук Т. М.

Електронні докази: трансформація методів та способів
доказування обставин у ході судового процесу 126

Логвиненко М. І., Диковець А. В.

Захист об'єктів авторського права
за допомогою технології BLOCKCHAIN 134

Сердюк О. В.

MisterRegister-патентний повірений у смартфоні: онлайн
сервіс для пошуку, моніторингу та реєстрації торгових марок 138

Фонарьова Т. А., Петренко В. О., Бушуєв К. М.,

Нейронні мережі в інформаційно-технологічному
обслуговуванні юридичної діяльності 145

Троцька В. М.

Інтелектуальний аналіз тексту та даних в умовах формування
Єдиного цифрового ринку: правові аспекти 157

Від редакційної колегії

В останні роки однією з головних тенденцій розвитку економіки і суспільства є проникнення інформаційних технологій у різні сфери діяльності людини. Інформатизація стає настільки важливим фактором зростання продуктивності праці і підвищення якості життя, що зміни, які відбуваються, розглядаються дослідниками як настання нової ери економічного розвитку, який в літературі характеризується терміном «цифрова, або інформаційна економіка». Нині розвиток інформатизації пов'язаний насамперед із впровадженням цифрових комунікаційних технологій і платформ, для яких Інтернет і мобільні пристрої є основою. Сектори економіки, засновані на інформаційних і комунікативних технологіях, отримали назву «цифрова економіка». Сам термін «цифрова економіка» «Digital Economy» (інколи — електронна економіка) з'явився в 1995 р. одночасно у канадського професора менеджменту Д. Топскотта з Університету Торонто (його праця оприлюднена в 1997 р.) та американського інформатика Н. Неропонте і швидко набув поширення, витіснивши на периферію економічної науки поняття: «New Economy», «Web Economy», «Internet Economy», «Network Economy» і надавши цьому терміну більш конкретний зміст. Отже, цифрова економіка — це економіка, що базується на цифрових комп'ютерних технологіях та інформаційно-комунікативних технологіях (ІКТ), але, на відміну від інформатизації, цифрова трансформація не обмежується впровадженням інформаційних технологій, а докорінно перетворює сфери і бізнес-процеси на базі Інтернету та нових цифрових технологій. Цифрова економіка, як головна прикмета сучасності, зачіпає всі сфери життя суспільства. Як тренд розвитку світової економіки і суспільства цифровізація активно впливає на різні сфери. А від ступеня впливу цифровізації на національне економічне та соціальне життя залежить місце кожної країни у світовому співтоваристві.

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, оскільки цифрова економіка має включати три основні компоненти, серед яких підтримуюча інфраструктура (цифрова інфраструктура, апаратне та програмне забезпечення, телекомунікації та мережі), *e-business* (ведення господарської діяльності та будь-яких інших процесів

через комп'ютерні мережі) та *e-commerce* (дистрибуція товарів через Інтернет). Ключовим і практично невичерпним ресурсом економіки давно визнана інтелектуальна власність. Сьогодні вона стає ще й основним інструментом розвитку цифрових технологій, формує самостійний, глобальний цифровий ринок, зростання якого перевищує позитивну динаміку багатьох традиційних «матеріальних» товарних ринків.

В Концепції розвитку цифрової економіки України на 2018–2020 р. зазначено, що розвиток цифрової економіки України полягає у створенні ринкових стимулів, мотивацій, попиту та формуванні потреб щодо використання цифрових технологій, продуктів та послуг серед українських секторів промисловості, сфер життєдіяльності, бізнесу та суспільства для їх ефективності, конкуренто-здатності та національного розвитку, зростання обсягів виробництва високотехнологічної продукції та благополуччя населення. Очікується, що в найближчі роки саме цифрова економіка стане основним джерелом росту ВВП України. Вона потребуватиме все більшої кількості фахівців різного профілю. Цифровізація економіки означає новий рівень цифрових сервісів, коли в онлайн переходять оплати комунальних платежів, через смартфон ми реєструємося в черзі, оплачуємо покупки тощо. Вона спрямовна на опанування нових цифрових технологій (електронні розрахунки і транзакції, хмарні обчислення, блокчейн, *e-government*), цифрових товарів та послуг, методів інтелектуального аналізу даних (Data Mining, Big Data, машинне навчання, штучний інтелект), а також їх застосування в управлінні, у виробництві, бізнесі, фінансових установах, електронній комерції. Особливість українського цифрового розвитку в тому, що користувачі і бізнес значно випереджають державу і промисловість. Нині малий і середній бізнес вже так чи інакше працює в Інтернеті і здебільшого використовує цифрові методи просування своїх послуг. Водночас держава і велика промисловість в Україні ще відстають і потребують суттєвого інтелектуально-інноваційного розвитку, оновлення та модернізації.

В збірнику розглянуто кращий досвід українських розробників — MisterRegister — патентний повірений у смартфоні: онлайн сервіс для пошуку, моніторингу та реєстрації торгових марок; український чат-бот Patent Bot — реєстратор торгових марок; електронна система підтримки прийняття рішень «Кно-

wledge to royalty converter»: від послуг до роялті а також широкий спектр проблемних питань цифрової економіки: керівні принципи і практика ЄПВ щодо винаходів, реалізованих на комп'ютері; проблеми оподаткування електронних послуг (зарубіжний досвід та стан в Україні); кібербезпека в мережах прийняття рішень: стан і тенденції; тенденції розвитку патентно-інформаційних систем для забезпечення патентних досліджень; роль патентного ландшафту як інструменту аналітики інтелектуальної власності (на прикладі аналізу сфери військових технологій)»; нейронні мережі в інформаційно-технологічному обслуговуванні юридичної діяльності; системи електронного правосуддя, інструменти забезпечення цифрових доказів існування інтелектуальних активів: WIPO PROOF; Legal Tech проти кіберсквотингу: міжнародний досвід та українські реалії доменних спорів; електронні докази: трансформація методів та способів доказування; інтелектуальний аналіз тексту та даних в умовах формування Єдиного цифрового ринку: правові аспекти; захист об'єктів авторського права за допомогою технології BLOCKCHAIN.

*Андрощук Г. О.,
головний науковий співробітник
НДІ інтелектуальної власності НАПрН України
канд. екон. наук, доцент*

Бутнік-Сіверський О. Б.,
головний науковий співробітник економіко-правового
відділу НДІ інтелектуальної власності НАПрН України,
доктор економічних наук, професор,
академік АТН України та академік УАН
Андрощук Г.О.,
головний науковий співробітник
НДІ інтелектуальної власності НАПрН України
кандидат економічних наук, доцент

ЦИФРОВА ЕКОНОМІКА — ОПОДАТКУВАННЯ ЕЛЕКТРОННИХ ПОСЛУГ: ЗАРУБІЖНИЙ ДОСВІД ТА СТАН В УКРАЇНІ

Розглянуто науковий напрям, яким є цифрова економіка, що базується на інформаційно-комунікаційних та цифрових технологіях і є на сьогодні початковим трендом в Україні, що набуває пріоритет в бізнесі і максимально підтримується державою. Визначено особливість українського цифрового розвитку, досліджено проблемні питання оподаткування електронних послуг у сфері цифровізації економіки. Узагальнено підходи до розв'язання проблеми оподаткування е-послуг в проектах ОЕСР та європейському законодавстві розвинених країнах світу. Розглянуто перші кроки щодо оподаткування цифрових технологій в законодавстві України.

*Цифрова економіка (англ. *Digitaleconomy*) у поширеному визначенні — це економіка, що базується на цифрових комп'ютерних технологіях. Її іноді називають *інтернет-економікою*, *новою економікою* або *веб-економікою*. Термін «цифрова економіка» ввів 1995 р. канадський бізнес-гуру Дон Тепскотт, а термін «диджитал-економіка» (*digital economy*) введений у науковий обіг у 1995 р. американським ученим Ніколасом Негропonte, який відомий як засновник медіа-лабораторії Массачусетського технологічного інституту та фундатор асоціації One Laptopper Child [1].*

У класичному розумінні, зазначено в Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки [2], поняття «цифрова економіка» означає діяльність, в якій основними засобами (факторами) виробництва є цифрові (електронні, віртуальні) дані як числові, так і текстові. Вона базується на інформаційно-комунікаційних та цифрових технологіях, стрімкий розвиток та поширення яких вже сьогодні впливають на традиційну (фізично-аналогову) економіку, трансформуючи її від такої, що споживає ресурси, до економіки, що створює ресурси. Саме дані є ключовим

ресурсом цифрової економіки, вони генеруються та забезпечують електронно-комунікаційну взаємодію завдяки функціонуванню електронно-цифрових пристроїв, засобів та систем.

Цифрова економіка стала науковим напрямом, що займається застосуванням сучасних цифрових технологій до управління економічними системами. Все частіше цифрова економіка переплітається з традиційною економікою, роблячи чітке розмежування складніших економічних систем за рівнем діяльності та функціонування (кластери, бізнес-інкубатори, центри технологій та їх трансферу тощо) та взаємозв'язку. Під цифровою економікою розуміють виробництво, продажі та постачання продуктів через комп'ютерні мережі. Це передбачає цифрове відображення різних сфер людської діяльності зі створенням при цьому з досягненням значного економічного та соціального ефектів.

Цифрова економіка є сучасним динамічним трендом, що виник у результаті останньої (4-ої) технологічної революції. Її обсяг у світі оцінюється у 4 трлн доларів [3]. Як зазначено в Концепція розвитку цифрової економіки та суспільства України на 2018–2020 р., індустрія 4.0 — оновлена концепція «розумного виробництва», що ототожнюється з «четвертою промисловою революцією» та появою кіберфізичних систем. Індустрія 4.0 — наступний етап цифровізації виробництв та промисловості, на якому головну роль відіграють такі технології та концепти, як Інтернет речей, «великі дані» (*big data*), «предиктивна аналітика», хмарні та туманні обчислення, «машинне навчання», машинна взаємодія, штучний інтелект, робототехніка, 3D-друк, доповнена реальність. Інтеграція цифрових технологій у процеси виробництва, або цифровізація промисловості, є пріоритетом державної промислової політики. Державна політика стимулювання розвитку Індустрії 4.0 має три напрями: створення інфраструктури Індустрії 4.0 — індустріальних парків, галузевих центрів технологій тощо; доступ до капіталу для створення нових інноваційних виробництв; розвиток цифрових навичок для підготовки персоналу, здатного працювати з технологіями Індустрії 4.0.

Світова цифрова економіка охоплює глобальний цифровий простір, який динамічно розвивається під впливом активної інвестиційної діяльності провідних країн світу і агресивної політики найбільших ІТ-компаній. На ринку капіталу спостерігаються структурні зрушення: зростання інвестицій в глобальні проекти на основі формування консорціумів і інтеграційних угруповань; глобальні інвестиційні потоки направляються як в технології «масового попиту» (Інтернет-ігри, електронну комерцію), так і в технології зберігання масивів баз даних; розвиток глобального і локальних цифрових

ринків створює сприятливі передумови для країн з високим рівнем освіти населення і рівня інформатизації національних економік [4].

Цифровізація економіки на сьогодні є початковим трендом в Україні та набуває пріоритет в бізнесі і максимально підтримується державою. Підтвердженням цьому є прийнята Концепція розвитку цифрової економіки на 2018–2020 роки [2], яка відтворює державну політику, у якій зазначено, що розвиток цифрової економіки України полягає у створенні ринкових стимулів, мотивацій, попиту та формуванні потреб щодо використання цифрових технологій, продуктів та послуг серед українських секторів промисловості, сфер життєдіяльності, бізнесу та суспільства для їх ефективності, конкурентоздатності та національного розвитку, зростання обсягів виробництва високотехнологічної продукції та благополуччя населення. Ця концепція передбачає здійснення заходів щодо впровадження відповідних стимулів для цифровізації економіки, суспільної та соціальної сфер, усвідомлення наявних викликів та інструментів розвитку цифрових інфраструктур, набуття громадянами цифрових компетенцій, а також визначає критичні сфери та проекти цифровізації, стимулювання внутрішнього ринку виробництва, використання та споживання цифрових технологій. Шлях до цифрової економіки пролягає через внутрішній ринок виробництва, використання та споживання інформаційно-комунікаційних та цифрових технологій.

Очікується, що в найближчі роки саме цифрова економіка буде основним джерелом росту ВВП України. Вона потребуватиме все більшої кількості фахівців різного профілю. Цифровізація економіки означає новий рівень цифрових сервісів, коли в онлайн переходять оплати комунальних платежів, через смартфон ми реєструємося в черзі, оплачуємо покупки тощо. Вона спрямовна на опанування нових цифрових технологій (електронні розрахунки і транзакції, хмарні обчислення, блокчейн, *e-government*), цифрових товарів та послуг, методів інтелектуального аналізу даних (*Data Mining*, *Big Data*, машинне навчання, штучний інтелект), а також їх застосування в управлінні, у виробництві, бізнесі, фінансових установах, електронній комерції.

Особливість українського цифрового розвитку в тому, що користувачі і бізнес значно випереджають державу і промисловість. Наш малий і середній бізнес вже так чи інакше працює в Інтернеті і здебільшого використовує цифрові методи просування своїх послуг. Але держава і велика промисловість в Україні кардинально відстали та потребують суттєвого інтелектуально-інноваційного розвитку, оновлення та модернізації.

Складність розв'язання зазначених проблем полягає у надзвичайно високому ступені динамічності й різнобічності відносин, пов'язаних з майновими правами інтелектуальної власності. Зміст цього поняття, спрощено, «інтелектуальна власність» та його структура постійно розширюються і якісно оновлюються. Відносини, що виникають у зв'язку з цим, тісно пов'язані з найновітнішими технологіями — не лише в сенсі об'єкту цих відносин, але і їх регулювання, застосування нових підходів до забезпечення прав власності.

Проблеми інтелектуальної власності у світі вийшли на перший план і стали вже не просто юридичним, а і комерційним питанням, зокрема і в новій сфері знань — цифровій економіці. Внаслідок всеосяжної інтелектуалізації сучасної економіки вони дедалі більше стають політичною проблемою, яка вимагає розробки стратегічних комплексних підходів до її вирішення, впровадження державної інноваційної політики у сфері інтелектуальної власності та відповідного державного фінансування. За цих умов, проблеми стимулювання розвитку та охорони інтелектуальної власності набуває ролі одного з найважливіших чинників усього комплексу політико-економічних відносин та економічної безпеки як всередині кожної цивілізованої країни, так і в міжнародних відносинах.

З розвитком цифровізації економіки все гостріше постає питання оподаткування електронних послуг (е-послуг) у сфері цієї діяльності. На цьому напрямку актуалізується проблема вивчення теорії та практики оподаткування е-послуг не тільки в розвинених країнах світу, а зокрема і в Україні.

З позиції зазначеного, в рамках «Плану BEPS» (англ. Action Plan on Base Erosion and Profit Shifting) більшість країн світу працюють над можливістю контролювати «цифрові» податкові злочини. Основи «Проекту BEPS» були закладені ще в 2012 р. А вже в 2013 р. ОЕСР¹ представила свій перший звіт з цієї проблематики і запропонувала так званий «План дій щодо розмивання податкової бази і виведення доходів з-під оподаткування» або скорочено: «План BEPS». Він згадується при описі агресивних схем податкового планування, застосовуючи які міжнародні групи компаній штучно виводять свої доходи з високоподаткових країн (де вони генеруються) в країни з низьким або нульовим оподаткуванням.

«Проект BEPS» розроблявся в рамках ОЕСР за активної підтримки країн G20. Суть проекту зводиться до міжнародної співпра-

¹ Організація економічного співробітництва та розвитку (скор. ОЕСР, англ. Organisation for Economic Co-operation and Development, OECD) — міжнародна економічна організація розвинених країн, що визнають принципи представницької демократії та вільної ринкової економіки.

ці в боротьбі з вищезгаданими схемами транскордонного податкового планування і до розробки комплексу рекомендацій для національних органів влади та подальшої їх імплементації в законодавство країн.

Тому, ідея тут полягає не в покаранні платників податків, а в кардинальній зміні «правил гри». У жовтні 2015 р. ОЕСР завершила фінальну розробку всіх пунктів Плану і надала підсумковий звіт, який був схвалений у листопаді 2015 р. на саміті G20 в Туреччині [5].

Досить докладно оподаткування розглянуто в статті А. Швиденко «Оподаткування е-послуг: огляд світової практики» [6], на якій доцільно далі зупинитися. Як зазначає автор, оподаткування електронних (цифрових) послуг у Європі до недавнього часу зводилося лише до податку на додану вартість (ПДВ). Так, при наданні послуг компанією фізичній особі-резиденту країни ЄС перша має отримати локальний ПДВ-номер і звітувати й оплачувати ПДВ у країні місцезнаходження споживача. У такій ситуації за дотримання певних вимог підприємство мало б реєструватись для цілей оподаткування податком на додану вартість у кожній країні, в якій є споживачі його е-послуг. При цьому корпоративний податок на прибуток оплачувався компанією за місцем її реєстрації.

Поява системи MOSS (Mino One Stop Shop) у 2015 р. значно полегшила життя бізнесу в розрізі звітування і оплати ПДВ, оскільки за допомогою цієї системи не потрібно отримувати локальні ПДВ-номери в кожній країні ЄС, куди постачаються е-послуги. Досить зареєструватись у системі і надати інформацію про кількість і суму продажу своїх е-послуг у кожній країні ЄС, а вже далі система сама передає дані та оплату ПДВ у кожену країну, де виник цей податок.

У статті М. Тащи «Оподаткування digital: Який шлях обере Україна» [7] зазначено, що у листопаді 2017 р. ідея цифрового оподаткування знову стала першою на порядку дня ОЕСР. У США протягом шести годин проводилася публічна консультація: «Як боротися з Інтернет викликами для цілей оподаткування». Місяцем раніше, у вересні 2017 р., на зустрічі міністрів фінансів країн-членів Європейського Союзу в Таллінні, Франція і Німеччина виступили з ініціативою зобов'язати Інтернет-продавців платити податки не в країнах своєї реєстрації, а там, де такі підприємці отримують фактичне винагороду. Головними «неплатниками податків» були оголошені Google і Facebook. Сама ідея про місце сплати податків уже не перший рік обговорюється в ЄС і не тільки. Чого вартий хоча б один з гучних судових розглядів Італії щодо сайту Amazon на сотні мільйонів доларів нібито несплачених компанією податків в Італії. Ідея не була підтримана всіма державами. Так,

Люксембург та Ірландія виступили проти, хоча вони і є найчастіше «податковими притулками» для цифрових Інтернет-продавців. І тепер ЄС намагається знайти компроміс між необхідністю реформування податкового законодавства Співдружності і відмовою частини країн-членів від таких реформ. Поки без помітних результатів — все проходить у форматі зустрічей і діалогів. Новатором у цьому питанні можна назвати Італію. Країна прийняла першою не тільки в ЄС, але і в світі, закон про Інтернет або так званий web податок 29 грудня 2017 р. (як подарунок під ялинку для бюджету). Запропонована ставка податку відносно невисока — всього 3 % від вартості кожної Інтернет-покупки. Італія до кінця не визначилася з суб'єктами оподаткування, але озвучила план, згідно з яким у квітні 2019 р. система збору цього податку має запрацювати. Планується, що за рік цієї роботи вийде зібрати понад 200 млн доларів США в бюджет країни. Ініціативу можна назвати викликом для компаній-гігантів Amazon, Apple, Facebook і Google.

М. Тацци зазначає, що батьківщина Google, США, також не залишилася осторонь. У відповідь Італії, або просто прийнявши реалії нового світу, Верховний Суд США 12 січня 2018 р. виніс унікальне рішення, що створило новий прецедент в історії американського податкового права. Суд вирішив, що податкова служба штату може оподатковувати продавця товарів в Інтернеті, якщо він отримав виручку в цьому штаті, навіть якщо і зареєстрований, як платник податків, в іншому штаті країни. Такий прецедент багато що змінює.

Статистичні дані показують, що щодня відправляється близько 20 млрд електронних листів, користувачі соціальних мереж посилають по 150 млн повідомлень, пошукові системи обробляють близько 650 млн запитів, а практично половина населення Європи зареєстровані в Facebook. Крім цього, зростання річного прибутку цифрових компаній за останні 7 років склало 14 %.

Розглядаючи світові тенденції, автори статті [8, 73–74] зазначили, що країни-учасниці ОЕСР* розробили і затвердили дорожню карту для вирішення проблем цифрового оподаткування і серйозного реформування національних податкових кодексів. ОЕСР закликає держави-члени цієї організації застосовувати два підходи до введення цифрового податку.

Перший підхід оподаткування, стосується цифрових компаній, що працюють безпосередньо зі споживачами їх цифрової продукції. Передбачено, що країни зможуть обкладати податком частку світового прибутку транснаціональних корпорацій, таких як Google, Facebook, Amazon, Apple, отримуюмого на території цих країн, навіть

якщо прибуток компанії виводиться за кордон. При цьому основою для розрахунку податкової ставки є оборот компанії, що генерується на території тієї держави, де вона зареєстрована. ОЕСР планує досягти глобального консенсусу і привести цифровий податок до загального знаменника до кінця 2020 р. На практиці ж пропозицію про перерозподіл прибутку в країнах, де здійснюються продажі, передбачає систему, засновану на чистому (залишковому) прибутку організацій (навіть якщо формула для розрахунку залишкового прибутку поки такі не визначена ОЕСР). При цьому існує безліч цілком законних способів мінімізації такого прибутку. Так, наприклад, відсутність чіткого взаємозв'язку між доходами і прибутком цифрової багатонаціональної компанії підтверджує приклад Amazon. У 2018 р. її прибуток склав всього \$ 10,1 млрд при \$ 232,9 млрд виторгу, отриманого в різних країнах світу, в той час як податкові збори склали всього \$ 1,2 млрд, з яких більше третини були відкладеними платіжками. Тому в якості бази оподаткування інформаційно-комунікаційні технології компаній (ІКТ-компаній) може також розглядатися не чистий прибуток, а загальний обсяг виручки [9].

Другий тип оподаткування, призначений для країн з ринковою економікою, що формується, де транснаціональні корпорації продають свої продукти і послуги, але часто не мають фізичної присутності: тому існує можливість оподатковувати діяльність з розповсюдження продуктів, припускаючи мінімальну частку прибутку, який отримано на таких ринках. В цьому випадку мінімальний оборот ІКТ-корпорації буде служити в якості бази для оподаткування. Окремо ОЕСР планує внести пропозицію щодо мінімально допустимої ставки корпоративного податку.

До основного проекту ОЕСР з протидії розмивання бази оподаткування та виведення прибутку з-під оподаткування (англ. Base Erosion and Profit Shifting, BEPS) приєдналися 137 країн [10]. Урядом цих країн належить обкладати ІКТ-гігантів податком з прибутку від цифрових операцій, наданих в країнах, де вони генерують прибуток. Основна мета BEPS — ліквідувати найпоширеніші міжнародні схеми т. зв. подвійного неоподаткування, протидіючи штучному зниженню податків або узаконеного ухилення компаній від податків (наприклад, за допомогою перенесення джерела прибутку в низько податкової юрисдикції).

В подальшому у 2018 р. [6] Європейська комісія внесла на розгляд директиву № 2018/0072, яка визначає, на що, на нашу думку, слід звернути увагу:

Об'єкти: реклама, розміщена на цифрових інтерфейсах; передача даних про користувачів, які були зібрані під час взаємодії кори-

стувачів та розміщеної реклами; надання доступу користувачам до багатостороннього цифрового інтерфейсу, за допомогою якого користувачі можуть знаходити інших користувачів та взаємодіяти з ними, а також у т. ч. ті інтерфейси, які сприяють наданню послуг або постачанню товарів між користувачами.

Суб'єкти: компанія, яка підпадає під такі два критерії:

- а) світовий дохід за останній фінансовий рік перевищує 750 млн євро;
- б) з них дохід компанії всередині ЄС за відповідний фінансовий рік перевищує 50 млн євро.

Місце оподаткування та ставка: цифрові послуги оподатковуються за місцем знаходження користувача по єдиній для всіх країн-членів ЄС ставці 3 %.

Зважаючи на те, що країни-учасниці не дійшли консенсусу, і директива досі не прийнята [6], ряд країн вирішили запровадити оподаткування цифрових послуг в односторонньому режимі, практика яких пропонується до розгляду:

Франція. У липні 2019 р. Франція прийняла закон «за мотива-ми» згаданої вище директиви. Суб'єктами оподаткування є компанії та групи компаній, світовий дохід яких перевищує 750 млн євро, з них 25 млн євро — з джерелом походження у Франції. Об'єктом оподаткування є послуги, аналогічні тим, які визначаються директивою, і ставка податку становить ті ж 3 %. Однак агресивна, проте цілком логічна відповідь США на прийняття цього закону та погрози підвищити мито на певні товари з Франції мали наслідком згоду уряду Франції відкласти оплату податку на кінець 2020 р.

Туреччина. Відповідно до Закону № 7194, починаючи з березня 2020 р. Туреччина оподатковує цифрові послуги, надані на її території, за податковою ставкою 7,5 %. При цьому президент має право збільшувати або зменшувати ставку в межах від 1 % до 15 %. Об'єктами оподаткування Туреччина визначила цифрові рекламні послуги, в т. ч. передачу даних щодо користувачів; продаж звукового, візуального та цифрового контенту, включаючи продаж через цифрову платформу ігор, музики тощо; надання послуг щодо прослуховування, перегляду, відтворення, записування електронними приладами; а також послуги надання цифрової платформи, що сприяє взаємодії між користувачами та продажу товарів і послуг між ними. Суб'єктами оподаткування є компанії, світовий дохід яких становить більш ніж 750 млн євро, а дохід з джерелом походження на території Туреччини — більше 20 млн турецьких лір.

Австрія. Починаючи з 1 січня 2020 р., Австрія запровадила оподаткування цифрових послуг, наданих на її території. Місце надання послуг визначається IP адресою та іншими технологіями для ви-

значення геолокації. Послуги онлайн — рекламування визначаються як реклама, розміщена на цифровому інтерфейсі, в т. ч. рекламні банери, реклама, розміщена в пошукових системах, та подібні рекламні послуги. Для того, щоб бути суб'єктом оподаткування цим податком, необхідно, щоб світовий дохід підприємства перевищував 750 млн євро, а місцеві (на території Австрії) продажі становили дохід не менш як 25 млн євро. Ставка податку становить 5 %.

Великобританія. Великобританія запровадила податок на цифрові послуги (ставка 2 %), і оподатковуватись буде цифровий дохід підприємств з джерелом походження у Великобританії, отриманий, починаючи з 1 квітня 2020 р. Під оподаткування підпадають підприємства, світовий дохід яких становить понад 500 млн фунтів, з яких більше 25 млн отримані від користувачів Великобританії.

Практика інших країн. Ряд інших країн ЄС запровадили оподаткування цифрових послуг — Угорщина, Італія, Польща. Готовність та зацікавленість у введенні податку на цифрові послуги виявили також Бельгія, Чехія, Латвія, Норвегія, Словаччина, Словенія, Іспанія.

Нижче, для узагальнення, розглянемо світовий досвід реалізації процедур податкового адміністрування шляхом введення цифрового податку (таблиця 1) [8, 76].

У 2020 році, зазначають автори статті [8, 77], був введений податок на хмарні та інші цифрові послуги зарубіжних компаній і затверджені відповідні законопроекти в Узбекистані, Таїланді — країнах Азії, які мають намір збільшити податкові надходження за рахунок прибутку міжнародних ІКТ-компаній. У Республіці Узбекистан ставка ПДВ встановлена в розмірі 15 %. За підсумками першого кварталу 2020 р. Google LLC сплатила до бюджету республіки 85 тис. євро. На Філіппінах аналогічний законопроект був внесений до парламенту. Передбачається, що іноземні юридичні особи, які реалізують товари і послуги в електронній формі на території країни, будуть обкладатися цифровим ПДВ. Цифрову податкову реформу на національному рівні готові потримати також Канада, КНР, Республіка Колумбія, Ізраїль та інші країни. Як правило, в цих країнах податком обкладається прибуток ІКТ-компаній від трьох основних видів послуг: послуги цифрових платформ і маркетплейсів; онлайн-реклама, таргетована на користувачів в конкретній країні; продаж даних, отриманих на основі наданої користувачем інформації. Звичайно, левова частка прибутку йде від електронної торгівлі. Внаслідок бурхливого розвитку цифрової економіки в світі на сьогодні є величезна маса неврахованих доходів. В Інтернеті продається буквально все — від продуктів харчування до автомобілів. Весь цей оборот торгівлі, що обчислюється в

масштабах планети трильйонами доларів США, або взагалі не обкладений податками, або на відміну від звичайної стаціонарної торгівлі, обкладений податками в недостатній мірі.

На сьогодні, зазначають автори статті [8, 77], потенційні втрати доходів державних бюджетів від несплати або часткової сплати корпоративного податку економісти МВФ оцінюють в \$ 650 млрд на рік. Найбільшими у світі «ухильниками» від сплати цифрового податку вважаються американські компанії Apple, Facebook, Google, YouTube, Amazon, істотно недоплачують цифровий податок також китайські Alibaba, Aliexpress та інші подібні компанії.

Таким чином, підсумовують автори статті [8, 78], незважаючи на зусилля ООН, ОЕСР, ЄС та багатьох країн світу, єдиний підхід до оподаткування суб'єктів цифрової економіки поки не вироблений. Основними проблемами, з якими зіткнулися країни, що прийняли цифровий податок на законодавчому рівні, є такі:

- а) відсутність законодавчого визначення «цифрового податку»;
- б) нездатність всеохопно реалізувати контроль прибутку, одержуваного у сфері електронної торгівлі (особливо здійснюваної через анонімні платіжні системи), в зв'язку з чим можливості ІКТ-компаній для ухилення від цифрового податку є безмежними;
- в) переважання нематеріальних активів над матеріальними і їх транснаціональна мобільність створюють додаткові бар'єри;
- г) вирішені питання перегляду національних податкових законодавств і угод про уникнення подвійного оподаткування для виключення подвійного оподаткування ІКТ-компаній;
- д) і нарешті, витік і, як наслідок, брак інформації про обсяги цифрових товарів послуг, що надаються і одержуваних іноземними компаніями.

Найголовнішою складністю у введенні цифрового податку, зазначають автори статті [8, 78], є чітке обґрунтування розрахунку прибутку транснаціональної ІКТ-компанії, одержуваного в конкретній країні. Однак з появою технічних можливостей здійснення моніторингу отримання ІКТ-компаніями по всьому ланцюжку доданої вартості цифровий податок не тільки стане справжньою революцією в оподаткуванні, а й сприятиме подальшому науково-технічному прогресу.

Таблиця 1

Заходи щодо цифрового оподаткування, вжиті країнами
Країна

Країна	Вжиті заходи	Дата початку реалізації заходів	Стадія	Надходження до бюджету від цифрового оподаткування
Австрія	5 %-податок на доходи від інтернет-реклами	Січень 2019	Запропоновано	30 млн євро
Франція	3 %-податок з обороту цифрових компаній	Квітень 2020	Запропоновано	500 млн євро
Греція	2 %-податок на рекламні послуги та послуги про-вання + 2 % на вартість електронних пристроїв	2019	Законодавчо закріплено	
Угорщина	7,5 %-податок на виручку від реклами	2014	Законодавчо закріплено	
Італія	3 %-податок на е-е-послуги	Січень 2021	Законодавчо закріплено	
Нідерланди	Утримання податку на Дивіденди і виплати роялті дочірнім компаніям	2020/2021	Запропоновано	
Нова Зеландія	3 %-податок з обороту деяких цифрових компаній	2020	Запропоновано	18–47 млн євро
Іспанія	3 %-податок з обороту цифрових компаній	2019	Запропоновано	1,2 млрд євро
Турція	15 %-прибутковий податок з платежів, здійснюваних за транскордонні послуги онлайн-реклами	2019	Законодавчо закріплено	
Великобританія	2 %-податок на цифрові послуги з внутрішніх доходів постачальників цифрових послуг	Квітень 2020	Законодавчо закріплено	443 млн євро
Європейський Союз	3 %-ставка податку з обороту цифрових компаній	2018	Запропоновано	5 млрд євро

Джерело: складено на основі даних ОЕСР. Інформація станом на січень 2020 р.

Що стосується оподаткування в цифровій економіці, то Україна хоч і з запізненням, все ж намагається не відставати від європейського законодавства. 19 грудня 2019 р. до Верховної Ради України внесено законопроект № 2634 щодо оподаткування ПДВ електронних послуг, що постачаються нерезидентами без постійного представництва (далі — нерезидент) фізичним особам на території України. Метою проекту є приведення окремих норм Податкового кодексу України у відповідність до принципів Директиви Ради 2006/112/ЄС «про спільну систему податку на додану вартість» що передбачено ст. 353 Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. Метою проекту є також приведення деяких положень Податкового кодексу України у відповідність до принципу зазначеного у пп. 4.1.8 п. 4.1. ст. 4, а саме принципу нейтральності податкового законодавства, де установлення податків та зборів не повинне впливати на збільшення або зменшення конкурентоздатності платника податків. Він передбачає внесення змін до Податкового кодексу України щодо оподаткування ПДВ е-послуг, що надаються нерезидентами фізичним особам-резидентам України. Зокрема, пропонується: визначити перелік е-послуг; включити нерезидентів до переліку осіб, які реєструються платниками ПДВ; встановити правила визначення місця постачання е-послуг (B2C); встановити форму та визначено порядок надсилання податкового повідомлення нерезиденту та скарги на таке рішення; визначити спрощену процедуру реєстрації платника ПДВ для постачальників-нерезидентів, яка може здійснюватися віддалено в електронній формі на спеціально розробленому веб-порталі; визначити правила податкового обліку з податку на додану вартість для нерезидентів, що надають фізичним особам е-послуги, місце постачання яких розташовано на митній території України; звільнення від обов'язку нерезидента реєструвати податкові накладні; передбачити сплату податкового зобов'язання для нерезидента в іноземній валюті.

Електронними послугами запропоновано вважати послуги, які постачаються через Інтернет, автоматизовано, за допомогою інформаційних технологій та переважно без втручання людини. До визначення додається невичерпний перелік таких послуг, серед яких, зокрема, постачання зображень, фотографій, текстів тощо; постачання аудіовізуальних творів, відео на замовлення; доступ до інформаційних, освітніх, розважальних ресурсів; надання у користування хмарних технологій для розміщення даних; надання рекламних послуг в Інтернеті тощо.

Наразі більшість е-послуг, що постачаються компаніями-нерезидентами фізичним особам, фактично не оподатковуються податком на додану вартість: згідно законодавства, обов'язок сплати ПДВ покладається на споживача цих послуг у разі, якщо він є платником ПДВ або суб'єктом господарювання. Варто зазначити, що значна кількість е-послуг надаються споживачам-фізичним особам (які не є суб'єктами господарювання). Відсутність оподаткування таких послуг має наслідком розвиток неконкурентного середовища порівняно з вітчизняними постачальниками е-послуг (оскільки вони зобов'язані сплачувати ПДВ на такі послуги), призводить до ненадходження податків у бюджет країни.

У пояснювальній записці до згаданого проекту закону зазначається, що схожий досвід оподаткування таких послуг вже має місце в інших країнах, наприклад, у Європейському Союзі за допомогою системи мультиопераційного обстеження (MOSS, Mini One-Stop Shop), де компанії-резиденти/нерезиденти ЄС зобов'язані сплачувати ПДВ за місцем знаходження споживача наданих послуг.

Зважаючи на особливості запропонованого законопроекту, варто відзначити, що його положеннями пропонується впровадження в Україні європейського досвіду з оподаткування ПДВ е-послуг, наданих фізичним особам. Тобто цей законопроект не має відношення до спроб запровадження додаткового оподаткування цифрових послуг податком у 3 % (за пропозицією Європейської комісії). Щодо цього питання зазначає А. Швиденко, Україна, знаходиться на декілька кроків позаду. Варто спочатку впровадити і налагодити механізм оподаткування е-послуг, наданих нерезидентами фізичним особам, а вже потім розглядати можливість введення додаткового податку на цифрові послуги (*digital sales tax*), мова про який наразі і йде в Європі.

У законопроекті пропонується оподатковувати надані нерезидентами е-послуги по ставці 20 % від бази оподаткування, які включаються до ціни електронних послуг. Тобто, справедливо, у разі прийняття проекту Закону після того, як він вступить у дію, споживачам варто очікувати підвищення цін на е-послуги на 20 %.

Подорожчання на 20 % (ПДВ), зазначає у своїй електронній петиції Качановський Я. В. (№ 22/084410-еп від 31 січня 2020 р.), можуть відбутися з будь-якими послугами, які споживач отримує через Інтернет від компаній-нерезидентів (міжнародні корпорації на кшталт Youtube, Netflix, Google, Apple, Ali Express, тощо). Аналогічне подорожчання очікується і у сфері E-commerce. Мова йде про розміщення реклами на платформах Facebook та Google, YouTube і в мобільних додатках.

У 2020 р. відсутність в Україні механізму оподаткування ПДВ електронних послуг, наданих нерезидентами свідчить про наявність ознак архаїчності в українському законодавстві. Про певні неточності законопроекту свідчить висновок Головного науково-експертного управління апарату Верховної Ради України, однак у разі їх доопрацювання прийняття закону було б позитивним зрушенням для України.

Прогнозовано, після запровадження змін Державний бюджет може недоотримати 172 млн грн на 2020 р. У свою чергу, ці втрати можуть бути компенсовані такими перевагами реалізації запропонованого проекту:

1. Розвиток нових напрямків бізнесу в сфері міжнародних електронних комунікаційних послуг — транзит міжнародного трафіку.

Транзит міжнародного трафіку передбачає встановлення, підтримку електронною комунікаційною мережею операторів з'єднання та пропуск трафіка між двома електронними комунікаційними мережами, що призведе до створення так званого міжнародного HUB трафіку в Україні. У наслідку передбачається: отримання додаткового доходу від міжнародних електронних комунікаційних послуг та отримання нових надходжень від податку на прибуток; залучення додаткових інвестицій операторів в розвиток електронних комунікаційних мереж України; збільшення надходжень валютної виручки в Україну від експорту послуг, стабілізація та підтримка курсу національної валюти; посилення експортного потенціалу України. Очікується збільшення обсягу експорту послуг.

2. Додаткові інвестиції операторів у розвиток мережі.

- надходження з ПДВ від перенаправлення зазначених сум на імпорт нового обладнання компенсують 20 % втрат ПДВ. Очікується, що сума коригування ПДВ кредиту, яка може бути перенаправлена на імпорт, складе 172 млн грн;
- розвиток мережі операторів і як наслідок покращення якості надаваних послуг за рахунок збільшення можливості реінвестицій;
- створення додаткових робочих місць підрядників, що здійснюють роботи з розбудови мережі;
- покращення доступу населення до електронних комунікаційних послуг в Україні, що поліпшить користування мобільним зв'язком. З'являється можливість додаткового збільшення 3G/4G покриття у 250 малих населених пунктах на рік;
- за рахунок розвитку мережі та покращення якості надаваних послуг прогнозоване збільшення доходів операторів електрон-

них комунікацій, а відповідно і бази оподаткування податком на прибуток у 2019 р. з врахуванням запропонованих змін складе 3 938 млн грн;

- збільшення суми до сплати в Державний бюджет податку на додану вартість складе 125 млн грн;
- збільшиться сума спеціального збору з послуг мобільного зв'язку до Пенсійного Фонду на 122 млн грн (7,5 %).

Втрати Державну бюджету складуть 172 млн грн, а загальний компенсаторний ефект для бюджету від прийняття законопроекту становитиме 247 млн грн.

Отже, чистий компенсаторний економічний ефект для бюджету складе 75 млн грн. Таким чином, будуть повністю покриті прямі втрати бюджету від запровадження законопроекту із одночасним досягненням додаткових позитивних соціальних та макроекономічних ефектів.

Висновки.

1. Цифрова економіка стала науковим напрямом, що займається застосуванням сучасних цифрових технологій до управління економічними системами. Світова цифрова економіка охоплює глобальний цифровий простір, який динамічно розвивається під впливом активної інноваційної та інвестиційної діяльності провідних країн світу і агресивної політики найбільших ІТ-компаній. Цифровий податок ЄС буде охоплювати всі основні види цифрової діяльності, яка раніше не обкладалася податком в ЄС. Завдяки прийняттю законопроектів, планується внести в економіку Євросоюзу 415 млрд євро, за рахунок чого до 2020 р. цей внесок збільшиться до 739 млрд євро (на суму, що становить 4 % від сьогоденного ВВП Євросоюзу).

Цифровізація економіки нині є динамічним трендом в Україні та набуває пріоритет в бізнесі і максимально підтримується державою. Очікується, що саме цифрова економіка в найближчі роки буде основним джерелом росту ВВП України.

2. Особливість українського цифрового розвитку в тому, що користувачі і бізнес значно випереджають державу і промисловість. Наш малий і середній бізнес вже так чи інакше працює в Інтернеті і здебільшого використовує цифрові методи просування своїх послуг. Складність розв'язання зазначених проблем в цифровій економіці України полягає у подальшому розвитку надзвичайно високого ступеню динамічності й різнобічності відносин, пов'язаних з майновими правами інтелектуальної власності.

3. Проблеми інтелектуальної власності у світі вийшли на перший план і стали вже не просто юридичним, а і комерційним питанням, зокрема і в новій сфері знань — цифровій економіці. З розвитком цифровізації економіки все гостріше постає питання оподаткування е-послуг у сфері цієї діяльності. На цьому напрямку актуалізується проблема вивчення теорії та практики оподаткування е-послуг не тільки в розвинених країнах світу, а зокрема і в Україні.

4. ОЕСР закликає держави-члени цієї організації застосовувати *два підходи* до введення цифрового податку. *Перший підхід оподаткування*, стосується цифрових компаній, що працюють безпосередньо зі споживачами їх цифрової продукції. Передбачено, що країни зможуть обкладати податком частку світового прибутку транснаціональних корпорацій. *Другий тип оподаткування*, призначений для країн, що формують ринкову економіку, де транснаціональні корпорації продають свої продукти і послуги, але не мають фізичної присутності: тому існує можливість оподатковувати діяльність з розповсюдження продуктів, припускаючи мінімальну частку прибутку, отриманого на таких ринках. Попри зусилля ООН, ОЕСР, ЄС та багатьох країн світу, єдиний підхід до оподаткування суб'єктів цифрової економіки поки не вироблений. Однак з появою технічних можливостей здійснення моніторингу отримання ІКТ-компаніями по всьому ланцюжку доданої вартості цифровий податок не тільки стане справжньою революцією в оподаткуванні, а й сприятиме подальшому науково-технічному прогресу.

5. Україна хоч і з запізненням, все ж намагається не відставати від європейського законодавства. 19 грудня 2019 р. до Верховної Ради України внесено законопроект № 2634 щодо оподаткування ПДВ е-послуг, що постачаються нерезидентами без постійного представництва фізичним особам на території України. Він передбачає внесення змін до Податкового кодексу України щодо оподаткування ПДВ е-послуг, що надаються нерезидентами фізичним особам-резидентам України.

Список використаних джерел

1. Цифрова економіка / Матеріал з Вікіпедії — вільної енциклопедії. URL: <https://uk.wikipedia.org/wiki>.

2 Концепція розвитку цифрової економіки та суспільства України на 2018–2020 роки. Розпорядження Кабінету Міністрів України від 17 січня 2018 р. № 67-р. URL: <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80>.

3. Цифрова економіка. URL: <https://web.kpi.kharkov.ua/ekmm/tsyfrova-ekonomika>.
4. Джусов О. А., Апальков С. С. Цифрова економіка: структурні зрушення на міжнародному ринку капіталу. URL: http://journals.iir.kiev.ua/index.php/ec_n/article/view/3058.
5. План BEPS: кінець епохи агресивного податкового планування. URL: <https://www.nexus.ua/plan-beps-konets-epokhi-agresivno-go-nalogo-vo-go-planirovaniya>.
6. Швиденко Анна. Оподаткування е послуг: огляд світової практики / Юридична Газета № 19 (725). URL: <https://jur-gazeta.com/publications/practice/insh/opodatkovannya-eposlug-oglyad-svitovoyi-praktiki.html>.
7. Мария Тащи. Налогообложение digital: Какой путь выберет Украина. URL: <https://delo.ua/economyandpoliticsinukraine/nalogooblozhenie-digital-338525>.
8. Тетерятников К. С., Камолов С. Г., Блашкина Д. А. Цифровой налог: поучительный зарубежный опыт / Мировая экономика. Российский экономический журнал. 2020. № 4. С. 69–87. URL: <https://mgimo.ru/upload/2020/10/cifrovoj-nalog-pouchitelnyj-zarubezhnyj-opyt.pdf>.
9. Annual report, proxiesandshareholderletter 2018 // Amazon.com, Inc. URL: <https://ir.aboutamazon.com/annual-reportsproxies-and-shareholder-letters/default.aspx> (дата звернення 23.08.2020).
10. International collaboration to end tax avoidance, OECD. URL: <https://www.oecd.org/tax/beps/> (дата звернення: 07.08.2020).

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

СИСТЕМА ЗАБЕЗПЕЧЕННЯ ЦИФРОВИХ ДОКАЗІВ ІСНУВАННЯ ІНТЕЛЕКТУАЛЬНИХ АКТИВІВ: WIPO PROOF

Qui Prior Est Tempore Potior Est Jure
Перший за часом — сильніший за правом

Сучасний етап економічного розвитку суспільства характеризується формуванням нової сфери економіки — цифрової, обумовленої збільшенням ролі цифрових технологій та електронно-інформаційних технічних засобів зв'язку в розвитку всіх головних галузей науки. Цифрові технології, що з'явилися протягом останнього десятиліття, допомагають знайти джерела підвищення ефективності та нові можливості конкурентного розвитку ринкових бізнес-структур. Водночас, вони потребують перебудови наявних бізнес-процесів, їх організаційно-правового забезпечення на підставі нових викликів, цінностей, пріоритетів і технологічних можливостей. Всесвітня організація інтелектуальної власності (ВОІВ) 27 травня 2020 р. запустила нову он-лайн бізнес-послугу WIPO PROOF, яка надає захищені докази існування (в будь-який момент часу будь-якого) цифрового файлу, включаючи набори даних, в будь-якому форматі [1]. Система WIPO PROOF (*proof* (англ.) — доказ) доповнює існуючі системи ВОІВ у сфері інтелектуальної власності (ІВ), допомагаючи творцям і новаторам здійснювати діяльність, що піддається перевірці, для захисту багатьох результатів їх роботи впродовж життєвого циклу інновації: від створення концепції до розробки та комерціалізації продукту.

«У високо динамічній глобальній економіці, де цінність все більше залежить від людської діяльності, що забезпечується цифровими технологіями і великими даними, дуже важливо мати можливість довести, що ви володіли цифровими файлами свого інтелектуального активу. WIPO PROOF допомагає новаторам і творцям краще захищати свої цифрові розробки і являє собою значний крок у розширенні набору послуг ВОІВ, що відповідають вимогам цифрової економіки» — зазначив Генеральний директор ВОІВ Френсіс Гаррі, презентуючи цю систему [1].

Поява платформи WIPO PROOF є одним із закономірних етапів процесу цифровізації світової економіки. В її основі лежить техно-

логія криптографічного шифрування і інфраструктура відкритих ключів. Остання багато в чому схожа з технологією блокчейн, але на відміну від блокчейна вже прийнята більшістю юрисдикцій. Завдяки вбудованим технологічним інноваціям, платформа WIPO PROOF дозволяє створювати цифровий відбиток файлу будь-якого формату і обсягу з відміткою дати і часу. Тобто, в перспективі стає можливим довести, що файл з певною інформацією існував в конкретний період часу і належав конкретній особі.

В даний час величезні масиви даних зберігаються в електронному вигляді: літературні твори, напрацювання дизайнерів, сценарії, музика, комп'ютерні програми, наукові праці, інноваційно-технічні розробки, дані для навчання алгоритмів штучного інтелекту, — це далеко не повний список. Згадані об'єкти інтелектуальної власності не завжди підлягають охороні, часто створюються спільно декількома особами або компаніями, можуть довго існувати у вигляді начерків, ескізів, уривків програмного коду.

Платформа WIPO PROOF забезпечує захист продуктів інтелектуальної діяльності на будь-якому етапі життєвого циклу інновації: від концепції до комерціалізації, а також дозволяє підтвердити внесок окремої людини в підсумковий результат.

Інноваційна та творча діяльність в сучасному світі, який все більше оцифровується, часто носить глобальний і спільний характер, створюючи широкий спектр файлів даних, що містять цінний контент, який може легко стати жертвою неправомірного використання або привласнення. Цей контент може варіюватися від комерційних секретів до сценаріїв, музичних партитур та інших творчих робіт, до результатів досліджень, великих наборів даних, алгоритмів штучного інтелекту (ШІ) або будь-якого ділового запису. Всі вони мають розглядатися як інтелектуальні активи і повинні бути незалежно і надійно задокументовані на кожному етапі розробки, незалежно від того, чи стануть вони в кінцевому підсумку офіційними правами ІВ. Інтелектуальні активи — це вартість інтелектуальних ресурсів, які в господарському обігу приймають форму нематеріальних активів. Це вартість об'єктів права ІВ. Українським еквівалентом англо-американського терміну «неосязні активи» (*intangible assets*) є категорія «нематеріальні активи».

Нині не існує однозначності у трактуванні цього поняття. Нематеріальні активи — сукупність елементів майна (власності) юридичної або фізичної особи: що мають корисність (цінність) для їхнього володільця; що не мають матеріального складу (оцінюється не сам об'єкт, а права на нього); що використовуються в господарській діяльності достатньо довго (звичайно більше одного року); що

мають здатність приносити дохід [2, 11]. Наведене визначення базується на світовій практиці.

В Україні сутність нематеріальних активів визначається Законом «Про оподаткування прибутку підприємств», в якому ними визнаються об'єкти інтелектуальної, в тому числі промислової власності, а також інші аналогічні права, визнані в порядку, встановленому діючим законодавством, об'єктом права власності платника податку. Основну частину (за вартістю і цінністю) нематеріальних активів становить ІВ.

WIPO PROOF надає ефективний інструмент для збору та підтвердження доказів існування цифрових файлів активу в кожен конкретний момент часу, допомагаючи знизити ризик майбутніх правових спорів, а також закладаючи основу для будь-якої можливої реєстрації формального права ІВ [3]. За лічені секунди WIPO PROOF використовує передові в галузі безпечні технології для створення всесвітньо визнаного цифрового відбитка вашого інтелектуального активу. Ваш токен WIPO PROOF — унікальний відбиток вашого цифрового файлу, датований і позначений міткою з моменту його створення. Токен (від нім. *Zeichen* — знак, символ) — компактний пристрій у вигляді USB-флешки, призначений для забезпечення інформаційної безпеки користувача, віддаленого доступу до інформації та використовується для ідентифікації його власника. Ви отримуєте свій токен, а інша копія надійно зберігається на серверах BOIB у Швейцарії. WIPO PROOF спирається на 130-річний досвід BOIB з надання безпечних і надійних послуг у сфері ІВ в усьому світі. Створюючи цифровий відбиток з відміткою дати і часу, WIPO PROOF надає свого роду послуги цифрового нотаріуса, пропонуючи надійну, економічно ефективну послугу в усьому світі. WIPO PROOF приєднується до провідних на ринку послуг у сфері ІВ: патентів, промислових зразків, торгових марок, географічних зазначень, арбітражу і посередництва. WIPO PROOF — це проста у використанні глобальна онлайн-служба, яка швидко генерує захищені від несанкціонованого доступу докази, які підтверджують, що цифровий файл існував в певний момент часу і з тих пір не змінювався. Служба створює токен WIPO PROOF, цифровий відбиток дати або часу файлу або даних, які можуть використовуватися як доказ в судовому спорі. Токени WIPO PROOF можна придбати по одному за помірну плату або у вигляді декількох токенів за зниженими цінами, дійсними протягом дворічного періоду. Токени WIPO PROOF можуть використовуватися для встановлення попереднього існування, допомагаючи запобігти зловживанню та незаконному привласненню, і можуть бути корисні для захисту інтелектуальних

(нематеріальних) активів на всіх етапах розробки від концепції до комерціалізації, незалежно від того, чи стануть вони в кінцевому підсумку формальними правами ІВ.

WIPO PROOF доповнює існуючі системи ВОІВ у сфері ІВ, надаючи ще один інструмент стратегічного глобального управління інтелектуальними активами. Система WIPO PROOF включає багато додатків: Для стратегій комерційної таємниці використання WIPO PROOF для підтвердження існування файлу або даних в певний момент часу є типом конкретної дії, яка підкреслює її цінність і демонструє, що були зроблені кроки щодо її захисту. Залежно від виду бізнесу, комерційними таємницями і ноу-хау можуть бути програмний алгоритм, формула, рецепт, виробничий процес, список клієнтів, бізнес-план або багато інших активів. Всі вони можуть бути захищені законом, але тільки якщо ви можете довести, що отримуете від них економічну цінність і що ви вжили заходів для збереження їх конфіденційності та запобігання неправомірного використання або незаконного привласнення. Проте власнику комерційної таємниці важко домагатися судової заборони або вимагати відшкодування збитків: як ви можете довести, що ви володіли комерційною таємницею і використовували її в певний момент часу, якщо ви завжди тримали її в секреті? Вирішити цю проблему можна за допомогою системи WIPO PROOF. Вона не тільки надає докази того, що ви володіли комерційною таємницею в певний момент часу, але також може перешкоджати можливій крадіжці або неправомірному використанню.

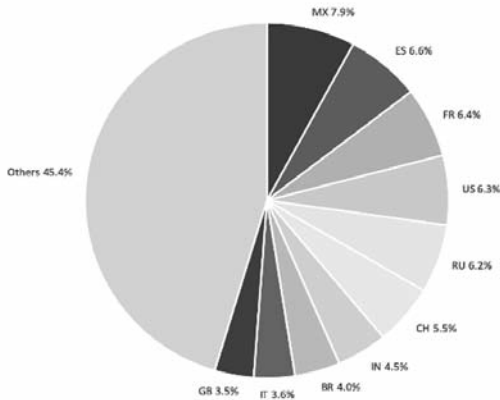
Для творчих робіт здатність доводити своє існування під час створення має основоположне значення для захисту їх від потенційного незаконного привласнення або порушення. WIPO PROOF також є корисною при управлінні цінними наборами даних, такими як дані наукових досліджень або дані для навчання моделей ШІ, оскільки існування і володіння кожною ітерацією набору даних може бути офіційно задокументовано за лічені секунди.

Як працює система доказів WIPO PROOF? Будь-який бажаючий може отримати доступ до системи WIPO PROOF — захищеного веб-сайту в Інтернеті, щоб запросити токен WIPO PROOF для конкретного цифрового файлу. ВОІВ не читає вміст файлу і не зберігає його копію. Безпечний односторонній алгоритм WIPO PROOF локально взаємодіє з браузером запитуючої сторони для створення унікального цифрового відбитка файлу. Крім того, будь-яка людина — навіть треті особи — можуть перевірити токени WIPO PROOF на веб-сайті, виконавши кілька простих кроків. WIPO PROOF використовує технологію інфраструктури відкритих ключів (PKI) для гене-

рації токенів WIPO PROOF. Технологія PKI — це усталена і надійна криптографічна технологія, яка є одним з найбільш визнаних у світі методів цифрової сертифікації. Крім того, WIPO PROOF була розроблена і створена відповідно до стандартів eIDAS, які є одними з найнадійніших у світі. Токени WIPO PROOF забезпечують найвищий рівень впевненості в тому, що дата і час на токени точні і не були підроблені. WIPO PROOF надає надійні і перевіряємі докази у разі виникнення суперечок і судових розглядів щодо існування і цілісності цифрового файлу і пов'язаних з ним прав ІВ [3].

Новітня цифрова служба ВОІВ, WIPO PROOF вже обслуговує клієнтів з 117 держав-членів. Менш ніж за 4 місяці нова послуга ВОІВ, що надає цінний доказ існування інтелектуальних активів, показала перспективне визнання інноваційним і творчим співтовариством більш ніж в 100 державах-членах. Станом на 15 вересня 2020 р. в системі WIPO PROOF зареєструвалися клієнти з 117 держав-членів. До п'ятірки країн з найбільшою кількістю користувачів WIPO PROOF входять Мексика, Швейцарія, Іспанія, Російська Федерація і Франція. При цьому клієнти з США, Індії, Італії, Бразилії та Великобританії замикають першу десятку. Причому переважна більшість завантажених файлів — це комп'ютерні програми.

Top 10 Countries with registered WIPO PROOF customers



WIPO PROOF надає простий і надійний спосіб допомоги встановити доказ існування в певний момент часу. Ця послуга доступна за ціною при початковій ціні 20 швейцарських франків за токен WIPO PROOF (це приблизно 560 грн), що дозволяє винахідникам і творцям — як приватним особам, так і підприємствам — користува-

тися послугами, підтримуваними ВОІВ, провідним світовим авторитетом в області інтелектуальної власності. Нині WIPO PROOF доступний десятима мовами: англійською, китайською, іспанською, французькою, російською, німецькою, японською, португальською, арабською та корейською [4].

ВОІВ наводить чотири фактори, що свідчать на користь застосування WIPO PROOF та унеможливають для судді не прийняти як доказ файл з платформи ВОІВ:

- 1) політичний — система у вересні 2019 р. була схвалена 190 країнами-членами ВОІВ;
- 2) технічний — спеціальна технологія відкритих ключів, що широко застосовується в різних юрисдикціях;
- 3) дата — найважливіший фактор, оскільки це та дата, яку ставить на токени платформа WIPO PROOF (за дату відповідає ВОІВ);
- 4) репутація ВОІВ як незалежного міжнародного органу у сфері інтелектуальної власності для підтвердження достовірності, конфіденційності та збереження відповідної інформації.

Створення нормативно-правової бази. Поточний розвиток технологій та ринків в Україні та світі мав своїм наслідком створення нових об'єктів цивільних прав, що існують виключно у цифровій (нематеріальній) формі, фактично перебувають у цивільному обігу та істотним чином впливають на суспільно-економічні відносини, формуючи особливий та новий ринок. Необхідним елементом нової економічної парадигми будь-якої держави стає розвинений ринок віртуальних активів. В Україні він фактично вже є сформованим та існує протягом приблизно 5 років, але знаходиться повністю поза межами правового поля держави.

Учасники ринку віртуальних активів повинні отримати можливість користуватися банківськими послугами, сплачувати податки з отриманих доходів і отримувати юридичний захист в судах при порушенні їх прав.

Також дуже важливим завданням є забезпечення захисту українських інвесторів при здійсненні інвестицій на ринку віртуальних активів.

Відтак ринок віртуальних активів потребує належного законодавчого врегулювання, яке покликане не лише надати можливість учасникам суспільних правовідносин розпоряджатись такими об'єктами, але й забезпечити баланс інтересів учасників ринку та сприяти надходженню інвестицій в Україну.

Нині в Україні повноцінному функціонуванню та подальшому розвитку ринку віртуальних активів заважає цілий ряд невирішених проблем, серед яких: відсутність правового регулювання відно-

син, що виникають у сфері обігу віртуальних активів; відсутність механізмів оподаткування доходів, отриманих від операцій з віртуальними активами; відсутність правових гарантій захисту права власності учасників ринку віртуальних активів; регулювання діяльності професійних учасників ринку віртуальних активів; відсутність механізмів контролю за обігом віртуальних активів, які можуть використовуватись з метою легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансування тероризму та фінансування розповсюдження зброї масового знищення; відсутність дієвих механізмів залучати іноземні інвестиції в високотехнологічні галузі економіки України.

У більшості юрисдикцій законодавці та органи державної влади регулюють вказані вище питання відповідно до власних цілей та з урахуванням особливостей національного законодавства. Відповідне законодавче врегулювання впроваджено у США, Німеччині, Мальті, Гібралтарі, Швейцарії, Ліхтенштейні, Естонії, Японії тощо.

Доказування є центральним інститутом цивільного процесуального права. У процесі реформування цивільного процесуального законодавства в Україні цей інститут зазнав значних змін, які мають своїм результатом зближення елементів континентальної та англосаксонської систем права, і, як наслідок, інтернаціоналізацію національних систем цивільного судочинства. Серед основних змін в інституті доказування варто згадати розширення переліку засобів доказування за рахунок виокремлення електронних доказів (п. 1 ч. 2 ст. 76 ЦПК). Віртуальні (цифрові) активи — це особливе явище, до якого досить складно застосувати правове регулювання, з точки зору речового права та майнових відносин. Вони нематеріальні і не потребують матеріалізації в реальному світі. Вони існують тільки в цифровій формі, створюються за допомогою кодування із застосуванням криптографії і можуть бути відтворені тільки за допомогою спеціальних технічних пристроїв.

Один з найскладніших викликів при розробці нормативної бази та документів щодо правового регулювання віртуального світу — це пошук консенсусу у визначенні термінологічного апарату. 28 квітня 2020 р. набув чинності Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового ураження» (№ 361-IX). Відповідно до Закону віртуальним активом є цифрове вираження вартості, яким можна торгувати у цифровому форматі або переказувати, та яке може використовуватися для платіжних або інвестиційних цілей.

Як бачимо, визначення досить широке, під нього можуть потрапити різні активи, що мають вартість. Адже для того, щоб об'єкт вважався віртуальним активом, він має відповідати трьом критеріям: наявність вартості (*value*), можливість до обігу в цифровому форматі (*transferability*) та можливість до його обміну на інші об'єкти цивільного права (*payment or investment purpose*) [5].

Відповідно до підпункту 14.1.120 пункту 14.1 статті 14 Податкового кодексу України (Кодекс) «нематеріальні активи — право власності на результати інтелектуальної діяльності, у тому числі промислової власності, а також інші аналогічні права, визнані об'єктом права власності (інтелектуальної власності) ...» Згідно зі статтею 139 Господарського кодексу України, «майном у цьому Кодексі визнається сукупність речей та інших цінностей (включаючи нематеріальні активи), які мають вартісне визначення...». Отже, нематеріальні активи відповідають критеріям віртуальних активів. У проекті Закону України «Про віртуальні активи» дається таке визначення: «віртуальний актив — особливий вид майна, який є цінністю у цифровій формі, яка створюється, обліковується та відчувається електронно. До віртуальних активів належать криптоактиви, токен-активи та інші віртуальні активи». Тобто, маємо незавершений перелік. Право власності на віртуальний актив набувається за фактом створення віртуального активу, укладення або виконання угоди про розпорядження віртуальним активом або об'єктами цивільних прав, якими забезпечений віртуальний актив, норм закону або рішенням суду.

Необхідно терміново легітимізувати цифрові активи, почавши їх введення в правове поле. Існуюче поняття «нематеріальні активи», як ми показали, не відображає нову сутність. Вже зараз видно, що зміни можуть торкнутися значної кількості нормативно-правових актів, починаючи з рівня кодексів і законів. Держава повинна прирівняти віртуальні (цифрові активи) до будь-яких інших, захистити права власності на них, врегулювати такі поняття, як купівля-продаж, обмін та дарування, спадкування, питання обліку і звітності, фіскальну політику. А в рамках міжнародної торгівлі та економічних об'єднань — питання транскордонного переміщення і недискримінаційного доступу до них. Першим кроком України в забезпеченні прав і обов'язків у частині цифрових активів міг би стати Цифровий кодекс.

Список використаних джерел

1. WIPO PROOF: WIPO Introduces New Business Service That Provides Evidence of an Intellectual Asset's Existence. URL: https://www.wipo.int/pressroom/en/articles/2020/article_0012.html.

2. Андрощук Г. О. Інтелектуальна власність у науково-технічній сфері: методи та принципи вартісної оцінки : монографія / Г. О. Андрощук, С. А. Давимука. – К. : Парламентське видавництво, 2014. – 304 с.

3. WIPO PROOF TRUSTED DIGITAL EVIDENCE FOR YOUR INTELLECTUAL ASSETS. URL: <https://wipoproof.wipo.int/wdts>.

4. WIPO's Newest Digital Service, WIPO PROOF, Already Serves Customers From 117 Member States. URL: https://www.wipo.int/wipoproof/en/news/2020/news_0003.html.

5. Микола Рехлицький Віртуальні активи: що це таке і навіщо нам їх законодавче регулювання? URL: <https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/virtualni-aktivishcho-se-take-i-navishcho-nam-yih-zakonodavcheregulyuvannya.html>.

*Андрощук Г. О.,
головний науковий співробітник
НДІ інтелектуальної власності НАПрН України
кандидат економічних наук, доцент
Работягова Л. І.,
провідний науковий співробітник НДІ
інтелектуальної власності НАПрН України*

ВИНАХОДИ, РЕАЛІЗОВАНІ НА КОМП'ЮТЕРІ: КЕРІВНІ ПРИНЦИПИ І ПРАКТИКА ЄПВ

Сучасна цифрова економіка переважно базується на інформаційно-комунікаційних технологіях (ІКТ). Комп'ютер не може працювати без програмного забезпечення. Програмне забезпечення (ПЗ) та апаратура в нинішньому інформаційному суспільстві діють спільно. Тому не дивно, що охорона ПЗ, як інтелектуальної власності, є важливою не тільки для галузі інформаційних технологій (ІТ), але і для інших галузей економіки. У реальному світі, що переживає четверту промислову революцію, важливість ПЗ залишається незаперечною. Продемонструємо це на наступних прикладах:

- США є найбільшим ринком технологій в світі, на які припадає 32 % від загальної суми, або приблизно 1,7 трлн дол. від передбачуваних витрат на ІТ, до 2020 р.;

- у 2019 р. глобальна активність у сфері злиттів і поглинань в сфері ПЗ та Інтернет — послуг досягла 206 млрд доларів США, що склало більше 3656 угод;
- за прогнозами, зайнятість розробників ПЗ з 2018 по 2028 р. виросла на 21 %, що набагато швидше, ніж в середньому по всіх професіях.
- розробник прикладного ПЗ в 2019 р. була найбільш затребуваною роботою з річною середньою зарплатою в 10 1790 доларів США і перспективою зростання на 31 % до 2024 р.
- у 2018 р. в США налічувалося 79 598 спеціалістів з ступенем бакалавра, 46 468 з ступенем магістра і 2017 кандидатів наук в галузі комп'ютерних та інформаційних наук.
- ринок ІТ стрімко зростає до 2026 р. до 3 трлн доларів США в рік; і до 2025 р. буде більш 64 млрд пристроїв ІТ, порівняно з 10 млрд. в 2018 р.;
- до 2025 р. 60 % підприємств будуть впроваджувати код у виробництво не рідше одного разу в день (порівняно з 3 % сьогодні); і до 2023 р. 30 % будуть отримувати не менше 20 % свого цифрового доходу від використання цифровими службами і додатками в цифрових екосистемах. У 2019 р. 61,8 % виданих в США патентів були «пов'язані з ПЗ» (на 21,64 % більше, ніж у 2018 р.).

Саме тому проблема винаходів, реалізованих на комп'ютері, або як ще їх називають софтверних патентів є однією з найбільш «гарячих» у світовій індустрії ІТ. Публікації, присвячені софтверним патентам, регулярно з'являються на сторінках провідних спеціалізованих ЗМІ. Проте це питання отримало не тільки внутрішньогалузевий, а й політичний резонанс — у зв'язку із законопроектами про легітимізацію винаходів, реалізованих на комп'ютері в Європі.

Винахід, реалізований на комп'ютері (Computer Implemented Inventions) — *це винахід, який включає в себе використання комп'ютера, комп'ютерної мережі або іншого програмованого пристрою, де одна або кілька функцій реалізуються повністю або частково за допомогою комп'ютерної програми.* Більш докладно ці питання розглянуто авторами в роботах [1–4].

Наскільки ж поширені такі винаходи? За оцінками експертів, патентні виплати становлять для смартфонів близько 20 % всієї вартості, що виплачується клієнтом. Як приклад варто навести всім відому компанію Google. Вона є власником більш ніж 2600 патентів у сфері ІТ. Якщо ознайомитися з останніми отриманими компанією патентами, то можна чітко проілюструвати умови отримання патенту на винахід, реалізований на комп'ютері. Умова щодо прив'язки до матеріального носія прямо вказана у назві винаходу: «Реалі-

зований комп'ютером спосіб і система вміщення в карантин інформації про місцезнаходження користувача / A computer-implemented method and system of quarantining user location information».

Історія софтверних патентів в США [2]. Поява софтверних патентів в США пов'язана з прецедентним характером американської правової системи. Тривалий час софтверні патенти в США не видавалися, що обґрунтовувалося прецедентним рішенням у справі 1853 року, згідно якого винахіднику Семюелу Морзе було відмовлено у визнанні виключного права на «використання електромагнетизму для передачі букв та інших символів на відстань» на підставі того, що закони природи і безпосереднє їх використання на практиці не можуть бути об'єктом патентування.

Водночас 1981 р. ознаменувався відходом від цієї практики. В рамках справи «Даймонд проти Дайера» (Diamond v. Diehr) [5] Верховний Суд США прийняв рішення, що допускало патентування алгоритмів, але не самих по собі, а в складі пристроїв, в яких вони використовуються. З цього моменту процес видачі софтверних патентів в США прийняв масовий, але ніяк не організований характер. Справа в тому, що визначення випадків, коли винахід містить здатний до патентування математичний алгоритм, а коли — нездатний, багато в чому залежало від суб'єктивного погляду експертів патентного відомства США і патентних повірених. У 1995 р. Патентне відомство США затвердило Керівництво для патентних експертів, в яких підсумовувалися результати судових рішень минулих років. Нарешті, в 1998 р. Апеляційний суд федерального округу прийняв рішення у справі State Street Bank & Trust проти Signature Financial Group, відповідно до якого патентоспроможними визнавалися, зокрема, алгоритми, що стосуються бізнес-методів.

Спроби легалізації софтверних патентів в Європі. Неможливість отримання софтверних патентів в Європейському Союзі пов'язана з прийняттям в кінці 1970-х рр. Європейської патентної конвенції (далі — ЄПК) і створенням Європейського патентного відомства (далі — ЄПВ). Стаття 52 ЄПК регламентує наступне:

(1) Європейські патенти видаються на винаходи у всіх областях техніки, які є новими, промислово придатними і мають винахідницький рівень.

(2) Зокрема не вважають винаходами в сенсі пункту 1:

(А) відкриття, наукові теорії та математичні методи;

(В) естетичні рішення;

(С) схеми, правила і методи виконання розумових дій, ведення ігор, і ведення бізнесу, а також програми для комп'ютерів;

(D) просте представлення інформації.

(3) Перераховані вище положення пункту 2 виключають патентоспроможність об'єктів або діяльності лише в тому випадку, якщо заявка на європейський патент або європейський патент стосуються таких об'єктів або діяльності **як таких**. (Виділено нами).

Разом з тим існує точка зору, згідно з якою патентування перерахованих об'єктів неприпустимо тільки «як таке». Якщо ж патентна формула передбачає неочевидне технічне рішення деякої технічної проблеми, то це вже є підставою для патентування. Саме на цьому тлумаченні організована діяльність ЄПВ, яке систематично видає софтверні патенти з другої половини 1990-х рр. Однак видача ЄПВ софтверних патентів не мала практично ніякого впливу на європейську індустрію ІТ, і жоден з судових розглядів, пов'язаних з визнанням софтверних патентів, не увінчався успіхом на рівні національних судів. Таким чином, незважаючи на те що механізм отримання таких патентів в Європі існує, можливість застосування виданих патентів була відсутня.

У 2002 р. Європейською комісією був запропонований проект «Пропозиції про директиву Європейського парламенту і Ради про патентоспроможність винаходів, реалізованих на комп'ютері» (Proposal for a Directive of the European Parliament and of the Council on the patentability of computer-implemented inventions), який спрямований на гармонізацію національних патентних законів і практики щодо видачі патентів на винаходи, реалізовані на комп'ютері (далі — Директива). Метою Директиви оголошувалась гармонізація законодавчої практики в сфері патентного права щодо винаходів, реалізованих на комп'ютері в загальноєвропейських масштабах і уточнення статусу таких патентів, які видаються ЄПВ. Основна новизна Директиви полягала в тому, що в ній патенти на винаходи, реалізовані на комп'ютері, вперше вводились в законодавство за допомогою чітких визначень, тоді як раніше і в Європі, і в США такі патенти видавалися на підставі небезперечних тлумачень норм закону і судових прецедентів.

Після декількох років дебатів і численних поправок до цієї Директиви, що суперечили одна одній, Директива була відхилена 6 липня 2005 р. Європейським парламентом переважною більшістю в 648 голосів проти 14. Рішення парламенту скасувати остаточний проект Директиви призвело до того, що національні закони залишилися незгодженими. При цьому національні законодавчі органи могли продовжувати приймати закони, які дозволяють видавати патенти на винаходи, реалізовані на комп'ютері, якщо вони того побажають, а національні суди могли застосовувати таке законо-

давство. Теж саме стосується ЄПВ, яке юридично не пов'язане з будь-якими Директивами ЄС, але в цілому адаптує свої правила і керівництва до законодавства ЄС. В цьому випадку ЄПВ не повинне було вносити зміни в свою практику видачі патентів на винаходи, реалізованих на комп'ютері.

Однак, в 2018 р. на веб-сайті ЄПВ була опублікована наступна редакція Керівництва ЄПВ, у якій велика увага приділялась саме патентуванню винаходів, реалізованих на комп'ютері (далі — СІ) [6–8]. Всі суттєві зміни в цих Керівних принципах стосувались головним чином розділів, які обговорювали перший бар'єр ЄПВ — технічний характер винаходу. Хоча першу перешкоду можна подолати, просто додавши присутність комп'ютера, для вирішення другої перешкоди або відповідності винаходу винахідницькому рівню було необхідно охарактеризувати винахід певною кількістю технічних ознак і визначити взаємозв'язок між цими технічними ознаками і досягнутим технічним результатом.

Ретельний аналіз того, чи є кожна заявлена ознака технічною чи ні, має важливе значення для набуття правової охорони в ЄПВ і судового захисту патенту на винахід, реалізований на комп'ютері (далі — СІ). Багато хто вважає, що цей документ може допомогти оцінювати охороноздатність таких винаходів в Патентному відомстві США. Отже, практикам, що працюють з СІ, необхідно ретельно ознайомитися з цими Керівними принципами ЄПВ, що вступили в силу з 1 листопада 2018 р. Як і в попередньому виданні, Керівні принципи включають суттєві і цінні поліпшення стосовно рекомендацій щодо охороноздатності СІ. Веб-сайт ЄПВ включає корисний html-показчик для Керівництва, включаючи розділи, присвячені винаходам, реалізованим на комп'ютері.

Зміни в Керівних принципах 2018 р. були представлені головним чином в частинах F-IV і G-VII і містять детальні рекомендації з добре зарекомендованих практик, які складаються з, так званого, підходу «двох бар'єрів»:

1. Перший бар'єр. Заявлений об'єкт повинен мати технічний характер, але формула може містити поєднання технічних і нетехнічних ознак.

2. Другий бар'єр. Всі ознаки, що характеризують технічний характер винаходу, враховуються для оцінки його винахідницького рівня, включаючи кроки математичного методу, які вносять вклад в технічний характер винаходу. Цей критерій винаходу оцінюється за допомогою добре розробленого підходу «Проблема і рішення для формул, що включають технічні і нетехнічні ознаки» (див. G-VII, 5.4), який не зазнав істотних змін.

У Керівних принципах також пояснюється, що формула в патентній заявці щодо винаходу, реалізованого на комп'ютері, може мати пункти, які стосуються:

- способу, наприклад спосіб роботи з системою обробки даних;
- пристрою або системи, наприклад система обробки даних;
- комп'ютерної програми [продукту];
- носія даних або носія даних з формулою на комп'ютерну програму.

Комп'ютерна програма і носій даних або носій даних з формулою на комп'ютерну програму зазвичай допускаються, якщо відповідний спосіб або пристрій також дозволені за умови, що всі етапи способу виконуються комп'ютером.

Нижче подається інформація щодо основних розділів, що містяться в Керівних принципах ЕПО 2018 р. стосовно СП.

Математичні методи, основи (G-II 3.3). Розділ з математичних методів був повністю переглянутий і перероблений, додавши відмінність між внеском у створення технічного результату, який служить технічній меті, його застосуванням в області технології і / або шляхом адаптації до конкретної технічної реалізації.

Що стосується вкладу в вигляді застосування в конкретну область техніки, то наводиться багато прикладів, зокрема:

- виявлення людей в цифровому зображенні, оцінює якість переданого цифрового аудіосигналу;
- відображення мовного введення в текстовий висновок;
- кодування з помилкою для передачі даних по каналу з шумом, стиснення аудіо, зображень, відео або даних датчиків;
- оптимізацію розподілу навантаження в комп'ютерній мережі;
- визначення витрат енергії суб'єкта шляхом обробки даних, отриманих від фізіологічних датчиків;
- надання оцінки генотипу на основі аналізу зразків ДНК, а також надання довірчого інтервалу для цієї оцінки для кількісної оцінки її надійності;
- надання медичної діагностики автоматизованою системою обробки фізіологічних вимірювань.

Слід зазначити, що кожен з наведених вище прикладів дуже специфічний, оскільки зазначення загальної мети недостатньо. Однак в Керівних принципах не міститься ясної вказівки щодо розкриття необхідної специфіки винаходу. В цій ситуації ми пропонуємо покладатись на відповідний прецедентне рішення (див. Т 1029/06), в якому йдеться про те, що використання мета-формулювання, що включає слова «технічний» або «фізичний», є недостатнім.

У Керівних принципах пропонується (в якості прикладу), що достатня специфіка в технічному результаті може бути досягнута

шляхом функціональної ув'язки і обмеження застосування методу до технічного результату, явно чи неявно.

Що стосується вкладу за допомогою конкретної технічної реалізації, математичний метод також може сприяти технічному характеру винаходу незалежно від будь-якого технічного застосування, якщо вимога направлена на конкретну технічну реалізацію математичного методу. Тут також слід уникати загальної технічної реалізації, і твердження, що математичний метод алгоритмічно більш ефективний, ніж математичні методи попереднього рівня техніки, не вирішує проблему. Дійсно, ми повинні пам'ятати, що технічний характер повинен оцінюватися незалежно від попереднього рівня техніки.

Штучний інтелект і машинне навчання (G-II 3.3.1). Вперше в Керівництві ЕРО 2018 р. з'явився розділ, що стосується штучного інтелекту (далі — ШІ) і машинного навчання, які спочатку визначаються як обчислювальні моделі і алгоритми класифікації, кластеризації, регресії і зменшення розмірності. Вони вважаються саме по собі абстрактними математичними принципами, незалежно від того, чи можуть вони бути «навчені» на основі (реальних) системи адаптації.

Заявник або практик, який складає заявку, пов'язану зі ШІ і машинним навчанням, повинен приділяти особливу увагу виразами, таким як «нейронна мережа» або «підпрограма AI», оскільки вони не вносять вклад в технічний характер формули.

Замість цього заявник або практик, що прагне отримати охорону в Європі в цій галузі, повинен встановити причинний зв'язок з технічним результатом, наприклад, використання математичного методу в пристрої для моніторингу серця з метою виявлення нерегулярних серцевих скорочень, класифікації цифрових зображень, відео, аудіо або мови сигнали на основі країв або атрибутів пікселів і уникати використання виразів, які можуть охоплювати когнітивні аспекти даних (наприклад, текстовий зміст документа).

У зв'язку з цим дуже корисно, що в нових Керівних принципах тепер вказується, що кроки створення набору для навчання і навчання моделей ШІ також можуть сприяти технічному характеру винаходу, якщо вони підтримують досягнення технічного призначення.

Керівні принципи не розглядають, такі вирази, як «нейронна мережа», «штучний інтелект» і «глибоке навчання», хоча і відносно добре прийняті і зрозумілі (наприклад, рішення Т 1285/10 Апеляційних рад), як такі, що використовуються в формулах винаходу. Швидше, в формулах використовуються наступні ключові слова, як «навчений розпізнавач», «адаптована модель», «компонент учня»

або навіть «визначення». Крім того, якщо у формулі винаходу використовуються такі терміни, як «нейронна мережа», вони зазвичай з'являються тільки в залежних пунктах формули винаходу.

Моделювання, проектування або моделювання (G-II 3.3.2).

Формули винаходу, спрямовані на методи моделювання, проектування або моделювання, можуть вважатися технічними відповідно до тих же принципів як і інші СП.

Наприклад, комп'ютерна реалізація поведінки адекватно певного класу технічних елементів або конкретних технічних процесів в технічно значущих умовах кваліфікується як технічний результат, як у випадку електронної схеми, схильною до шуму $1/f$ або конкретного промислового хімічного процесу. В цьому розділі Керівництва чітко вказано, що відсутність остаточного фізичного етапу виробництва продукту не потрібно для того, щоб метод моделювання мав право на патент.

Це відноситься не тільки до моделювання поведінки технічного елемента, але і в контексті комп'ютерного проектування конкретного технічного об'єкта (продукту, системи або процесу). Наприклад, визначення критичного параметра, такого як показник заломлення в оптичній системі або робочий параметр ядерного реактора є технічним результатом.

При складанні заявки на спосіб заявник або практик повинен уникати кроків, які пов'язують досягнення технічного результату з людськими рішеннями, а також простих конструктивних ознак, таких як опис багатопроцесорної системи в середовищі графічного моделювання.

Схеми, правила і методи виконання розумових дій, ігор або ведення бізнесу (G-II 3.5). Розділ, присвячений схемами і правилами для абстрактних цілей, таких як розумові дії, гра в ігри або ведення бізнесу, вже був присутній в попередніх редакціях Керівництва. Однак в редакції 2018 р. було надано велике і послідовне трактування цієї теми, з тим щоб допомогти заявникам і практикам визначити відповідні предметні області в цих областях.

Цей розділ досить великий з багатьма, різноманітними прикладами, і його можна поділити в такий спосіб.

Якщо заявка на спосіб включає в себе чисто інтелектуальну / ігрову / ділову реалізацію всіх етапів способу, вона стосується категорії неприйнятних методів. Наприклад, якщо симуляція включає в себе реальні значення, отримані технічними вимірами, це не є предметом винаходу, якщо тільки:

- відповідна формула включає в себе етап виконання технічних вимірювань або

- використання інших технічних засобів (наприклад, комп'ютер, вимірювальний прилад і т. ін.)
- якщо він виконує технічне завдання.

Кроки, які включають неохороноздатний предмет, можуть бути включені, однак вони будуть враховуватися тільки в тому випадку, якщо в контексті винаходу вони сприяють створенню технічного результату.

У цих рамках для практиків і заявників важливо звернути увагу на мову формули, оскільки вона може охоплювати як технічні ознаки, так і нетехнічні ознаки. Наприклад, такі терміни, як «система» або «засіб», будуть ретельно вивчені, тому що «система» може, наприклад, посилатися на фінансову організацію та «означає» організаційні одиниці.

Відповідно до Керівництва приклади охороноздатного предмета винаходу включають:

- при реалізації умови збігу випадкових чисел для оплати гри використання комп'ютера, що обчислює псевдовипадкову послідовність або механічних засобів, таких як кубічні кубики або рівномірно секціоновані барабани;
- мережева реалізація азартної гри, такої як бінго, в якій номери, фізично намальовані оператором, піддаються випадковому відображенню для передачі віддаленим гравцям, оскільки скремблювання результатів має технічний ефект забезпечення передачі даних; а також
- інтерактивне управління маневрами реального часу в ігровому світі, відображення яких схильне суперечливим технічним вимогам.

Навпаки, в якості прикладу обчислення, що визначає ігровий рахунок або рейтинг навичок для гравців, навіть якщо він є складним для обчислення, зазвичай вважається нетехнічним.

Нарешті, щодо другого бар'єру, наведеного вище, дається кілька прикладів для оцінювання предмета винаходу, в якому, хоча і вказана технічна проблема, однак, вона не вирішена, а обійдена. Так скорочення обсягу пам'яті, мережі або обчислювальних ресурсів, що досягається за рахунок обмеження складності гри, не долає технічні обмеження технічним рішенням. Автоматичний метод обліку, який дозволяє уникнути надмірної бухгалтерської звітності, не вирішує технічної задачі, якщо таке скорочення робочого навантаження пов'язане зі скороченням числа операцій, які повинні виконуватися через обмеження бізнесу.

Винаходи, реалізовані в розподіленому обчислювальному середовищі (F-IV 3.9.3). Нарешті, в Керівництво доданий

новий розділ, який пов'язаний з винаходами, реалізованими на комп'ютері, реалізованими в розподіленому обчислювальному середовищі, з тим щоб дати вказівки щодо вимог про єдність винаходу.

У Керівних принципах вказується, що може знадобитися послатися на конкретні особливості різних об'єктів в навколишньому середовищі і визначити, як вони взаємодіють, щоб забезпечити наявність всіх суттєвих ознак, якщо це не є суттєвим для здійснення винаходу. Різні суб'єкти, які беруть участь в розподіленій системі, можуть бути заявлені без виникнення заперечень, не пов'язаних з єдністю, однак може статися так, що ні всі заявлені об'єкти є новими і мають винахідницький рівень. Це той випадок, коли, наприклад, об'єкт кодує інформацію більш ефективним чином, але об'єкт, який приймає інформацію, декодує таку закодовану інформацію звичайним способом. Тобто об'єкт отримує інформацію звичайним чином, що є не новим і не має винахідницького рівня.

ЄПВ 30 травня 2018 р. провело міжнародну конференцію з патентування ШІ в Мюнхені, щоб детально вивчити цю тему. Матеріали і відеоролики конференції були опубліковані в розділі електронних курсів веб-сайту ЄПВ.

Однак в Керівних принципах міститься тільки короткий розділ з цього питання щодо того, що обговорювалося на конференції та інших пов'язаних з цим подій. Наприклад, застосування еквівалентності відповідно до статті 69 ЄПК поки не має вирішення. У Керівництві немає натяку на те, як відповідати на такі питання:

- чи може заявка на патентування процесу ШІ вважатися еквівалентною заявці на патентування класичного процесу з певною, докладною послідовністю етапів, наприклад, в форматі дерева рішень?;
- який ефект попереднього рівня техніки міг би розкривати рішення, що відноситься до класичних винаходів, реалізованих на комп'ютері, за формулою на методи ШІ, що відносяться до однієї і тієї ж технічної задачі, і навпаки (тобто розкриття ШІ в порівнянні із заявкою на класичний процес).

Заявники та практичні працівники можуть розглянути альтернативні рішення однієї і тієї ж технічної задачі і спробувати охопити як класичні, так і ШІ кроки в формулі винаходу, якщо формула не стане занадто загальною. В якості альтернативи може бути подана окрема патентна заявка, спеціально призначена для дерева рішень і / або методів ШІ, з тим щоб запобігти висновку про відсутність єдності.

Ще один важливий момент, щодо якого Керівні принципи не дають роз'яснень, полягає в тому, як оцінити вимогу достатності

розкриття суті винаходу у разі патентів на ШІ. У цій ситуації рекомендується надати якомога більше детальних рішень, включаючи порівняльні приклади і діапазони параметрів, а також приблизні набори навчальних даних.

Слід зазначити, що в Керівних принципах 2018 р. не має ніяких змін у визначенні кваліфікованого фахівця, хоча ця тема неодноразово обговорювалася. Це залишає відкритими проблеми, наприклад, чи має кваліфікований фахівець інструменти ШІ типових завдань роботи і чи може кваліфікований фахівець бути замінений машиною, яка пройшла підготовку в даній області техніки.

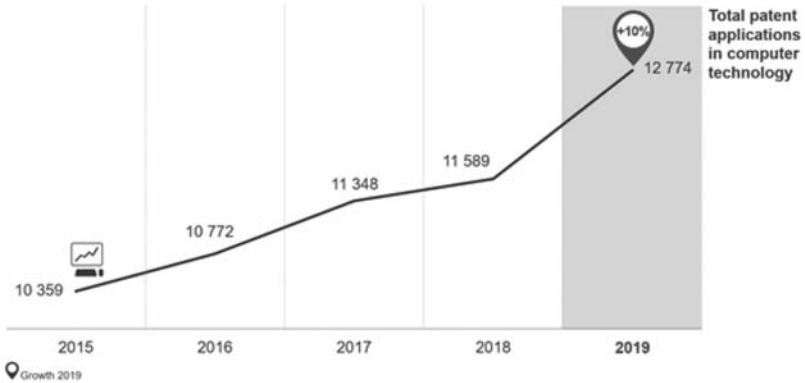
Ці проблеми, а також інші проблемні питання, такі як винахідницький рівень, можуть оцінюватися в національних судах або Апеляційними радами ЄПВ. У Керівних принципах 2018 р. розглядаються винаходи ШІ і роз'яснюються, що вони оцінюються такими самими критеріями, як й інші винаходи, реалізовані на комп'ютері. У будь-якому випадку ретельний розгляд стратегії патентування має вирішальне значення для отримання бажаної правової охорони.

Розвиток комп'ютерних технологій. У міру того, як четверта промислова революція (4IR) отримує подальший розвиток, в 2019 р. в ЄПВ відбулося також різке зростання кількості заявок на видачу патентів в області комп'ютерних технологій. Однак зростання в цій галузі обумовлене різними галузями, і не всі гравці є ІТ-фірми. Транспортні компанії, постачальники автомобільної промисловості та медичні фірми знаходяться в грі, з інноваціями в галузі безпеки, медичної візуалізації та управління рухом, які сприяють збільшенню кількості заявок на винаходи в області комп'ютерних технологій.

Друге місце за темпами зростання в ЄПВ. Зі збільшенням патентних заявок на 10 % комп'ютерні технології в 2019 р. стали другою найбільш швидко розвиваючою технологічною областю в ЄПВ.

Зростання було обумовлено в основному патентними заявками з Китаю (+ 19 % до 2018 р.), США (+ 14 %), а також з країн-членів ЄПВ (+ 9 %). Частка патентних заявок в області комп'ютерних технологій залишалася відносно стабільною протягом п'яти років, причому основна частина заявок надходила з США і країн-членів ЄПВ [9, 10].

Sharp rise – Total European patent applications² in computer technology



З практики розгляду спорів. Підхід ЄПВ до патентів на СІ. Існує значна частина прецедентного права ЄПВ про тлумачення ст. 52 (2) і (3) ЄПК в зв'язку з патентами на СІ, яке в основному і застосовується більшістю національних судів і патентних відомств держав-членів ЄПК.

ЄПВ вперше 27 січня 2020 р. опублікувало своє рішення з викладенням причин недавньої відмови видачі патентів за двома європейськими заявками, в яких система ШІ була позначена як винахідник. Подані фізичною особою восени 2018 р., заявки EP 18275163 і EP 18275174 були відхилені ЄПВ після усного розгляду з заявником у листопаді 2019 р. на тій підставі, що вони не відповідають юридичним вимогам ЄПК, а саме: винахідник, вказаний у заявці, повинен бути людиною, а не машиною. В обох заявках в якості винахідника названа машина, що має назву «DABUS», яка описується як «тип штучного інтелекту зв'язності». Заявник стверджував, що він придбав право на подання заявки на європейський патент у винахідника, будучи його правонаступником, стверджуючи, що як власник машини йому були передані будь-які права інтелектуальної власності, створені цією машиною.

У своїх рішеннях ЄПВ визначило, що тлумачення правових положень ЄПК приводить до висновку, що винахідник, зазначений в європейському патенті, повинен бути фізичною особою. ЄПВ також відзначило, що розуміння терміна «винахідник», який відноситься до фізичної особи, є міжнародним стандартом, і що різні національні суди ухвалили відповідні рішення. Крім того, зазначення винахідника є обов'язковим, оскільки воно має ряд правових наслідків,

зокрема, для забезпечення того, щоб зазначений винахідник був законним і щоб він або вона могли користуватися правами, пов'язаними з цим статусом. Щоб скористатися цими правами, винахідник повинен мати правосуб'єктність, якої не мають системи ШІ або машини. Нарешті, присвоєння імені машині недостатньо для задоволення вимог вищевказаної ЄПК [11, 12].

І на завершення декілька рекомендацій від експертів ЄПВ. Перша — у ЄПВ віддають перевагу терміну «винаходи, реалізовані на комп'ютері», а не «патенти на програмне забезпечення», тому що у законі чітко регламентується, що програмне забезпечення як таке не може бути запатентовано. Це можливо тільки в чіткій комбінації з комп'ютерами або датчиками. Друга — необхідно в описі визначити технічну задачу, яка вирішується винаходом, і як вона вирішується за допомогою ШІ або машинного навчання, а потім описати, як це рішення відрізняється від попереднього рівня техніки. Третя — графічне або письмове описування процесу повинно бути однаково зрозумілим для фахівця. Блок-схеми можуть бути дуже корисними в розумінні логіки самого процесу. Обидва способи написання і визначення суттєвих ознак винаходу є прийнятними.

Використання наведених рекомендацій при складанні заявки є дуже корисним для експерта в подальшому при розгляді заявок на патенти ШІ. Так вони дозволяють на стадії підготовки заявки правильно зазначити, якими є заявлені удосконалення, і оцінити, чи є який-небудь несподіваний технічний результат, який не може бути очікуваним заздалегідь на основі існуючого рівня техніки до дати подання заявки. Також добре мати запасну позицію, зазначивши в описі деякі конкретні приклади, які підтверджують можливість здійснення винаходу.

Список використаних джерел

1. Андрощук Г.О. Патентування комп'ютерних програм і методів підприємництва: стан і тенденції // Інтелектуальна власність. 2012. - № 4. С. 41-44., № 6. - С. 18-26.
2. Андрощук Г. О. Правова охорона програмного забезпечення (комп'ютерних програм і баз даних): монографія / Г. О. Андрощук, С. А. Петренко. К.: НДІ ІВ НАПрНУ, 2013. 300 с.
3. Андрощук Г. О. Патентне право: міжнародно-правове регулювання: монографія / Андрощук Г. О., Работягова Л. І.; Нац. акад. прав. наук України, НДІ інтелект. власності. Київ : Інтерсервіс, 2018. - 285 с.
4. Андрощук Г. О. Патентні системи зарубіжних країн: структурований аналіз законодавства / Андрощук Г. О., Работягова Л. І.;

Нац. акад. прав. наук України, НДІ інтелект. власності. - Київ : Інтерсервіс, 2018. - 213 с.

5. Raymond Millien Six Years After Alice: 61.8% of U.S. Patents Issued in 2019 Were 'Software-Related'—up 21.6% from 2018. URL: <http://www.ipwatchdog.com/2020/02/17/six-years-alice-61-8-u-s-patents-issued-2019-software-related-21-6-2018/id=118986>.

6. Guidelines for Examination. URL: <https://www.epo.org/law-practice/legal-texts/html/guidelines/e/j.htm>.

7. Andrea Perronace. EPO Publishes Revised Guidelines on Computer-implemented inventions. URL: <http://www.ipwatchdog.com/2018/11/15/epo-publishes-revised-guidelines-computer-implemented-inventions/id=103316>.

8. Andrea Perronace What to Know About the 2019 European Patent Office Guidelines for Examination. URL: <https://www.ipwatchdog.com/2019/11/05/know-european-patent-office-2019-guidelines-examination/id=115620>.

9. Digitalisation triggers patenting growth. URL: <http://www.epo.org/about-us/annual-reports-statistics/statistics/2019/digitalisation-triggers-patenting-growth.html>.

10. Welcome to the Patent Index 2019. URL: <http://www.epo.org/about-us/annual-reports-statistics/statistics/2019.html>.

11. EPO publishes grounds for its decision to refuse two patent applications naming a machine as inventor. URL: <https://www.epo.org/news-issues/news/2020/20200128.html>.

12. Андрощук Г.О. Машина винахідник: що вирішило ЄПВ // Інтелектуальна власність в Україні. 2020. №2. С.58-59.

СИСТЕМИ ЕЛЕКТРОННОГО ПРАВОСУДДЯ: ЗАПРОВАДЖЕННЯ ПРОЕКТУ «ЕЛЕКТРОННИЙ СУД»

Весь світ рухається вперед. Для спрощення певних процесів, економії часу та матеріальних ресурсів, в різних сферах життя запроваджуються нові технології. Однією з таких сфер є судочинство.

В більшості провідних країн (таких, як Сінгапур, Німеччина, Швейцарія, Франція, Норвегія, Португалія, Австрія) активно використовуються системи електронного правосуддя.

Україна в цьому напрямку на даний час не поспіває за провідними країнами. Одним із засобів підвищення ефективності судочинства запропонований проект «Електронний суд», який покликаний спростити комунікацію між судом та учасниками судового процесу, судом та іншими органами державної влади (швидкий обмін документами, зменшення судових витрат та ін.).

У зв'язку з ситуацією, яка склалась на території України через поширення коронавірусної інфекції COVID-19, стала нагальною потреба в удосконаленні та швидкому впровадженні електронного судочинства, оскільки на даний час існує низка недоліків у використанні Єдиної судової інформаційно-телекомунікаційної системи, яка була запроваджена у «тестовому режимі».

1. Перші кроки щодо запровадження проекту «Електронний суд» в Україні.

Запровадження проекту «Електронний суд» як модуля Єдиної судової інформаційно-телекомунікаційної системи (далі — ЄСІТС) вперше було передбачено у Господарському процесуальному кодексі, Цивільному процесуальному кодексі та Кодексі адміністративного судочинства, які набули чинності 15 грудня 2017 р.

Ця система була покликана спростити взаємодію між учасниками судового процесу та судом шляхом забезпечення обміну електронними документами між ними (подача процесуальних документів, ознайомлення з матеріалами судової справи, направлення повісток, судових рішень, прийнятих за результатом розгляду справи та ін.).

В процесуальних кодексах зазначається про те, що ЄСІТС починає функціонувати через 90 днів з дня опублікування Державною судовою адміністрацією України у газеті «Голос України» та на веб-порталі судової влади оголошення про створення та забезпечення функціонування ЄСІТС, але на практиці цього так і не відбулось.

01.12.2018 р. Державна судова адміністрація України оголосила про створення та забезпечення функціонування ЄСІТС в газеті «Голос України» та на офіційному веб-порталі «Судова влада України».

Однак вже 28.02.2019 р. Вищою радою правосуддя прийнято рішення 624/0/15-19 про повернення на доопрацювання проекту Положення про ЄСІТС, в якому вирішено запропонувати Державній судовій адміністрації України відкликати оголошення про створення та забезпечення функціонування ЄСІТС.

Після цього Державна судова адміністрація України повідомила про відкликання оголошення, опублікованого в газеті «Голос України» (№ 229 (6984) від 01.12.2018 р.).

22.12.2018 р. Державна судова адміністрація України затвердила наказ «Про проведення тестування підсистеми «Електронний суд» у місцевих та апеляційних судах» № 628, під час якої зобов'язано дотримуватись вимог Положення про автоматизовану систему документообігу суду, затвердженого рішенням Ради суддів України № 30 від 26.11.2010 р. у відповідній редакції.

З огляду на те, що запровадження підсистеми «Електронний суд» відбулось у «тестовому режимі», не всі суди (судді) та інші учасники судового процесу розпочали використовувати її у своїй діяльності. Насамперед це пов'язано із відсутністю у діючому законодавстві поняття «тестового режиму» у якому наразі працює ЄСІТС.

2. Щодо положень Закону, якими встановлюється обов'язковість використання ЄСІТС.

Відповідно до п. 15 «Перехідних положень» Закону України «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів» № 2147-VIII від 03.10.2017 р. **до дня початку функціонування ЄСІТС:** подання, реєстрація, надсилання процесуальних та ін. здійснюються в паперовій формі; розгляд справи у суді здійснюється за матеріалами справи у паперовій формі.

В Перехідних положеннях процесуальних кодексів встановлено, що ЄСІТС починає функціонувати через 90 днів з дня опублікування Державною судовою адміністрацією України у газеті «Голос України» та на веб-порталі судової влади оголошення про створення та забезпечення функціонування ЄСІТС.

Крім того, відповідно до ч. 6 ст. 6 ГПК України адвокати, нотаріуси, приватні виконавці, арбітражні керуючі, судові експерти, державні органи, органи місцевого самоврядування, суб'єкти господарювання державного та комунального секторів економіки та

особи, які провадять клірингову діяльність у значенні, наведеному в Законі України «Про ринки капіталу та організовані товарні ринки», реєструють офіційні електронні адреси в ЄСІТС в обов'язковому порядку, інші особи — в добровільному порядку.

Отже жодний нормативно-правовий акт не встановлює обов'язку користування цією системою до спливу 90 денного строку з дня опублікування Державною судовою адміністрацією України оголошення про створення ЄСІТС. Крім того наразі відсутнє визначення терміну «тестовий режим», а тому, використання підсистеми «Електронного суду» не має обов'язкового характеру.

3. Проблеми, які виникли під час використання «Електронного суду» у «тестовому режимі» та недоліки системи.

• Не всі місцеві та апеляційні суди розпочали використовувати «Електронний суд» навіть в тестовому режимі.

Оскільки оголошення про створення та забезпечення функціонування ЄСІТС було відкликано, а поняття «тестового режиму» функціонування ЄСІТС так і не здобуло правової визначеності, деякі суди не розпочали використовувати «Електронний суд», а подані сторонами електронні процесуальні документи, хоч і приймаються системою, в подальшому залишаються без реакції з боку суду або така реакція є негативною для заявника (наприклад, позовна заява вважається не підписаною).

І хоча статтями 44 КАС України, 43 ЦПК України, 42 ГПК України, передбачено, що сторони можуть подавати до суду документи (в тому числі процесуальні документи, письмові та електронні докази тощо) в електронній формі з використанням ЄСІТС, це не гарантує того, що у подальшому користувач матиме можливість відстежувати стан розгляду справ, переглядати документи суду, документи інших учасників судового процесу тощо.

І пов'язано це не тільки із так званим «тестовим режимом», коли судді відмовляються від роботи у системі, яка законодавчо не існує, а у багатьох випадках із технічною неможливістю апарату суду здійснювати роботу у системі.

Правову невизначеність спробував виправити Верховний Суд. У своїй постанові від 06.08.2020 р. по справі 160/1841/19 суд дійшов висновку, що з 22.12.2018 р. отримані всіма місцевими та апеляційними адміністративними судами заяви та інші процесуальні документи через підсистему «Електронний суд» мають реєструватися та розглядатися в установленому порядку. Відсутність факту початку повноцінного функціонування ЄСІТС не може бути перешкодою для роботи її підсистеми «Електронний суд» та відповідно, права особи на подання процесуальних документів через цю підсистему в електронній формі.

Відповідно до пункту 2 Розділу XI Положення № 30 від 26.11.2010 р. учасники судового процесу за допомогою зареєстрованого Електронного кабінету можуть надсилати копії електронних документів іншим учасникам судової справи, крім випадків, коли інший учасник не має зареєстрованого електронного кабінету, подавати позовні заяви та інші передбачені законом процесуальні документи, що подаються до суду і можуть бути предметом судового розгляду, а також отримувати судові рішення та інші електронні документи.

Отже, учасники судового процесу мають право подавати до суду електронні документи, але у разі невикористання певним судом підсистеми «Електронний суд», існує вірогідність, що у подальшому він матимете можливість відстежувати стан розгляду справ, переглядати документи суду, документи інших учасників судового процесу тощо.

Крім того, відсутнє нормативно-правове регулювання порядку переведення працівниками суду документів з паперової форми в електронну. З цього приводу судді скаржаться на те, що відсутня технічна можливість сканування документів та розміщення їх в «Електронному суді».

Слід відзначити, що, не дивлячись на відсутність нормативно-правових актів, які б встановлювали процедурні моменти, місцеві адміністративні суди та апеляційні суди активно використовують цю систему, що значно спрощує комунікацію учасників судового процесу з судом.

•З моменту запуску підсистеми «Електронний суд» в ній існувала невелика кількість шаблонів процесуальних документів, які можна було заповнити та направити до суду.

Так, в системі були відсутні шаблони клопотань про ознайомлення з матеріалами судової справи, про перенесення розгляду справи, про розгляд справи за відсутністю учасника судового процесу та ін.

У зв'язку з цим учасник судового процесу вимушений був скласти окремо такий документ в Word, а потім шляхом копіювання переносити на чистий аркуш Електронного суду.

У подальшому цей недолік здебільшого було усунуто шляхом доповнення необхідними шаблонами.

На даний час існує ряд проблем у користування підсистемою, які створюють учасникам значні незручності.

Наприклад, якщо ви є відповідачем або третьою особою у цивільній справі, і маєте бажання подати процесуальний документ в електронному вигляді (відзив на позовну заяву, пояснення та ін.), але раніше не звертались у цьому провадженні до суду з електрон-

ними документами, то спочатку Вам необхідно направити до суду заяву про вступ у справу та зазначити у якості кого ви звертаєтесь (зазначити свій процесуальний статус) та надати підтвердження своїх повноважень. Лише після задоволення судом цієї заяви ви отримуєте доступ до електронної справи та зможете формувати електронні документи саме по цій справі.

Після отримання доступу (якщо конкретний суд має технічну можливість його надати) ви маєте можливість побачити стан розгляду справи, документи, які подані іншою стороною, рішення суду, які були прийняті, а також отримуєте можливість подавати процесуальні документи по цій справі.

Слід пам'ятати: якщо певний суд не використовує у своїй діяльності підсистему «Електронний суд», то заяву про вступ до справи взагалі не буде розглянуто. Відповідно і доступу до неї ви не отримаєте.

• У зв'язку з технічними недоліками, відсутня можливість подачі процесуальних документів в інтересах юридичної особи.

Наступним недоліком системи слід зазначити проблему із зазначенням коду ЄДРПОУ юридичної особи при формуванні документу у системі.

Так, при формуванні документу необхідно зазначити певні відомості щодо заявника (сторони), зокрема має бути зазначено ідентифікаційний номер (РНОКПП), який складається з 10 цифр.

Якщо документ в інтересах юридичної особи формує представник, то він також має зазначити ідентифікаційний код. При цьому код юридичної особи (ЄДРПОУ) складається з 8 цифр. На практиці з цим виникають проблеми, оскільки в Електронному суді неможливо зазначити тільки 8 цифр, необхідно ввести 10, інакше система не дає можливості продовжити формування документа. Отже, особа фактично вимушена зазначити недостовірний код для переходу до наступного розділу (додавати ще дві вигадані цифри) або взагалі доведеться відмовитися від подачі документа, бо перейти до іншого кроку не вийде.

• Відсутність контролю доступу певної особи до електронного перегляду справи.

В зв'язку з відсутністю законодавчо закріпленого порядку роботи з системою «Електронний суд» є ризик розголошення персональних даних осіб, комерційної таємниці та іншої інформації з обмеженим доступом.

Мова йде про те, що доступ до електронної судової справи не контролюється зі сторони суду. Так, представник, приєднавшись до електронної справи у першій інстанції, маючи повноваження тільки на першу інстанцію, фактично бачить весь рух справи і всі доку-

менти вже після припинення його повноважень (у апеляційній та касаційній інстанції). Така ж ситуація виникає і в тому випадку, коли у представника закінчуються повноваження в процесі розгляду справи у першій інстанції. Навіть при повідомленні суду про такий факт, доступ до електронної справи не припиняється.

• Неможливість перевірити справжність електронно-цифрового підпису та пересвідчитись в тому, що саме ця особа направляє до суду певні процесуальні документи.

На даний час, на жаль, не існує жодного нормативно-правового акту, який би передбачав контроль та перевірку виданих електронно-цифрових підписів. Не визначені і програмні засоби якими можливо здійснити перевірку автентичності ЕЦП.

При сучасному розвитку технологій та знань існує велика вірогідність використання зловмисниками підробленого чи вкраденого ЕЦП. Тобто будь-яка особа може звернутись до суду від іншої фізичної або юридичної особи, встановити реального заявника просто неможливо. Отже необхідно розробити систему контролю автентичності ЕЦП, законодавчо закріпити програмні засоби та порядок такого контролю, встановити процедуру підтвердження особи заявника при роботі з системою «Електронний суд».

Наприклад, в Німеччині існує таке поняття, як «електронна адвокатська скринька». Для того, щоб увійти до неї, необхідно не тільки зазначити власне ім'я та прізвище, а ще й підтвердити свою авторизацію за допомогою спеціальної карти з чипом, на якій є електронний підпис адвоката.

Підсумовуючи вищезазначене, підсистема «Електронний суд» потребує подальшого законодавчого врегулювання, системного удосконалення, усунення чисельних технічних недоліків, розробки та застосування заходів, направлених на захист від стороннього втручання у систему.

Список використаних джерел

1. Закон України «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів» № 2147-VIII від 03.10.2017.
2. Рішення Вищої ради правосуддя «Про повернення на доопрацювання проекту Положення про Єдину судову інформаційно-телекомунікаційну систему» № 624/0/15-19 від 28.02.2019.
3. Наказ Державної судової адміністрації України «Про проведення тестування підсистеми «Електронний суд» у місцевих та апеляційних судах» № 628 від 22.12.2018.

4. Бринцев О. В. «Електронний суд» в Україні. Досвід та перспективи : монографія / О. В. Бринцев. – Х. : Право, 2016. – 72 с. – (Серія «Інноваційне суспільство і розвиток законодавства»).

5. НААУ залучили до роботи над розробкою та впровадженням підсистеми «Електронний суд». Тепер ВРП враховуватиме пропозиції та зауваження щодо потреб адвокатів при використанні деяких компонентів системи. URL: https://zib.com.ua/ua/143096-advokati_doluchilis_do_vprovadzhennya_elektronnogo_sudu.html.

6. Постанова Верховного Суду від 06.08.2020 по справі № 160/1841/19 (№ рішення в ЄДРСР 90846939).

Бакурова А. В.,
доктор економічних наук, професор,
Національний університет «Запорізька політехніка»,
Пасічник М. С.,
аспірант, Національний університет
«Запорізька політехніка»,
Терещенко Е. В.,
кандидат фіз.-мат. наук, доцент,
Національний університет «Запорізька політехніка»,
Філей Ю. В.,
кандидат юридичних наук, доцент,
Національний університет «Запорізька політехніка»

ПРОДУКЦІЙНА МОДЕЛЬ ПРИЙНЯТТЯ РІШЕНЬ НА ПРИКЛАДІ ПРИЗНАЧЕННЯ СУДОМ ПОКАРАННЯ ЗА КРАДІЖКУ

Призначення покарання це доволі складний та багатоаспектний процес. Відповідно до ст. 65 Кримінального кодексу України (КК України) [1], суд призначає покарання у межах, установлених у санкції статті Особливої частини КК, що передбачає відповідальність за вчинений злочин, відповідно до положень Загальної частини КК, враховуючи ступінь тяжкості вчиненого злочину, особу винного та обставини, що пом'якшують та обтяжують покарання. Під час призначення покарання суддя повинен оцінити усі ознаки складу злочину та обставини його вчинення з метою визначення міри відповідальності підсудного і призначення йому співрозмірного покарання. Міра покарання в залежності від складу злочину

регламентується нормами закону, що дозволяє формально визначати межі максимуму і мінімуму розміру покарання. Окрім об'єктивних факторів в цьому процесі присутній і суб'єктивізм, так званий судовий угляд. Вибір виду покарання у разі, коли закон передбачає альтернативні санкції залишається за суддею. Крім того, слабо формалізованою частиною вироку залишається урахування обставин вчинення злочину й характеристики особи винного. При тому, що від судді не вимагається детальне коментування критеріїв оцінки, чітко регламентується необхідність мотивованого вибору покарання. Для уніфікації врахування пом'якшуючих та обтяжуючих обставин, особи винного цілком природно формалізувати їхні оцінки. Розробка загальної бази знань винесення вироку при всіх можливих поєднаннях різних обставин дає надію на винесення схожих вироків при схожих за складом та обставинами злочинах.

Метою публікації є побудова загальної моделі системи підтримки прийняття рішень (СППР) у суді як нечіткої продукційної системи [2, 3, 4, 5, 6], а також проведення циклу експериментів з розробленою СППР на основі даних про реальні справи з бази Єдиного державного реєстру судових рішень в Україні [7]. У побудові відповідної моделі використовуються вирок за крадіжку (стаття 185 Кримінального кодексу України). Вибір цього злочину зумовлений тим, що крадіжки є найбільш частими злочинами, що вчиняються в Україні — вони складають більше 40 % від кількості всіх зареєстрованих злочинів. Запропоновано два варіанти реалізації нечіткої продукційної системи — алгоритмами Mamdani та Sugeno. Включення розробленої моделі до системи «Електронний суд», що є ознакою інформаційного суспільства, спроможне підвищити рівень автоматизації судової практики та запобігати корупції.

Так, суд призначає покарання у межах, установлених у санкції статті Особливої частини КК, що передбачає відповідальність за вчинений злочин, відповідно до положень Загальної частини КК, враховуючи:

- 1) ступінь тяжкості вчиненого злочину;
- 2) особу винного;
- 3) обставини, що пом'якшують та
- 4) обтяжують покарання [1].

Законодавча санкція статті враховує як кількісні показники відповідних обставин, так і якісні.

Зважаючи на це, методом прямого логічного виведення вхідними змінними було обрано такі.

Лінгвістична змінна *Severity*, що характеризує ступінь тяжкості вчиненого злочину, приймає значення з терм-множини {невелика,

середня, велика}. Ця змінна дозволяє враховувати повторність злочину, наявність раніше призначеного покарання, злочин, вчинений за попередньою змовою групою осіб, тощо.

Лінгвістична змінна *Personality* характеризує особу винного та приймає значення з терм-множини {негативна, нейтральна, позитивна}. Дозволяє враховувати, наприклад, працевлаштування, наявність суспільно корисної діяльності, характеристику за місцем проживання, тощо.

Необхідно зазначити, що відповідно до ч. 3 ст. 66 Кримінального кодексу України, якщо будь-яка з обставин, що пом'якшує покарання, передбачена в статті Особливої частини КК як ознака злочину, що впливає на його кваліфікацію, суд не може ще раз враховувати її при призначенні покарання як таку, що його пом'якшує [1]. Таких обставин визначено одинадцять. Для оцінки обставин, що пом'якшують покарання, було обрано дві лінгвістичні змінні. Лінгвістична змінна *Mitigation* дає оцінку можливості урахування суддею визначеної кількості реалізованих обставин. Лінгвістична змінна LM оцінює рівень пом'якшення покарання обставинами, які реалізувалися.

Також при побудові алгоритму призначення покарання нами були взяті до уваги зазначені в ст. 67 Кримінального кодексу України обставини, які обтяжують покарання. Таких обставин визначено чотирнадцять. При призначенні покарання суд не може визнати такими, що його обтяжують, інші обставини. Якщо будь-яка з обставин, що обтяжує покарання, передбачена в статті Особливої частини КК як ознака злочину, що впливає на його кваліфікацію, суд не може ще раз враховувати її при призначенні покарання як таку, що його обтяжує [1]. Вхідні змінні для оцінки обставин, що обтяжують покарання позначено через *Burden* та LB. Лінгвістична змінна *Burden* дає оцінку можливості урахування визначеної кількості реалізованих обставин. Лінгвістична змінна LB оцінює рівень обтяження покарання обставинами, які реалізувалися.

Лінгвістична змінна *Lawyer* характеризує рівень нейтральності судді та приймає значення з терм-множини {лояльний, нейтральний, суворий}. Будемо вважати, що справедливим є суддя за рівнем «нейтральний». Введення додаткових термів дозволить поставити задачу про адекватність винесеного вироку, про оцінку впливу особи судді.

Відповідно до ст. 185 КК України, суд може призначати покарання у виді штрафу, обмеження або позбавлення волі, громадські роботи. Назначимо такі змінні виходу системи.

Лінгвістична змінна виходу *Fine* визначає розмір штрафу.

Лінгвістична змінна виходу *Years* визначає кількість років позбавлення волі.

Лінгвістична змінна виходу *RF* (*Restriction of freedom*) визначає рівень обмеження волі.

Лінгвістична змінна виходу *Public Works* — громадські роботи

Лінгвістична змінна виходу *Condition* визначає реальне або умовне введення в дію.

Для всіх лінгвістичних змінних виходу було обрано терм-множини, що містять по три терми, які характеризують рівень реалізації {невисокий, середній, високий}.

Функції належності термів вхідних та вихідних лінгвістичних змінних визначаються експертно. Діапазони значень регулюються відповідними нормами законодавства окремо для кожної статті.

Таким чином загальна модель СППР у суді має вигляд:

(*Fine, Years, RF, Public Works, Condition*) = *F* (*Severity, Lawyer, Mitigation, Personality, Burden, LB, LM*), (1)

де *F* — відповідний алгоритм нечіткого виведення.

Для проведення експерименту авторами було обрано ст. 185 КК України про крадіжку. Різні частини статті ст. 185 КК України про крадіжку мають різні варіанти вироків. Складність бази нечітких продукційних правил буде визначатися змістом певної частини статті.

Юридичним документам притаманна певна структурованість та точність формулювань, що застосовують професійну термінологію норм права. Стиль юридичних документів відзначається стандартизацією і уніфікацією мови, широким вживанням сталих словосполучень, трафаретів, застосуванням типових текстів. Не дивлячись на це, далеко не всі юридичні терміни підвладні формалізації, що й виправдовує вибір методів нечіткої математики.

Для побудови нечіткої продукційної системи необхідно сформулювати базу з узгоджених нечітких продукційних правил, які містять формалізовані знання експертів предметної області. Базовим формалізмом є поняття лінгвістичної змінної, значенням якої можуть бути слова та словосполучення спеціалізованої природної мови експертів. Лінгвістична змінна приймає значення з терм-множини, елементами якої є терми, що задаються нечіткою множиною з визначеною функцією належності.

При побудові системи та проведенні експериментів автори ставили за мету отримати апроксимацію відомих значень вироків з джерела [7], що дозволить вихідні дані системи використовувати в подальшому як довідку, підґрунтя для винесення вироку суддею, загальну для всіх судів країни.

Як можна бачити з формули (1), деякі змінні виходу загальної моделі СППР — *Fine, Years* — приймають числові значення, тому представляється цікавим порівняти можливості найбільш пошире-

ної моделі нечіткого логічного виведення алгоритму Mamdani з можливостями алгоритму нечіткого логічного виведення Sugeno, яка має на виході чіткі значення деякої функції вхідних змінних.

Розглянемо етапи реалізації алгоритму Mamdani та алгоритму Sugeno в Fuzzy Logic Toolbox MatLab [8].

Не втрачаючи узагальненості для більшої визначеності далі будемо розглядати процес прийняття судового рішення на прикладі ст. 185 КК України про крадіжку, що складається з п'яти частин. Для проведення експерименту обираємо частину третю цієї статті, за якою крадіжка, що поєднана з проникненням у житло, інше приміщення чи сховище або що завдала значної шкоди потерпілому, карається позбавленням волі на строк від 3 до 6 років.

Таким чином загальна модель СППР у суді за формулою (1) трансформується для частини третьої ст. 185 КК України у формулу, що має вигляд:

$$Years = F(Severity, Personality, Mitigation, LM, Burden, LB, Lawyer), \quad (2)$$

де F — відповідний алгоритм нечіткого виведення.

Функції належності термів вхідних та вихідних лінгвістичних змінних визначалися на матеріалах вироків за кримінальними справами за ч. 3 ст. 185 КК України. Найбільш вдалим виявилися трапецеївидні функції належності термів для вхідних змінних *Severity*, *Lawyer*, *Mitigation*, *Personality*, *Burden* та трикутні для *LB*, *LM*.

Функції належності термів вхідних змінних представлені у табл. 1.

Таблиця 1

**Вхідні лінгвістичні змінні СППР та їхні терми
з функціями належності**

Лінгвістична змінна	Позначення термів та відповідних функцій належності		
Severity	d1 [0 0 0.6 1.2]	d2 [0.5 1 2 2.5]	d3 [1.8 2.4 3 3]
Personality	Disrepute [0 0 0.4]	Norm [0.14 0.46 0.54 0.86]	Good [0.6 1 1.4]
Mitigation	m1 [0 0 3 4]	m2 [3 5 6 8]	m3 [7 8 11 11]
LM	lm1 [0 0 0.4]	lm2 [0.1 0.5 0.9]	lm3 [0.6 1 1.4]
Burden	b1 [0 0 4 6]	b2 [4 6 8 10]	b3 [8 10 14 14]
LB	lb1 [0 0 0.4]	lb2 [0.1 0.5 0.9]	lb3 [0.6 1 1.4]
Lawyer	Soft [0 0 0.15 0.4]	Middle [0.05 0.4 0.6 0.85]	Hard [0.6 0.85 1 1]

Функції належності термів змінної виходу за алгоритмом Mamdani, що характеризує кількість років ув'язнення, представлені на рис. 1 та у табл. 2.

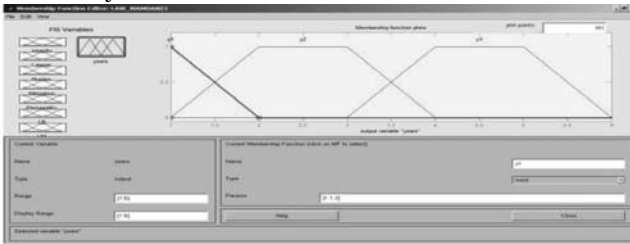


Рисунок 1. Функція належності термів змінної виходу Years за алгоритмом Mamdani

Функції належності термів змінної виходу Years будувалися з огляду на судову практику, за якою відомо, що найменший строк, який призначається за ч. 3 ст. 185 КК України — це один рік. Найбільший строк — шість років — є дуже суворим покаранням, що зустрічається у судових вироках дуже рідко.

Таблиця 2

Значення змінної виходу СППР

Алгоритм	Змінна	y1	y2	y3
Mamdani	Years	[1 1 2]	[1 2 3 4]	[3 4 5 6]
Sugeno	Years (linear)	[0.01 0 0.22 -0.144 - 0.01 0.1 -0.09 2.9]	[0.01 0 0.22 -0.144 - 0.01 0.1 -0.09 2.9]	[0.01 0 0.22 - 0.144 -0.0 0 -0.0 2.9]

Для прикладу результату роботи СППР на рис. 2 наведено поверхню відгуку для моделі Mamdani для вихідної змінної Years від вхідних змінних Severity, Mitigation.

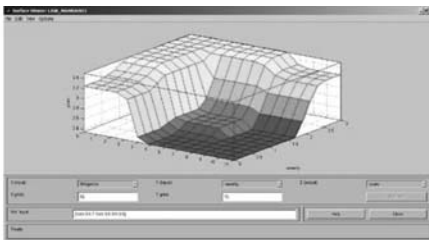


Рисунок 2. Поверхня відгуку для вихідної змінної Years від вхідних змінних Severity, Mitigation

Для реалізації алгоритму Mamdani було розроблено базу нечітких продукційних правил (табл. 3) виду:

«ЯКЩО ступінь тяжкості вчиненого злочину = «велика» ТА особа винного = «негативна» ТА обставини, що пом'якшують = «від 7 до 11» ТА обставини, що обтяжують покарання = «від 8 до 14» ТА рівень справедливості судді = «нейтральний» ТА рівень обтяжуючих обставин = «великий» ТА рівень пом'якшуючих обставин = «великий» ТО покарання буде «від 1 до 4 років»».

Таблиця 3

Нечіткі продукційні правила R_s , $s = 1-28$ для системи нечіткого виведення за алгоритмом Mamdani

R_s	S e v e - rity	Lawyer	B u r - den	M i t i - gation	Perso-nality	LB	LM	Years
1	D1					Lb1	Lm3	Y1
2	D2	middle			norm			Y2
3	D2	soft		M3	norm		Lm3	Y2
4	D3	hard	B3		disrepute	Lb3		Y3
5	D3	middle	B3		good	Lb3		Y2
6		middle	B3	M3	disrepute	Lb1	Lm3	Y2
7		soft		M3			Lm3	Y1
8		hard	B3			Lb3		Y3
9	D3	middle	B3	M3	disrepute	Lb3	Lm3	Y2
10	D3	middle	B3	M1	disrepute	Lb3	Lm1	Y3
11			B3			Lb3		Y3
12				M3			Lm3	Y1
13			B3	M3		Lb3	Lm3	Y2
14	D1							Y1
15	D2							Y2
16	D3							Y3
17		soft						Y1
18		middle						Y2
19		hard						Y3
20					disrepute			Y3
21					norm			Y2
22					good			Y1
23			B1			Lb1		Y1
24			B2			Lb2		Y2
25			B3			Lb3		Y3
26				M1			Lm1	Y3
27				M2			Lm2	Y2
28				M3			Lm3	Y1

Функції виходу алгоритму *Sugeno* було побудовано як лінійні функції вхідних змінних, коефіцієнти яких представлені у табл. 2. Коефіцієнти обиралися з огляду на вже відомі міри покарання за даними джерела [7].

У випадку реалізації алгоритму *Sugeno* було розроблено базу нечітких продукційних правил:

«ЯКЩО рівень нейтральності судді = «нейтральний» ТО покарання буде u_2 »,

«ЯКЩО рівень нейтральності судді = «лояльний» ТО покарання буде u_1 »,

«ЯКЩО рівень нейтральності судді = «суворий» ТО покарання буде u_3 ».

У випадку алгоритму *Mamdani* база знань об'єднує 28 продукційних правил (табл.3), три з яких співпадають з базовими правилами алгоритму *Sugeno*. Завдяки такій кількості правил досягається більша відповідність до нелінійності процесу прийняття судових рішень.

У табл. 4 та табл. 5 наведено результати експерименту з розробленою СППР за даними вироків шести типових справ з реєстру судових рішень в Україні [7].

Таблиця 4

Вхідні дані експерименту

Дані про злочин за вироком	Змінна входу	Значення терму
Справа № 207/2695/17		
повторно, з проникненням у житло; матеріальна шкода у розмірі 42059 грн.	<i>Severity</i>	d3=2,5
рецидив злочину	<i>Burden</i>	b3=5,8
щире каяття	<i>Mitigation</i>	m3=7,65
не працює, не одружений, раніше судимий	<i>Perso-nality</i>	Disrepute=0,159
-	<i>LB</i>	lb3=0,635
-	<i>LM</i>	lm3=0,3
Справа №206/4630/17		
проник до будинку;		
матеріальна шкода у розмірі 762,50 грн	<i>Severity</i>	d1=0,7
судом не встановлено	<i>Burden</i>	0
судом не встановлено	<i>Mitigation</i>	0
не працює, за місцем мешкання характеризується негативно; зловживає спиртними напоями, не судимий	<i>Perso-nality</i>	Norm=0,5
-	<i>LB</i>	0
-	<i>LM</i>	0

Таблиця 4 (продовження)

Дані про злочин за вироком	Змінна входу	Значення терму
Справа №315/1155/17		
проникнення у інше приміщення, матеріальний збиток на 290 грн	<i>Severity</i>	d1=0,2
вчинення злочину в стані алкогольного сп'яніння	<i>Burden</i>	b3=1
щире каяття та активне сприяння розкриттю злочину	<i>Mitigation</i>	m3=1
не одружений, не працюючий; схильний до вживання спиртного, схильний до стійкої злочинної діяльності, не судимий	<i>Perso-nality</i>	Disrepute=0,4
-	<i>LB</i>	lb3=0,5
-	<i>LM</i>	lm3=0,3
Справа № 127/14282/16-к		
повторно, з проникненням у житло; матеріальна шкода у розмірі 4131,70 грн.	<i>Severity</i>	d3=2,5
рецидив злочину	<i>Burden</i>	b3=5,8
щире каяття	<i>Mitigation</i>	m3=7,65
не працює, одружений, раніше судимий	<i>Perso-nality</i>	Disrepute=0,2
-	<i>LB</i>	lb3=1
-	<i>LM</i>	lm3=0,1
Справа №161/13758/17		
проник на територію будинку; матеріальна шкода становить 516,15 грн.	<i>Severity</i>	d1=0,7
вчинення злочину в стані алкогольного сп'яніння	<i>Burden</i>	b3=1
щире каяття, активне сприяння розкриттю злочину	<i>Mitigation</i>	m3=1
не працює, не одружений, раніше судимий	<i>Perso-nality</i>	Disrepute=0,25
-	<i>LB</i>	lb3=0,5
-	<i>LM</i>	lm3=0,3
Справа №311/2510/17		
повторно, поєднане з проникненням у житло;		
майнова шкода на загальну суму 10 800 грн 28 копійок + 8 527 грн	<i>Severity</i>	d2=2,3
судом не встановлено	<i>Burden</i>	0
провину визнав повністю, щиро кається	<i>Mitigation</i>	m3=1
не працює, не одружений, раніше судимий	<i>Perso-nality</i>	Norm=0,5
-	<i>LB</i>	0
-	<i>LM</i>	lm3=0,3

У всіх випадках, наведених в табл. 4, вважалося, що рішення приймає справедливий суддя, тобто вхідна змінна *Lawyer* приймає значення *Middle* з відповідним значенням функції належності 0,5.

Таблиця 5

Порівняння рішень за вироком справи та рішень, отриманих за роботою СППР для змінної виходу *Years*

Справа №	Термін позбавлення волі за вироком суду	Алгоритм	Рекомендація СППР	Відхилення
207/2695/17	3 роки і 3 місяці (3,25)	<i>Mamdani</i>	3,25	0
		<i>Sugeno</i>	3,17	-0,08
206/4630/17	3 роки	<i>Mamdani</i>	3,25	+0,25
		<i>Sugeno</i>	2,9	-0,1
315/1155/17	3 роки	<i>Mamdani</i>	3,25	+0,25
		<i>Sugeno</i>	3	0
127/14282/16-к	3 роки 6 місяців (3,5)	<i>Mamdani</i>	3,5	0
		<i>Sugeno</i>	3,1	-0,4
161/13758/17	4 роки (з встановленням іспитового строку 2 роки)	<i>Mamdani</i>	3,25	-0,75
		<i>Sugeno</i>	3	-1,0
311/2510/17	4 роки (покарання зі звільненням на підставі ст.75 КК України від його від-бування з випробуванням 3 роки)	<i>Mamdani</i>	3,25	-0,75
		<i>Sugeno</i>	2,75	-1,25

Алгоритм Mamdani для перших чотирьох справ, що представлені в табл. 5, згенерував міру покарання, що, або співпадає, або є суворішою на 0,25 року, ніж було винесено за вироком суду. Алгоритм Sugeno в цих випадках показав абсолютне відхилення від -0,4 до 0 року, тобто зменшуючи термін позбавлення волі.

Для двох останніх справ з табл. 5 обидва алгоритми Mamdani та Sugeno згенерували більш м'яке покарання в порівнянні зі строком позбавлення волі за рішенням суду. Це пояснюється впливом більш складного змісту вироку, що містить посилання на інші статті КК України. Зменшити або уникнути такої розбіжності можливо ускладненням моделі (2) додатковим виходом Condition, що передбачений у загальній моделі (1).

При обґрунтуванні вибору алгоритму нечіткого виведення необхідно брати до уваги можливі похибки у генерованих рішеннях та трудомісткість обчислень за обраним алгоритмом.

На рівні проведеного експерименту обидві системи нечіткого логічного виведення Mamdani та Sugeno показали адекватність генерованих результатів вироків без видимої переваги одного з алгоритмів. Але лінійність функцій виходу алгоритму Sugeno забезпечує більш просту настройку системи нечіткого виведення та дає вираш з обчислювальної точки зору.

Обидві системи прореагували однаково на наявність додаткових умов, що на практиці підтвердилось пом'якшенням вироку суду. Це

є підтвердженням необхідності введення якісних, нечислових параметрів на вхід системи. Введення таких змінних більш зручно відбувається в системі нечіткого логічного виведення за алгоритмом Mamdani.

Наступні кроки з вдосконалення СППР у судах продиктовані необхідністю розробки уніфікованих правил ініціалізації вхідних змінних, що дозволять виконувати налаштування нечітких продукційних моделей для отримання певного справедливого вироку у випадку справ, що мають склад злочину за кількома частинами однієї статті та/або кількома різними статтями КК України.

Практична цінність даної роботи полягає в тому, що застосування методів нечіткого логічного виведення є потенційно продуктивним для підтримки прийняття справедливих судових рішень, оскільки дозволяє наблизитись до формалізації самого поняття справедливо-го судового рішення. Вбачається перспективним впровадження такої підсистеми в систему Єдиної судової інформаційно-телекому-нікаційної системи (ЄСІТС) — «Електронний суд».

Список використаних джерел

1. Кримінальний кодекс URL:<https://zakon.rada.gov.ua/laws/show/2341-14>.
2. Bakurova, A. and Tereschenko, E. and Filei, Y. and Pasichnyk, M. and Ropalo, H.: Modeling of decision making ontology. Proceedings of the 3rd international conference on computational linguistics and intelligent systems (colins-2019). Vol.1: Main Conference, Kharkiv, Ukraine, April 18-19, 2019, p. 197-207.
3. Bakurova, A., Pasichnyk, M. and Tereschenko, E. Fuzzy Modeling of Verbal Information for Production Systems. Innovative Technologies and Scientific Solutions for Industries. 2019, №4(10), P.5-13 DOI: <https://doi.org/10.30837/2522-9818.2019.10.005>.
4. Anna Bakurova, Mariia Pasichnyk, Elina Tereschenko and Yurii Filei Production model for administration of judicial decisions in the case of theft // 8th International Conference «Monitoring, Modeling and Management of Emergent Economy, May 22-24, 2019, Odessa.
5. Anna Bakurova, Mariia Pasichnyk, Elina Tereschenko, Yurii Filei Formalization of Ukrainian-Language Content for Fuzzy Product in Court // Proceedings of the 4th International Conference on Computational Linguistics and Intelligent Systems (COLINS 2020). Volume I: Main Conference, Lviv, Ukraine, April 23-24, 2020. CEUR Workshop Proceedings 2604, CEUR-WS.org 2020 P. 428-441.
6. Бакурова А.В., Пасічник М.С., Терещенко Е.В., Філей Ю.В. Моделювання оцінки особи винного для системи нечіткої продукції

в суді // Комбінаторні конфігурації та їхні застосування: Матеріали XXII Міжнародного науково-практичного семінару імені А.Я. Петренюка (Запоріжжя - Кропивницький, 15-16 травня 2020 року) / за ред. Г.П. Донця – Кропивницький: ПП «Ексклюзив-Систем», 2020. С. 27-30.

7. Єдиний державний реєстр судових рішень. URL: <http://www.reyestr.court.gov.ua/Page/1>.

8. Academic version of MATLAB <https://uk.mathworks.com/campaigns/products/trials.html>.

Бочарова Н. В.,

д.ю.н., професор

кафедри права, політології та міжнародних відносин університету імені Альфреда Нобеля

ПРОБЛЕМИ ГУМАНІЗАЦІЇ ЗАКОНОДАВСТВА З ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В УМОВАХ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Проблема гуманізації законодавства з інтелектуальної власності постала у зв'язку з тим, що розвиток інформаційних технологій у 1980-х і, особливо, у 1990-ті роки визначив не тільки економічний потенціал сучасних держав, але і обумовив суспільно-політичні процеси, які безпосередньо впливають на права людини. Вироблення нових норм регулювання у сфері інтелектуальної власності повинно перш за все здійснюватися з урахуванням нових факторів суспільного розвитку, обумовлених виникненням Інтернету як технології, яка в найбільшій мірі втілює перехід людства до інформаційного суспільства.

В цьому плані звертає на себе увагу цікавий і, на наш погляд, недооцінений у нас документ *soft law*, створений у результаті діяльності *Міжурядової ради по реалізації спеціальної Програми ЮНЕСКО «Інформація для усіх» (UNESCO Information for All Programme — IFAP)*. Програма була розпочата у 2000 році, і влітку 2001 року прийнята на 31-й сесії Генеральної конференції ЮНЕСКО. Концепція Програми — це уявлення про світ, у якому кожен має доступ до інформації, важливої для нього, і має можливість і необхідні навички використання отриманої інформації для вирішення життєво важливих проблем і побудови більш досконало-

го суспільства². Планування та реалізація в рамках *Програми* здійснюється під керівництвом Міждержавної ради, в яку входять 26 держав-членів ЮНЕСКО, обраних Генеральною конференцією ЮНЕСКО. Метою Програми «Інформація для всіх» є: сприяння міжнародному розгляду та обговоренню етичних, правових і соціальних проблем, що породжуються інформаційним суспільством³.

Спеціальна Робоча група *Програми «Інформація для всіх» у 2011 р. підготувала Кодекс етики для інформаційного суспільства*, який був представлений на розгляд 36 сесії Генеральної конференції ЮНЕСКО⁴.

Кодекс етики є безпосереднім результатом роботи міжурядового органу і включає в себе підсумки ряду регіональних нарад і конференцій ЮНЕСКО з питань інформаційної етики. ЮНЕСКО співпрацювала з основними зацікавленими сторонами та науковим співтовариством з метою проведення досліджень і підвищення рівня інформованості в області етичних аспектів інформаційного суспільства. Кодекс етики не має обов'язкового характеру, він звернений до всіх зацікавлених сторін інформаційного суспільства та суспільства знань. У 18 пунктах (статтях) викладено ряд універсальних цінностей і керівних принципів, які у подальшому пропонуються використовувати урядам у правотворчості та правозастосуванні.

Етичні норми інформаційного суспільства встановлюються на основі *Загальної декларації прав людини* і включають в себе право на свободу вираження поглядів, право на загальний доступ до інформації, зокрема, до інформації, яка відноситься до суспільного надбання, право на освіту та право на участь у культурному житті. Однією з найскладніших етичних проблем є проблема нерівності доступу до інформаційно-комунікаційних технологій (ІКТ) між різними країнами і між міськими і сільськими громадами всередині країни.

Особливу зацікавленість викликає *проблема інтелектуальної власності в інформаційному суспільстві*, розкрита у п. 17 документу⁵. Тут міститься своєрідна програма дій і методологічні настанови

² IFAP. Программа ЮНЕСКО Информация для всех. Информация для жизни. Организация Объединенных Наций по вопросам образования, науки и культуры. URL: <https://www.ifap.ru/ofdocs/unesco/program.htm>.

³ Про участь України у Програмі див.: Юрченко О.А. Реалізація Програми ЮНЕСКО «Інформація для всіх» в Україні. Бібліотекознавство. Документознавство. Інформологія. 2014. № 3. С. 66-71.

⁴ Генеральная конференция, 36-я сессия, Париж 2011 г. 36 С/49 10 октября 2011 г. Пункт 5.24 предварительной повестки дня. Кодекс этики для информационного общества, предложенный Межправительственным советом программы «Информация для всех». URL: <http://unesdoc.unesco.org/images/0021/002126/212696r.pdf>.

⁵ Code of Ethics for the Information Society. The Intergovernmental Council of the Information for All Programme of UNESCO. URL: <http://unesdoc.unesco.org/images/0021/002126/212696e.pdf>.

щодо визначення особливої ролі інтелектуальної власності на якісно новому етапі розвитку людства. Аналіз дозволяє виділити такі логічні компоненти:

1. Інтелектуальна власність на твори в цифровому середовищі повинна бути предметом регулювання і захисту з боку законодавства про право інтелектуальної власності.
2. Несанкціоноване копіювання та розповсюдження матеріалів, що охороняються авторським правом, не повинно допускатися.
3. Слід підтримувати правові рамки, що дозволяють власникам інтелектуальної власності ділитися своїми знаннями і поширювати їх з метою заохочення відкритого доступу до знань і сприяння творчій діяльності.
4. Застосування міжнародних конвенцій в сфері інтелектуальної власності має ґрунтуватися на справедливій збалансованості між інтересами правовласників і громадськості.

У *Кодексі* зазначено, що держави-члени несуть відповідальність за забезпечення інклюзивного, актуального і сучасного правового середовища для розвитку інформаційного суспільства. Таке середовище може бути сформоване і за допомогою конституційних приписів при створенні нових законодавчих актів, пов'язаних з реаліями інформаційного суспільства, в тому числі з права інтелектуальної власності.

На регіональному рівні формування оновленого каталогу прав людини в інформаційному суспільстві позначене в новітніх документах Ради Європи.

Вплив інформаційно-комунікаційних технологій на права людини і цінності демократії вперше був розглянутий на конференції Ради міністрів РЄ у грудні 1997 р. у Греції. Створений за її рішенням *Комітет експертів РЄ по інформаційному суспільству* розробив документ, який було прийнято у травні 2005 р. під назвою «*Декларація Комітету міністрів про права людини і верховенство права в інформаційному суспільстві*»⁶.

Основна ідея *Декларації* полягає в тому, що такі цінності, як права людини, демократія, верховенство права, суспільна згода і довіра між людьми зберігаються при застосуванні інформаційно-комунікаційних технологій (ІКТ).

Особливу увагу звертає на себе п. 6 *Декларації Комітету міністрів* «Захист власності». В ньому підкреслено, що у сфері ІКТ пи-

⁶ Declaration on Human Rights and the Rule of Law in the Information Society. CM(2005) final. Publ. N060508/h/2). URL:www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/Declaration-Information Society/011_DeclarationFinal %20 text _en.asp.

тання захисту власності виникають перш за все по відношенню до *інтелектуальної власності*, такої як патенти, торговельні марки і авторські права.

Звернення Ради Європи до питань захисту інтелектуальної власності у зв'язку з розвитком інформаційного суспільства не випадкове. Зі зміною функції знання в цивілізації ХХІ століття різко зросла цінність інтелектуальної власності, яка невід'ємна від інформаційної революції. Вона регулює процеси творчої, культурної і економічної практики, забезпечує охорону прав на об'єкти творчої діяльності, стає основним предметом управління і набуває характеру інституційного явища, структури якого є провідними в інформаційному суспільстві, як колись, у минулому, структури власності на засоби виробництва.

Декларація Комітету міністрів Ради Європи підкреслює діалектику взаємовідносин інтелектуальної власності і ІКТ. Останні, з одного боку, забезпечують нові можливості доступу до об'єктів права інтелектуальної власності, а, з іншого боку, можуть сприяти порушенню прав інтелектуальної власності і перешкоджати переслідуванню правопорушників. Між тим, відсутність ефективних заходів захисту інтелектуальної власності перешкоджає інноваціям і творчості, скорочує інвестиції. В документі сформульоване важливе методологічне положення щодо державної політики відносно інтелектуальної власності. Така політика повинна реалізовувати дві цілі: по-перше, забезпечити захист інтелектуальної власності відповідно до положень міжнародних угод, по-друге, у той же час повинен бути збережений вільний доступ до інформації, яка є суспільним надбанням, та відкинуті спроби обмеження такого доступу і використання такої інформації. Держави-члени Ради Європи повинні намагатися відносити політичну, соціальну, економічну та дослідницьку інформацію до суспільного надбання, розширюючи тим самим загальний доступ до життєво важливій інформації. Одночасно *Декларація* наголошує на необхідності підтримки положень ст. 10 («Правопорушення, пов'язані з порушенням авторських і суміжних прав») *Конвенції Ради Європи про кіберзлочинність*⁷, яка рекомендує ввести кримінальне переслідування за порушення авторських і суміжних прав в Інтернеті.

Конвенція про кіберзлочинність заснована на принципах Європейської Конвенції про захист прав людини і основоположних свобод. У ній передбачені умови і гарантії забезпечення прав людини у випадках кримінального переслідування, а також збереження прав

⁷ Конвенція про кіберзлочинність (ETS №.185). URL: http://zakon.rada.gov.ua/laws/show/994_575.

на свободу вислову думок і право людини на приватне життя. Важливе методологічне значення мають положення про боротьбу з кримінальними порушеннями прав інтелектуальної власності у кіберпросторі. У ст. 10 Конвенції зазначено, що кримінальна відповідальність не повинна застосовуватися до порушення будь-яких моральних прав авторів, передбачених міжнародними угодами. Крім того, кожна Сторона може залишити за собою право не встановлювати кримінальну відповідальність у обмежених випадках, за умови існування інших ефективних засобів впливу і за умови того, що таке застереження не порушує міжнародних зобов'язань Сторони відповідно до міжнародних документів, на які містяться посилання.

Таким чином, у првозахисних документах на рівні Ради Європи підтверджена можливість застосування кримінальних процедур і покарань у випадках навмисного порушення прав інтелектуальної власності у комерційних масштабах, передбачена у розділі 5 ст. 61 *Угоди про торговельні аспекти прав інтелектуальної власності* (*Угода ТРІПС*), підписаної в рамках Світової організації торгівлі у 1994 р.

Ідеї *Декларації Комітету міністрів РЄ про права людини і верховенство права в інформаційному суспільстві* отримали подальший розвиток в інших документах цієї міжнародної організації. Так, у 2014 р. була прийнята *Рекомендація СМ/РЕС(2014)6 Комітету міністрів Ради Європи державам-членам щодо посібника з прав людини для інтернет-користувачів*. В ній визначена можливість «вільно створювати, повторно використовувати і поширювати Інтернет-контент із повагою до права на захист інтелектуальної власності, в тому числі авторського права»⁸. Таким чином наголошується, що великомасштабні перетворення, пов'язані із впровадженням інформаційно-комунікаційних технологій практично у всі сфери життя, повинні контролюватися і спрямовуватися в інтересах суспільства і людей. Інтернет впливає на традиційну систему регулювання авторського права в плані переходу від регулювання зафіксованих на матеріальних носіях прав до захисту інформації, але шляхи регулювання нових телекомунікаційних технологій залишаються в межах використання інтелектуальної власності.

Інформаційно-комунікативні технології змінюють якість життя людини у всіх площинах. Вони впливають і на зміну об'єктного складу права інтелектуальної власності. Так, інформаційні технології сприяли появі нового класу творів — мультимедійних, які створені в

⁸ Рекомендація СМ/РЕС(2014) 6 Комітету міністрів Ради Європи державам-членам щодо посібника з прав людини для інтернет-користувачів (ухвалена Комітетом міністрів 16 квітня 2014 року на 1197-му засіданні постійних представників міністрів). URL: <https://rm.coe.int/16802e3e96>.

цифровій формі, використовуються на комп'ютерах і для створення яких також завжди необхідна комп'ютерна техніка. Прикладом можуть бути електронні книги, що представляють собою версії книг в електронному (цифровому) форматі. Такі книги мають ряд переваг у порівнянні з традиційними паперовими: компактність, спеціальні можливості (змінювати шрифт, переходити до будь-якого розділу), дешевша вартість тексту, доступність, екологічність, зручність використання. Деякі сучасні автори художніх творів хоча б на початку своєї кар'єри знаходять в цьому альтернативу традиційному виданню книг, оскільки такий спосіб не передбачає витрат на оплату видавництва, а також дозволяє знайти значно більшу кількість читачів, яким не потрібно купувати книги. Крім того, такі публікації в цифровому контенті забезпечують більш тісний взаємозв'язок між автором і його читачами, полегшують можливість особистого спілкування. При цьому авторські права зберігаються — в програмне забезпечення для виробництва закладені функції, що перешкоджають несанкціонованому копіюванню даних з електронної книги⁹.

У ряді країн вже існують громадські організації і рухи, які виступають за обмеження прав розробників комп'ютерних програм в інтересах людини і суспільства. Як приклад можна привести створену у 1985 році програмістом, колишнім співробітником лабораторії штучного інтелекту Массачусетського технологічного інституту Річардом Столлменом організацію *Фонд вільного програмного забезпечення*. Вона розробляє ліцензії, що створюють альтернативні механізми захисту авторських прав¹⁰. Найбільш значущим внеском Фонду в ідеологію охорони інтелектуальної власності є принцип, який отримав назву «копілефт». Суть його полягає в тому, що так званою публічною ліцензією передбачається передача всім особам, які прийняли ці умови ліцензії, того ж набору прав щодо твору, який ліцензія залишає за самим автором. Цей принцип активно застосовується розробниками комп'ютерних програм з відкритим вихідним кодом. В каталозі вільного програмного забезпечення, що складається Фондом вільного програмного забезпечення спільно з ЮНЕСКО, значиться понад 5000 програм. На умовах «копілефтної» ліцензії, наприклад, існує і розвивається, і найбільша онлайн-енциклопедія «Вікіпедія»¹¹. свою позицію Столлмен аргументує посиланнями на Консти-

⁹ Конюшкіна Ю.А. Права человека на свободу творчества в Сети. *Вестник Московского финансово-юридического университета*. 2013. № 4. URL: <https://cyberleninka.ru/article/n/prava-cheloveka-na-svobodu-tvorchestva-v-seti>.

¹⁰ Столлман Р.М. Говорите, «интеллектуальная собственность»? Соблазнительный мираж. URL: <http://linuxrsp.ru/artic/not-ipr.html>.

¹¹ Williams S. Free as in Freedom: Richard Stallman's Crusade for Free Software. March 2002. URL: <https://www.oreilly.com/openbook/freedom>.

туцію США і права людини. «Коли створювалася Конституція Сполучених Штатів», — пише він, — думка про те, що автори мають право на монополію відтворення, пропонувалася — і була відкинута. Замість цього засновники нашої держави взяли іншу концепцію авторських прав — концепцію, в якій перше місце займає суспільство. Авторське право в Сполучених Штатах призначене служити інтересам користувача; воно дає переваги видавцям і навіть авторам не заради цих осіб, а тільки як стимул для зміни їхньої поведінки...»¹².

Один з найуспішніших прикладів нового механізму пов'язання інтересів правовласників і громадян-споживачів інтелектуальних продуктів — це створена у 2001 р. професором Стенфордського університету Лоуренсом Лессігом некомерційна організація Creative commons. Ця організація ставить перед собою мету сприяти вільному поширенню інформації, і для цього її фахівці розробляють тексти юридично значущих ліцензій, що дозволяють власникам авторських прав передати деякі з прав на свої твори громадськості і в той же час зберегти за собою інші права. Ставлячи замість звичайного авторського знака © (Copyright) знаки CC (Creative commons), автор включається в міжнародне творче співтовариство, яке відкриває можливість використовувати сучасні досягнення культури і науки.

У світі існують десятки правозахисних організацій, які борються за відкритий Інтернет та вільний доступ людей до знань. Найбільш відомі і впливові з них *Будапештська ініціатива відкритого доступу*, *План S* (ініціатива відкритого доступу до наукових публікацій), *IP Justice*, *Електронна інформація для бібліотек (eIFL)*, *Європейський фонд вільного програмного забезпечення (FSFE)* та інші. З кожним роком росте підтримка Open Access — це міжнародний академічний рух, спрямований на забезпечення безкоштовного, швидкого, постійного, повнотекстового доступу до навчальних і наукових матеріалів в мережі Інтернет. Публікації відкритого доступу можна вільно читати, завантажувати, копіювати, поширювати, друкувати, використовувати в навчальних та дослідницьких цілях, за умови коректності посилання на автора.

У жовтні 2003 р. була проголошена *Берлінська декларація про відкритий доступ до наукових і гуманітарних знань*. Академічна спільнота, неурядові організації та уряди кількох країн запропонували проєкт міжнародного договору про доступ до знань (*Access to Knowledge Treaty — A2K treaty*)¹³. У ньому наголошується на свобо-

¹² Столлмен Р. Пересмотр системы авторских прав: общество должно преобладать. Oregon Law Review. Spring 1996 (переклад статті по версії 03.03.2000). URL:<http://www.gnu.org/philosophy/reevaluating-copyright.ru.html>.

¹³ Structure of an Access to Knowledge Treaty. The KEI intervention at SCCR 38, on copyright limitations and exceptions. URL: <https://www.keionline.org/30279>

дах, а не на обмеженнях режимів інтелектуальної власності, і йдеться про доступ до інформації, освіти, ресурсів для навчання, досліджень, культури та розваг. Пропонується новий погляд на винятки та обмеження в авторському й патентному праві, зокрема для бібліотек, сліпих і людей зі слабким зором, дистанційної освіти; на відкритий (вільний) доступ до дослідницької літератури; на засади реагування на зловживання правами, зокрема контроль за практикою підриву вільної конкуренції у договірному ліцензуванні; на системи управління цифровими правами та системи застереження від неправомірного подолання технічних засобів захисту цифрових прав; на бази даних патентів, які стосуються суспільного добробуту; на вільне (відкриті) програмне забезпечення та відкриті (прозорі) стандарти.

У преамбулі проекту *Договору про доступ до знань* говориться: «Інтелектуальні монополії, такі як авторське право та патенти, створювалися як засоби для стимулювання творчості для суспільного збагачення. Нині ця система дедалі більше схиляється у бік захисту правовласників. А проблема в тому, що для творчості й інновацій ми потребуємо спиратися на чинне знання. Спіратися на нього стає дедалі дорожче, а отже, залишається менше підґрунтя для творчості та інновацій. *Договір про доступ до знань* поверне авторське право та патентне право на службу суспільному збагаченню, а не вузькому колу правовласників»¹⁴.

Перераховані вище рухи і ініціативи ставлять питання про гуманізацію інтелектуальної власності і базують свої вимоги на положеннях міжнародних правозахисних документів, де зафіксовані права на свободу вираження думок і свободу слова (ст. 19 *Загальної декларації прав людини*, ст. 10 *Конвенції по захист прав людини і основоположних свобод*, ст. 19 *Міжнародного пакту про громадянські і політичні права*). З початком 21 століття з'являються нові документи так званого м'якого права, щодо свободи інформації в Інтернеті (наприклад, Декларація про свободу спілкування в Інтернеті Ради Європи, прийнята 28 травня 2003 р.¹⁵) вони будуть все в більшій мірі впливати на законодавство з інтелектуальної власності.

¹⁴ «Access to Knowledge» treaty, as proposed in the World Intellectual Property Organization (WIPO). Development Agenda. URL: <https://www.opensocietyfoundations.org/events/meeting-access-knowledge-treaty>.

¹⁵ Декларація о свободе обмена информацией в Интернете (принята Комитетом Министров Совета Европы от 28 мая 2003 г. на 840-ом заседании заместителей Министров. URL: <http://base.garant.ru/71036560>.

Буров О. Ю.,
*доктор технічних наук, старший дослідник
провідний науковий співробітник
НДІ інтелектуальної власності НАПрН України*

КІБЕРБЕЗПЕКА В МЕРЕЖАХ ПРИЙНЯТТЯ РІШЕНЬ: СТАН І ТЕНДЕНЦІЇ (досвід США)

Важливою особливістю умов, в яких опинилась економіка людства [1], є стрімкий перехід до цифрового бізнес-середовища [2], що починає суттєво перетинатися з навчальним середовищем (не тільки в навчанні економістів, але й інших дисциплін і навіть шкільних предметів), яке також вибухоподібно перейшло до цифрового простору, практично не маючи для цього розробленого методологічного та технологічного фундаменту [3]. Цифровізація навчання та бізнес-процесів, з одного боку, були викликані пандемією COVID-19 і введенням карантинних обмежень на життя та діяльність людей усьому світі, а з іншого — супроводжується стрімким зростанням кіберзагроз як для бізнесу, так і для окремої людини [4], оскільки цифрове середовище — це найбільш сприятливе та «природне» середовище для кіберзлочинності, яка починає переходити зі стану «зовнішньої», нелегальної, діяльності у стан відкритого мережного бізнесу [5].

Постановка проблеми.

Безпрецедентна криза, спричинена COVID-19, прискорює актуальність переходу світової економіки до впровадження критеріїв гнучкості, пристосованості та трансформації. Галузеві структури та бізнес-моделі перестають ефективно працювати, а цифровізація економіки стрімко прискорюється. Проте всебічна цифровізація життя потребує не просто цифрової грамотності, а широких цифрових знань і готовності учитися та працювати в цифровому світі [6], зокрема в дистанційному форматі [7]. Проте слід зауважити, що дистанційно працююча людина опинилась поза межами корпоративного захисту, а практично будь-яка виробнича інформація, як і людський капітал, в таких умовах стають значно вразливішими і потребують відповідних методів кібербезпеки [8]. В той же час, кількість кібератак на працівників, які працюють дистанційно, за час пандемії зросло на 70 %, у т.ч. вимагання — на 600 % [9]. Тобто атаки на критичну інфраструктуру держави значно доповнюються атаками на творців і носіїв інтелектуального капіталу, що потребує зміни не тільки технологій захисту, але й самої парадигми кібербезпеки [10].

Аналіз останніх досліджень і публікацій.

Криза, викликана пандемією COVID-19, суттєво вплинула на робоче середовище: фізичне дистанціювання, покращений досвід роботи з інформаційно-комунікаційними технологіями (ІКТ), а також переналаштовані виробничі та постачальні лінії, щона часі стали нормою [11]. Відбувається різке зростання віддалених операцій на дому або необхідність персоналу виконувати нові завдання, дотримуючись суворих додаткових правил безпеки життєдіяльності [12]. Водночас із новими труднощами виникають нові можливості для інновацій в технологіях та організації бізнесу [13], проте ці зміни потребують змінне тільки кваліфікації персоналу, але його готовності та здатності продуктивно працювати із забезпеченням життєстійкості кіберпростору діяльності [14]. Кібер-ризик є головним питанням для керівників підприємств, які розуміють, що цей виклик стане ще важливішим, оскільки компанії перекладуть більшу частину своїх функцій на цифрову, безпосередню взаємодію споживачів, обмін даними розшириться, а агенти загроз спричиняють все серйозніші зриви у бізнесі [15] та соціальній сфері [6; 16]. Але в той час як компанії намагаються запобігти дорогим порушенням системи, боротися з хакерством, фішингом, програмами-вимагателями та іншими загрозами для бізнесу, часто роблячи це з обмеженими ресурсами, багато хто з осіб, які приймають рішення (ОПР), досі не застосували ефективних інструментів для вимірювання потенційного фінансового впливу конкретних ризиків, з якими вони стикаються, та тому не можуть визначити шляхи усунення загроз або пом'якшення їх дії [17], незважаючи на те, що існують компанії, які професійно на основі досвіду можуть надавати відповідні послуги як безпосередньо, так і шляхом інформаційних консультацій.

Мета статті. Аналіз актуальних підходів до забезпечення кібербезпеки ведення бізнесу в кіберпросторі в умовах мережної діяльності на прикладі США.

Результати дослідження.

Найбільший досвід із рішення зазначених проблем має країна з найбільш потужною економікою, яка виявилася найбільш підготовленою до захисту бізнесу та в якій вже є низка компаній з кваліфікованими та досвідченими фахівцями у сфері кібербезпеки, розуміючими необхідність нових підходів до об'єктивного оцінювання ризиків і виявлення та знешкодження кіберзагроз.

За оцінками HarvardBusinessReview (HBR) AnalyticServices, «просто знати, що існують кібер-ризик, недостатньо. Потрібно знати наскільки вагомий кожен ризик. Зокрема, слід кількісно визначити варіюючи фінансові ризики для конкретної компанії через різні кі-

берзагрози. Через певний час сильного фінансового тиску внаслідок економічних наслідків пандемії, кількісна оцінка кібер-ризиків може принести велику вигоду: вона дозволяє досягти найбільшої ефективності зусиль, оцінивши ймовірний прибуток — з точки зору зменшення ризику — від різних кібер-інвестицій» [17, с. 2].

Максимізація рентабельності інвестицій в кібербезпеку стає важливішою в міру просування ініціатив цифрової трансформації. У той же час, цифровізація бізнес-процесів та інтелектуальної власності збільшує кількість активів, які потребують захисту від кіберзагроз. Недарма наглядові ради компаній та C-suite все частіше вимагають кількісної оцінки кібер-ризиків. Вони хочуть мати на озброєнні точні та надійні оцінки ймовірних витрат, пов'язаних з різними кіберзагрозами.

Виграш виходить за рамки більш ефективної (і більш економічно ефективної) кібербезпеки. Коли бізнес може кількісно оцінити кібер-ризик, він може краще визначити пріоритети та захистити нові продукти та швидше підготувати їх до виходу на ринок. За дослідженнями аналітиків HBR, серед ризиків для бізнесу 74 % ОПР (із 168 опитаних, 46 % з них представляли найвищий рівень менеджменту компаній з чисельністю більше 10 000 працівників, 38 % — компаній з чисельністю від 1000 до 9 999 працівників) вважають найбільш важливими кібер-ризиком (для порівняння: два роки тому такої думки були 67 %). Причому 55 % респондентів вважають, що найбільш вагомою причиною кількісної оцінки ризиків є необхідність постійно оцінювати план ризиків та пріоритети щодо змін бізнес-цілей [17, с. 5]. Головною особливістю оцінок кібер-ризиків бізнесменами є вираження ризиків в перерахунку на долари та центи: грошова вартість кібер-пов'язаних відключень, втрата клієнтів, втрата співробітників та втрата продуктивності, коли дефіцитні ресурси потрібно переорієнтувати на відповідь на порушення чи загрозу. Це робить кількісну оцінку кібер-ризиків важливою частиною стратегії цифрового зростання. Кількісно визначений кібер-ризик — це керований кібер-ризик. І *de facto*, і *de jure* оцінювання кібер-ризиків стає складником цифрової системи підтримки прийняття рішень.

Найкращий захист — це запобігання правопорушенню. Що стосується кібербезпеки, державні установи борються за побудову, управління та підтримку безпеки власного ІТ-середовища, а також вирішення проблеми дефіциту кібер-працівників. За даними Центру стратегічних та міжнародних досліджень, глобальний дефіцит робочої сили в галузі кібербезпеки досягне 1,8 мільйона вакансій до 2022 р. [18]. Ключові урядовці США вважають, що цей дефіцит буде проблемою національної безпеки, якщо його вчасно не вирі-

шити. Щоб допомогти автоматизувати кібербезпеку та заповнити нестачу кваліфікованих фахівців, системні інтегратори, такі як Microsoft, Verizon та AT&T, зараз використовують програми Enterprise-IT-as-a-Service або Cybersecurity-as-a-Service для державних установ, відповідаючи на виклики кібер-злочинності [6].

Суттєвим для розуміння можливих дій щодо зменшення негативної дії ризиків є аналіз видів кібер-загроз і тактик можливої протидії ним з огляду на ситуацію, що склалася зі швидким переходом бізнесу та соціальних процесів (здоров'я, освіта тощо) у цифровий простір. Показовою з цих позицій є діяльність найбільш впливових спеціалізованих компаній США (які працюють насамперед не з технічними аспектами кібербезпеки як великі ІТ компанії [19], а з орієнтацією на людський капітал), працюючих у сфері кібербезпеки на федеральному та регіональному рівні США.

Досвід федеральної компанії Fidelis. FidelisCybersecurity є провідним постачальником рішень щодо виявлення загрози, полювання та реагування на них. У лютому 2020 р. американське кіберкомандування оголосило компанію переможцем у заході швидкого прототипування DreamPort.

FidelisCybersecurity пропонує аналіз мережевого трафіку, цифрову криміналістику та реагування на інциденти як окремі рішення або як інтегровану уніфіковану платформу для виявлення, пошуку та реагування на найсучасніші загрози [20]. Найбільш важливі можливості для уряду та бізнесу, що надають вирішальну перевагу:

- Проактивні можливості завдяки мережі Fidelis для забезпечення постійної видимості кібер-місцевості клієнта (кіберпростір та кібер-ресурси, які мають критичне значення для успішної діяльності);
- Оманливі (*deceptive*) контрзаходи за допомогою FidelisDeception, щоб зменшити перевагу зловмисників, змінивши кіберсередовище сотнями або тисячами пасток;
- Запобігання втраті даних для забезпечення попереджувального захисту;
- Можливості реагування шляхом включення автоматичного виявлення, полювання на загрози, а також автоматизації розслідувань та реагування до початку дій, націлених на викрадення даних;
- Прогнозуючі можливості машинного навчання та штучного інтелекту для виявлення аномалій, визначення ймовірності компромісу та допомоги в аналізі метаданих під час пошуку відомих та невідомих загроз;

- Ретроспективні контрзаходи для аналізу інформації щодо загрози та забезпечення більшої видимості для фахівців з кібербезпеки.

Поверхня кібер-атак (задіяні мережеві ресурси) швидко розширюється і з розвитком технологій немає підстав очікувати, що ця тенденція сповільниться. Аналітики прогнозують різке збільшення використання хмарних технологій на підприємствах протягом наступних років і, відповідно, подальше впровадження мобільних технологій та технологій IoT. По суті, межі безпеки поширюються за межі інфраструктури традиційних приміщень на середовище постачальників хмарних послуг, де периметри (обмеження простору) більше не існують, і організації не можуть захищатись за допомогою однакових стратегій і тактик.

Платформа безпеки FidelisElevate® забезпечує організаціям видимість, можливість аналізу і контролю мережі і кінцевих точок, необхідні для управління захистом від сучасних загроз і для запобігання вторгнень. Засноване на запатентованій платформі FidelisElevate®, рішення здатне бачити, вивчати і зупиняти поширення просунутих загроз в режимі реального часу, працюючи на сеансовому рівні, де і виникають сучасні загрози. Платформа FidelisElevate® складається з трьох основних компонентів:

- FidelisNetwork — потужна система виявлення вторгнень і захисту від витоків інформації.
- FidelisEndpoint — автоматична система виявлення, реакції на загрози і управління кінцевими точками — серверами і робочими станціями.
- FidelisDeception (*postbreachdetectionsystem*) — зменшує час виявлення спрямованих атак. Рішення дозволяє класифікувати всі мережеві ресурси, канали зв'язку і мережевої активності для створення профілю користувачів, служб і активів в мережі. Результатом буде мережевий профіль-пастка, в якому знаходяться всі активи, включаючи сервери, робочі станції, корпоративні IoT-пристрої і тіньові IT-ресурси.

Оскільки форми і засоби атак постійно удосконалюються, багато команд безпеки зрозуміли, що традиційний підхід моніторингу та реагування на попередження вже не є достатнім. Практика полювання на кіберзагрози продовжує викликати багато дискусій, оскільки організації продовжують шукати нові шляхи підвищення своїх оборонних можливостей. Натомість необхідний перспективний пошук зловмисників та своїх слабких місць, щоб запобігти ескалації витрат на відновлення після кібератаки. За аналогією з воєнними діями, поки люди брали участь у (кібер-)війні, найсильніші армії не

лише зосереджувались на потужних наступальних можливостях, але й активно патрулювали свою оборону, шукаючи ознаки нападу та методи вдосконалення. Давно є загальноприйнятою практикою постійно оцінювати свій стан безпеки на предмет невдач.

Зараз, коли поля бою постійно еволюціонує у сучасну кібер-місцевість, цей підхід також еволюціонував із сучасною хвилею мисливців за кіберзагрозами. Організації, які займаються питаннями безпеки, знають, що найсильніший захист більше не може позиціонувати себе як чисто реактивний. Натомість вони повинні шукати невиявлені загрози та ідентифікувати непередбачувані, перш ніж атака може розвинутися поза їх контролем.

Слід зауважити, що «полювання на загрози» (*threathunting*) — це не реакція на подію, не тестування на проникнення за допомогою команд RedTeam (це також методи захисту середовища за допомогою контрольованих наступальних вправ, проте оцінюється не можливість скомпрометувати об'єкт атаки, а встановити, наскільки він може бути скомпрометований, тобто пошкоджений). Ефективне «полювання на загрози» має 6 важливих елементів:

- проактивний (упереджувальний) характер,
- кероване гіпотезою,
- брати до уваги ретроспективний аналіз,
- дослідження, а не виявлення, тобто аналіз походження фактору ризику,
- виявлення артефактів і підозрілої діяльності,
- метою мисливця за загрозами має бути поєднання як виявлення артефакту та діяльності, так і постійного вдосконалення пасивної оборони.

Кінцевий результат «полювання на загрози» полягає у визначенні оптимальних дій щодо їх попередження, нейтралізації (наскільки це можливо), пом'якшення наслідків атаки та максимального швидке з мінімальними витратами відновлення бізнес-процесів після неї.

Важливим складником діяльності Fidelis Cybersecurity є постійний щомісячний моніторинг і аналіз змін на федеральному рівні, що відбуваються у сфері кібербезпеки. Такий аналіз виконується за різними напрямками, зокрема: тренди вразливостей компаній, тренди видів найбільш поширеного шкідливого програмного забезпечення, тренди видів найбільш поширеного шкідливого програмного забезпечення для електронної пошти, суб'єкти загроз, галузі діяльності. Наприклад, у жовтні найбільше потерпали від кібер-атак державний сектор та технології/виробництво (відповідно, 33 % і 29 % від загальної кількості атак) США (Рис. 1).

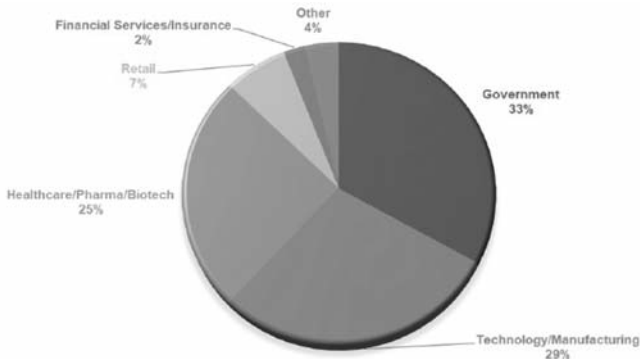


Рис. 1 Активність кібер-атак за галузями США у жовтні 2020 р. (за [21], с. 13)

Такий моніторинг дозволяє оцінювати не тільки види загроз, але й, у певній мірі, джерела загроз.

Досвід федеральної компанії PurpleSec. PurpleSec — це компанія з питань попереджуючих і захисних аспектів кібербезпеки, що спеціалізується на безпеці медичного страхування, сертифікації систем кіберзахисту та відповідних питаннях Міністерства оборони США.

Фахівці компанії вважають, що кібер-атаки та загрози постійно розвиваються, щодня виявляється 350 000 нових підписів шкідливих програм [22]. Проте незважаючи на те, що кібератаки та загрози тривають постійно, їх можна запобігти, знаючи про різні типи протоколів, експлойтів, інструментів та ресурсів, які використовуються зловмисниками. Крім того, знаючи, де і як слід очікувати атаку, можна гарантувати створення превентивних заходів для захисту систем.

Кібератаки виконуються зі зловмисним наміром, коли актор загрози намагається використати вразливість або слабкість у системі або окремих особах організації. Загрози атаки — викрасти, змінити, знищити, відключити або отримати доступ до несанкціонованого активу чи використовувати його. Втратами компанії при цьому стають гроші, дані або репутаційні втрати. «Кібератаки, погрози та вандалізм є небезпечною і зростаючою проблемою для бізнесу. Майже всі сучасні компанії потребують мережі комп'ютерів, серверів, принтерів, комутаторів, точок доступу та маршрутизаторів. Компанії також застосовують програмні засоби для впорядкування функцій, наприклад QuickBooks для ведення бухгалтерії» [22, с. 2]. Слід визнати, що хоча ці пристрої та додатки надають компанії ве-

личезну користь, вони також стають джерелом ризику. Достатньо лише, щоб один працівник натиснути на шкідливе посилання і воно може отримати доступ до всієї корпоративної мережі та заразити всю систему.

Враховуючи, що за час пандемії COVID-19 кіберзлочинність зросла на 600 % [9], важливим є аналіз змін у типах атак и небезпек. Серед найбільш поширених на сьогодні типів кібератак та погроз виділяють наступні чотири [23]:

- Атаки мережевої безпеки
- Атаки бездротової безпеки
- Атаки шкідливого програмного забезпечення
- Атаки соціальної інженерії.

Експерти PurpleSec виділяють три типи контролю безпеки — фізичний, технічний і адміністративний, які виконують три головні функції — превентивну, виявлення і коригуючу.

Проте, оскільки практика і аналіз ситуації у цифровому світі показали, що забезпечити 100 % захист неможливо, пропонується концепція пом'якшення ризику дії кіберзлочинців: прийняття ризику, запобігання ризику, перенесення ризику та його зниження.

Найважливішою рисою кіберзлочинності у 2020 р. стала соціальна інженерія як спроба маніпулювати користувачем з метою зниження його критичності мислення по відношенню до конфіденційності інформації, наприклад, такої як дані облікового запису користувача, проводка коштів або особиста інформація про клієнта. Ця форма кібератаки є однією з найпопулярніших для розгортання шкідливого коду в мережі. За останніми даними, 98 % кібератак використовують методи соціальної інженерії, тобто впливають націлені не на технічний або інформаційний ресурс безпосередньо, а на людську ланку, яка безпосередньо пов'язана з людським капіталом. І в цьому відношенні роль правових аспектів кібербезпеки суттєво зростає.

Список використаних джерел

1. Shaping the Future of Digital Economy and New Value Creation. 2020 World Economic Forum. URL: <https://www.weforum.org/platforms/shaping-the-future-of-digital-economy-and-new-value-creation>.

2. Reddy S., Morelix A. Companies now face an urgent choice: go digital, or go bust. 2020 World Economic Forum, 19 Oct 2020. URL: <https://www.weforum.org/agenda/2020/10/digital-transformation-or-bust>.

3. Memon Asif Saeed, Rigole Annika, Nakashian Taleen Vartan, Taulo Wongani Grace, Chßvez Cirenía and Mizunoya Suguru. COVID-

19: How prepared are global education systems for future crises? Innocenti Research Brief 2020-21. UNICEF Office of Research – Innocenti, Florence, Italy. 7 p. URL:<https://www.unicef-irc.org/publications/1138-covid-19-how-prepared-are-global-education-systems-for-future-crises.html>. Accessed: 02.12.2020.

4. Resetting the Future of Work Agenda: Disruption and Renewal in a Post-COVID World. White paper, October 2020. 2020 World Economic Forum. URL:http://www3.weforum.org/docs/WEF_NES_Resetting_FOW_Agenda_2020.pdf.

5. RaaS: Ransomware as a Service. URL: <https://zvelo.com/raas-ransomware-as-a-service/> Accessed: 05.12.2020.

6. LiC., andLalanF.The COVID-19 pandemic has changed education forever. This is how. URL: <https://www.weforum.org/agenda/2020/04/coronavirus-education-global-covid19-online-digital-learning>. Accessed 21.08.2020.

7. GuterresAntónio. The future of education is here. Launch of the policy brief: education during COVID-19 and beyond, United Nations. URL: <https://www.un.org/en/coronavirus/future-education-here>. Accessed: August 04, 2020.

8. Vigliarolo B. Employees new to working remotely are a security risk. Security, June 22, 2020. <https://www.techrepublic.com/article/employees-new-to-working-remotely-are-a-security-risk>.

9. 2020 Cyber Security Statistics. The Ultimate List Of Stats, Data & Trends. PurpleSec LLC. URL:<https://purplesec.us/resources/cyber-security-statistics>.

10. Биков В.Ю., Буров О.Ю., Дементієвська Н.П. Кібербезпека в цифровому навчальному середовищі. Інформаційні технології і засоби навчання. 2019. Том. 70. № 2. С. 313-331. URL:<https://journal.iitta.gov.ua/index.php/itlt/article/view/2876>. (<https://doi.org/10.33407/itlt.v70i2.2876>).

11. Manavi J. The Next Normal: Building resilience in the post-COVID-19 workspace. Observer research foundation. Oct 20. 2020. URL:<https://www.orfonline.org/expert-speak/next-normal-building-resilience-post-covid19-workspace>.

12. The Future of Jobs 2020. October 2020. 2020 World Economic Forum. URL:www.weforum.org. Accessed 02.11.2020.

13. Chearavanont S. How digitization and innovation can make the post-COVID world a better place. World Economic Forum. URL: <https://www.weforum.org/agenda/2020/08/how-digitization-and-innovation-can-make-the-post-covid-world-a-better-place>.

14. Pipikaite A., and Davis N. Why cybersecurity matters more than ever during the coronavirus pandemic. World Economic Forum.

URL: <https://www.weforum.org/agenda/2020/03/coronavirus-pandemic-cybersecurity.2020>.

15. Marozas L. We need to rethink cybersecurity for a post-pandemic world. Here's how. World Economic Forum. URL: <https://www.weforum.org/agenda/2020/08/rethink-cybersecurity-post-pandemic-world>.

16. Beware of criminals pretending to be WHO. World Health Organization. URL: <https://www.who.int/about/communications/cyber-security>.

17. Blaesing N. and Stauffenecker J. The Necessity of Cyber Risk Quantification. Harvard Business Review. Business Analytics. Nov 6, 2020. Harvard Business School Publishing. URL: hbr.org/hbr-analytic-services.

18. Hernandez K. The Future of Cyber Security – The Best Defense is an Impenetrable Offense. Fidelis Cybersecurity. Aug 18, 2020. URL: <https://fidelissecurity.com/threatgeek/network-security/the-future-of-cyber-security-the-best-defense-is-an-impenetrable-offense>.

19. Weinberg N. The 10 most powerful cybersecurity companies. CSO United States. URL: <https://www.csoonline.com/article/3531668/the-10-most-powerful-cybersecurity-companies.html?upd=1607377226733>. Accessed: 06/12/2020.

20. Deception, Confusion, Diversion: Altering your cyber terrain to gain tactical advantage. White Paper. Fidelis Cybersecurity. URL: <https://fidelissecurity.com/resource/whitepaper/deception-confusion-diversion-cyber-terrain/>. Accessed: 06/12/2020.

21. Threat Intelligence Summary. Fidelis Threat Research Team - 2020 October. Fidelis Cybersecurity. URL: <https://fidelissecurity.com/resources/?search=&report>. Accessed 07.12.2020.

22. Swanagan M. How To Prevent The Top Cyber Attacks In 2020 And Beyond. PurpleSec. URL: <https://purplesec.us/prevent-cyber-attacks>.

23. Swanagan M. The 3 Types Of Security Controls (Expert Explains). PurpleSec. URL: <https://purplesec.us/security-controls>.

Васильєв О. В.,

*к.т.н., патентний повірений, Асоціація
«Інформатіо-Консорціум», oleksii.vasyliiev@gmail.com,
ORCID: 0000-0002-2312-8838*

Чьочь В. В.,

*к.т.н., патентний повірений, Інформатіо,
victoria.choch@gmail.com,
ORCID: 0000-0001-9706-9570*

ТЕНДЕНЦІЇ РОЗВИТКУ ПАТЕНТНО-ІНФОРМАЦІЙНИХ СИСТЕМ ДЛЯ ЗАБЕЗПЕЧЕННЯ ПАТЕНТНИХ ДОСЛІДЖЕНЬ

Реферат. На основі опублікованих паспортних даних ряду патентно-інформаційних і патентно-аналітичних систем та практичного досвіду їх використання для патентно-інформаційного пошуку та патентного аналізу проведено порівняльний аналіз можливостей таких систем, як STNInternational, Patbase (Minesoft, UK), OrbitIntelligent(Questel), TotalPatent (Lexis-Nexis), PatentPulse/MateoPatent (Matheo-Software, FR), Lens, PatentScopetaEspacenet. В результаті проведеного аналізу виявлено певні тенденції розвитку та еволюції функціональних моделей таких систем.

Ключові слова: патентні дослідження, патентний пошук, патентний ландшафт, патентне цитування, STNInternational, PatBase, Questel, PatentPulse, Lens, Patentscope, Espacenet.

Діяльність у сфері інтелектуальної власності, зокрема при проведенні патентних досліджень та патентуванні, неможлива без використання різноманітних джерел патентної, науково-технічної, економічної, маркетингової та промислової інформації, починаючи з підготовки заявки на об'єкт права інтелектуальної власності (ОПІВ) і закінчуючи тривалим у часі менеджментом зареєстрованого ОПІВ. Майже кожна національна чи регіональна патентна установа має публічно-доступні бази даних з інформацією про подані заявки, зареєстровані патенти на винаходи, корисні моделі, промислові зразки, торговельні марки. З переліком таких баз даних можна ознайомитися на сайті ВОІВ (WIPO) [1], а також із аналогічним переліком на сайті Укрпатенту [2]. Більшість з таких систем обмежують свої функції лише простим (за кількістю пошукових атрибутів) інформаційним пошуком, який забезпечує встановлення факту реєстрації відповідного ОПІВ, наданням метаданих (бібліографічних даних), що описуються ОПІВ, повнотекстовими матеріалами (формула, опис, креслення тощо). Відомі публікації, присвячені порівнянню різних патентно-інформаційних систем, але

формат опису носив або загальний характер [3], або вивченню підлягали узагальнені функціональні моделі таких систем [4].

Термін «патентні дослідження» має різні за повнотою визначення та відповідне наповнення. Відправною точкою є діючий стандарт ДСТУ 3575-97 «Патентні дослідження. Основні положення та порядок проведення» [5]. Проте різні патентні установи і компанії роблять різні доповнення до тлумачення цього терміну, включаючи операції, які в Україні відносяться до патентно-кон'юнктурних досліджень.

Деякі десятки років тому виникли і успішно розвиваються інформаційні платформи, які забезпечують не тільки пошук відомостей про ОПІВ, але й забезпечують проведення комплексних (різнопланових) патентних досліджень.

В даній публікації аналіз буде зосереджено тільки на системах, які спеціалізуються на патентних документах (винаходи та корисні моделі).

Системи, що забезпечують пошук і дослідження інших об'єктів промислової власності (торговельні марки, промислові зразки) можуть бути предметом окремого аналізу.

Серед систем обраного класу необхідно відмітити такі патентно-пошукові системи (далі — патентні системи, або ПС): STNInternational [6], Patbase (Minesoft, UK) [7], DerwentInnovation (Clarivate) [8], OrbitIntelligence (Questel, FR), TotalPatentOne (Lexis-Nexis, USA), PatentPulse або Mateo-Patent (Matheo-Software, FR), а також безплатні системи Lens (Cambia, Australia), Espacenet (EPO, Austria), PatentScope (WIPO, Switzerland). Аналіз і дослідження можливостей цих систем дозволив сформулювати тенденції розвитку подібних систем та рекомендації по їх використанню. В даному дослідженні практично відсутні порівняльні дані для Derwent World Patent Index (DerwentInnovation) та Total Patent через те, що автори не мали доступу до системи протягом певного часу.

Сучасна інформаційно-пошукова/аналітична система для проведення патентних досліджень — це складна інформаційна платформа, яка забезпечує доступ через мережу Інтернет до великого масиву (деякі десятки мільйонів) патентних документів або патентних сімейств у реферативному, бібліографічному та/або повнотекстовому форматі, дозволяє виконувати повнофункціональний інформаційний пошук на основі логічних функцій булевої алгебри, методів семантичного пошуку та штучного інтелекту.

Такі системи характеризуються параметрами, які можна поєднати у функціональні сегменти:

- Сегмент 1. Інформаційне наповнення масиву документів;
- Сегмент 2. Інформаційна структура опису документів;
- Сегмент 3. Реалізація пошукового інтерфейсу;

- Сегмент 4. Методи фіксації результатів;
- Сегмент 5. Методи патентного аналізу;
- Сегмент 6. Методи візуалізації результатів патентного аналізу.

Аналіз тенденцій розвитку згаданих вище систем в даному дослідженні здійснений на основі параметрів саме по цих сегментах (див. Табл. 1–Табл. 6).

1. Інформаційне наповнення масиву документів

Основні параметри сегменту інформаційного наповнення ПС наведені у Табл. 1.

Таблиця 1.

Загальні характеристики ПС

Параметр	STN International	Mathéo / Patent - Pulse	PatBase	Questel	Espacenet	PatentScope	Lens	Примітка
Кількість документів, млн док.	125	~ 100	125	>100	>100	92	125.4	1,2
Кількість країн (ареал)	90	90 (?)	120	90(?)	90	68	8	
Тенденції зростання ареалу	Фікс.	Фікс.	Позитив	Фікс.	Фікс.	Позитив	Фікс.	
Аналіз патентних сімейств	Так	Так	Так	Так	Так ⁴	Ні	Так ⁴	
Сегментація (документ, сімейство, статус)	Так	Інтегр.	І н - тегр.	Так	Так	Так	Так	3
Данні прямого цитування	Ні	Так (?)	Так	Так	Так ⁴	Ні	Так	
Данні зворотнього цитування	Ні	Так	Так	Так	Так ⁴	Ні	Так	
Інтеграція з патентно-консолід. публікаціями	Так	Ні	Так	Так	Ні	Ні	Так	
Наявність аналітичних функцій та процедур	Так ³	Так	Так	Так	Ні	Так ⁴	Так ⁴	3,4
Наявність метрик оцінки патентів	Так	Так	Так	Так	Ні	Ні	Ні	
Наявність API	Ні	Ні	Так	Так	Так	Так	Так	
Наявність спеціалізованого програмного забезпечення	Так	Так (Mathéo - Patent)	Ні	Ні	Ні	Ні	Ні	

1. Дані аносовані на порталі системи.

2. Для системи STNInternational наведено дані по базі даних INPADOCDB. Система додатково включає біля 40 БД патентної спеціалізації.

3. Сегментація означає наявність окремої інформаційно-пошукової (аналітичної системи).

4. Обмежені можливості.

Список скорочень (Табл.1): Фікс. — фіксована; позитив. — позитивна тенденція; Інтегр. — інтегрована (система включає крім опису документів, дані по патентним сімействам та даним статусу документу (по реєстру); API — ApplicationProgramInterface (можливість імплементації системи в програмах власної розробки).

Зростання колекцій патентних документів є стабільною тенденцією більшості ПС за рахунок природного приросту зареєстрованих документів. Ретроспективне наповнення ПС за останні 5 років підійшло до точки насичення (на цей момент близько 125 млн док.) і можливе тільки за рахунок підключення патентних архівів нових країн (на цей момент в ПС фігурують близько 90 країн світу). Найбільше зростання на цей час демонструє PatentScore (WIPO) — поступово наздоганяючи систему Espacenet.

2. Інформаційна структура опису документів

Інформаційна структура записів ПС включає, як мінімум, основні інформаційні поля метаданих опису патентних документів (зареєстрованих патентів та опублікованих заявок). Окремі національні патентні БД та ПС відрізняються повнотою доступних для пошуку інформаційних полів стандарту INID.

Можливості патентного аналізу зростають при введенні до структури ПС інформаційних полів з повного переліку стандарту INID [16] та додаткових інформаційних атрибутів, які характеризують властивості ОПІВ (юридичний статус, чинність, дані прямого або зворотного цитування, реєстраційні коди суб'єктів патентування, тощо), або природу предметів винаходу (хімічна структура, послідовності ДНК, класифікаційних кодів патентної класифікації/ предметної сфери тощо). Система Patbase розробила і починає впроваджувати спеціальні патентні метрики, які характеризують якість патентного документу.

Давно минув еволюційний етап ПС, коли в патентну пошукову систему включалась окрема пошукова підсистема кодів патентної класифікації. Сучасні ПС, такі як, PatBase, Questelі навіть безплатні PatentScore та Lens вже включили таку систему в основний пошуковий інтерфейс.

Основні параметри, що характеризують інформаційні структури ПС представлені у Табл. 2.

Таблиця 2.

Порівняння інформаційної структури опису документів

Параметр	STN International	Patent-Pulse/Mathéo-Patent	PatBase	Questel	Espacenet	Patent Scope	Lens	Примітка
Наявність класифікатора IPC	Так	Так	Так	Так	Так	Так	Так	
Наявність класифікатора CPC	Так	Так	Так	Так	Так	Ні	Так	
Наявність спеціалізованих класифікаторів (хім., фарм. тощо)	Так	Ні	Так	Так	Ні	Так	Ні	
Наявність тезаурусу	Так	Ні	Так	?	Ні	Ні	Ні	
Наявність статусної інформації	Так	Так	Так	Так	Так	?	Так	
Кодифікація суб'єктів	Ні	Ні	Ні	Ні	Ні	Ні	Ні	Derwent Innovation - Так
Наявність індексації суб'єктів	Так	Ні	Так	Так	Ні	Ні	Ні	
Данні прямого цитування	Ні	Так (?)	Так	?	Так ⁴	Ні	Так	
Данні зворотного цитування	Ні	Так	Так	?	Так ⁴	Ні	Так	

3. Реалізація пошукового інтерфейсу

Все більше зусиль витрачається для переходу від примітивного пошуку за ключовими словами до, так званого, інтелектуального пошуку. Більшість національних патентно-пошукових систем обмежуються простим та віконним (QBE) інтерфейсом, інколи, з можливостями пошуку по повнотекстовим описам. Практично всі ПС з переліку цього дослідження, за виключенням Espacenet, реалізують всі можливості використання логічних та логіко-семантичних функцій. На даний момент лише системи PatentScope та Lens пропонують групу функцій семантичного пошуку на основі методів штучного інтелекту. Крім того, за останні три роки такі ПС як PatBase, Questel, PatentScope та Espacenet (частково) реалізували машинний переклад текстових інформаційних полів патентних документів з колекцій ПС. Результати порівняльного аналізу функцій пошукового інтерфейсу ПС представлені в Табл. 3.

Таблиця 3.

Порівняння функцій пошукового інтерфейсу різних ПС

Параметр	STN International	Patent-Pulse/Mathéo-Patent	PatBase	Questel	Espacenet	Patent Scope	Lens	Правитка
Повнотекстовий пошук	Так	Ні	Так	Так	Ні	Так	Так	
Пошук по полям (QVE-тип)	Так	Так	Так	Так	Так	Так	Так	
Реалізація фіксованих логічних операторів	Так	Так	Так	Так	Так	Так	Так	
Реалізація пошукової мови на основі булевої алгебри	Так	Так	Так	Так	Ні	Так	Так	
Реалізація семантичних операторів	Так	Ні	Так	Так	Ні	Так	Так	
Штучний інтелект — підбір синонімів ключових слів (в т.ч. різними мовами)	Ні	Ні	Так	Ні	Ні	Ні	Так	
Штучний інтелект — переклад інформаційних полів та текстів	Ні	Ні	Так	Ні	Так	Так	Так	
Штучний інтелект — пошук по подібності документів	Ні	Ні	Так	Ні	Ні	Ні	Ні	
Пошук по хімічним структурам або назвам	Так	Ні	Так	Так	Ні	Так	Ні	
Пошук по дереву патентної класифікації	Ні	Ні	Так	Ні	Ні	Ні	Ні	
Обмеження складності пошуку	Ні	Так, частково	Ні		Так	Ні	Ні	
Каскадний пошук	Так	Ні	Так	Так	Ні	Ні	Ні	

4. Методи фіксації результатів

Результати виконання інформаційного пошуку щодо ОПВ можуть бути збережені в рамках відповідної інформаційної системи у вигляді формули запиту або результатів пошуку, як масиву документів. Це основна можливість, яка дає змогу повернутися до поточного результату і продовжити дослідження через деякий час. На жаль, така можливість повністю відсутня в інформаційній пошуковій системі Укрпатенту або аналогічних безоплатних систем. У некомерційному секторі лише Espacenet та Lens пропонують обмежені можливості фіксації результатів інформаційного пошуку для подальшого патентного аналізу.

Важливою є функція експорту результатів у інформаційні формати різних стандартів. Це дає змогу імпортувати дані у стандартне офісне програмне забезпечення або у численні пакети аналітичної обробки великих масивів даних (в тому числі статистичні або лінгвістичні).

Деякі системи пропонують послуги генерації повноформатних звітів про патентний пошук або дослідження відповідно до протоколів наповнення таких звітів. Результати порівняльного аналізу ПС представлені в Табл. 4.

Таблиця 4.

Порівняння функцій збереження результатів дослідження

Параметр	STInter-national	Patent-Pulse/Matheo-Patent	PatBase	Questel	Espacenet	Patent Scope	Lens	Примітка
Збереження формули пошуку	Так	Так	Так	Так	Ні	Так	Так	
Збереження результатів пошуку	Так	Так	Так	Так	Так, частково		Так	
Експорт результатів у формат XLS (Excel), або DOC (Word)	Так	Так	Так	Так	Так ³ частково	Так	Так	
Експорт результатів у формат RIS	Ні	Ні	Так	Ні	Ні	Ні	Так і	
Експорт результатів у формат XML	Ні	Ні	Так	Ні	Ні	Ні	Ні	
Прямий експорт до зовнішніх аналітичних систем	Так	Так	Так ²	Ні	Ні	Ні	Ні	1
Обмеження експорту, документів	50000	2000	10000	30000	500	10000	50000	
Генератор звітів про дослідження	Так	Так	Так	?	Ні	Ні	Ні	

1. Зовнішні аналітичні системи — такі як: BisIntSmartDataFile, VantagePoint, Centredoc, Matheo-Analytics та ін.
2. Обмеження до 500 документів
3. Не більше 500 документів кожного результатами, квотами по 30 документів за одну операцію

5. Методи патентного аналізу

Набір основних методів патентного аналізу є стандартним. Але наявність або відсутність певних інформаційних полів або спрощує, або ускладнює проведення таких досліджень. Кожна з пропріетарних (професійних або комерційних) систем пропонує власні алгоритми патентного аналізу, відповідно комплектуючи власну інформаційну структуру, пошуковий інтерфейс та способи візуалізації результатів (див. Табл. 5).

Таблиця 5.

Порівняння реалізованих методів патентного аналізу ПС

Параметр	STNInternational	PatentPulse/ M a t h e o - Patent	PatBase	Questel	Espacenet	PatentScope	Lens	Примітка
Дослідження «State of the Art»	Так	Так	Так	Так	Так	Так	Так	
Дослідження «Novelty and Inventiveness»	Так	Так	Так	Так	Так, частково	Так, частково	Так, частково	
Дослідження «Validity»	Так	Так, обмежено	Так	Так	Так, частково	Так, частково	Так, частково	
Дослідження «Freedom to Operate»	Так	Ні	Так	Так	Ні	Так, частково	Ні	
Дослідження «Technology Trends»	Так	Так	Так	Так	Ні	Так, частково	Так, частково	
Дослідження «Innovators»	Так	Так	Так	Так	Ні	Так, частково	Так, частково	
Дослідження «Competitor Activities»	Так	Так	Так	Так	Ні	Так, частково	Так, частково	

6. Методи візуалізації результатів аналізу

Візуалізація результатів патентного аналізу підвищує його когнітивну ефективність в умовах значної кількості параметрів та атрибутів, які характеризують патентний документ. Останній крок розвитку провідних ПС — це реалізація інтерактивного асоціативного зв'язку графічних елементів візуальної картини з відповідними патентними документами, що є важливим при ознайомленні з деталями опису конкретного патентного документу.

На даний час ПС реалізують десятки видів графіків, що відображають результати статистичного патентного аналізу. Тут проявляється тенденція до збільшення кількості видів графічної інтерпретації патентної інформації.

За останні роки збільшилась кількість ПС, які пропонують патентні ландшафти для інтерпретації результатів кластерного аналізу. Піонерами такої візуалізації були двадцять років тому системи STNInternational та Questel, проте зараз такі можливості пропонують майже всі без виключення пропрієтарні ПС.

Достатньо інформативними також є графові або мережеві діаграми, що візуалізують зв'язки прямого та зворотного цитування, аналіз яких дає інформацію про взаємозв'язок патентних документів, процеси впливу винахідницьких рішень одне на одне та ви-

явлення вузлових (кореневих) патентів у патентних сімействах або тематичних колекціях. Такі діаграми важливі при дослідженні зв'язків між конкурентами та партнерами у відповідних типах патентно-кон'юнктурного аналізу.

Головна проблема патентних ландшафтів — це вдала інтерпретація отриманих зображень при реалізованій можливості перейти до опису кожного потрібного документу, який на такій «топографічній поверхні» представлений окремою точкою. Така візуалізація дає чітку інтерпретацію «топографічних об'єктів» — кластерних груп патентних документів, «топографічною висоти» — кількості документів, але поняття відстані між об'єктами та точками носить лише якісний характер «семантичної близькості». Як правило, всі ПС пропонують синтез патентних ландшафтів на основі ключових слів (термінів) або рубрик патентної класифікації. На Рис. 1. представлена досить вдала мапа, яка відповідає результатам патентних досліджень, де чітко виявляються дві основних та один другорядний кластери патентних документів.

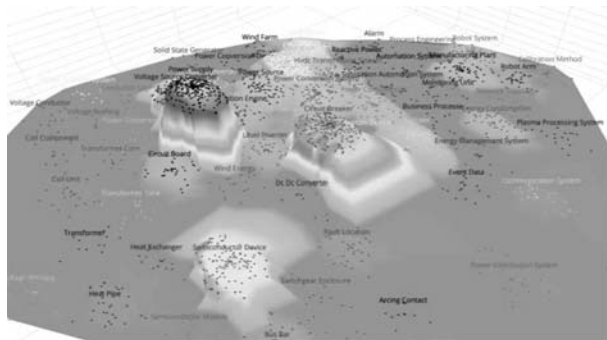


Рис. 1. Патентний ландшафт результатів патентного пошуку

Протилежним є приклад, що представлений на рис. 2, де спроба вивчення зв'язків між ОПВ приводить до неадекватного результату.

Таким чином, можливість синтезувати когнітивні графічні конструкції не є самоцілью, а лише засобом адекватно інтерпретувати результати пошукових або аналітичних процедур.

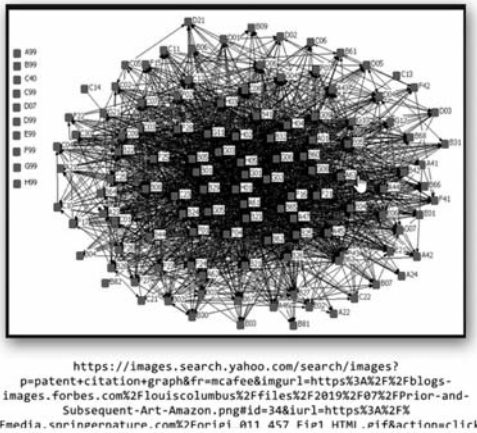


Рис. 2. Граф асоціативних зв'язків між суб'єктами патентування

В цілому головна тенденція розвитку ПС за критерієм візуалізації — це поступове розширення можливостей інтерпретування різноманітних графічних об'єктів, які асоціюються з певними параметрами або контентом колекції патентних документів.

Результати порівняльного аналізу ПС представлені у Табл. 6.

Таблиця 6.

Порівняння методів візуалізації ПС

Параметр	STNInternational	PatentPulse/Matheo-Patent	PatBase	Qustel	Espacenet	PatentScope	Lens	Примітка
Рейтингова візуалізація	Так	Так	Так	Так	Ні	Так	Так	
Хронологічна візуалізація	Так	Так	Так	Так	Ні	Так, частково	Так	
3D - візуалізація	Так	Так	Так	Так	Ні	Ні	Так	
Візуалізація патентних графів та мереж	Ні	Так	Так	Ні	Ні	Ні	Так	
Візуалізація патентних ландшафтів (патентні карти)	Так, частково	Так, частково	Так	Так	Ні	Ні	Ні	
Контент-аналіз	Так, частково	Так	Так	Так	Ні	Ні	Ні	
Аналіз структури патентних формул	Ні	Ні	Так	Ні	Ні	Ні	Так	

7. Висновки

У групі безоплатних ПС найбільш динамічно розвивається Patent Score (розвиток у Сегментах 1–3), Lens – поступається їй лише у Сегменті 1 (охоплює менше 20 країн або регіональних об'єднань). Крім того, Patent Score є відкритою системою, до якої було б варто приєднатися Україні, що значно підвищило б рівень представлення українських винаходів у результатах патентних досліджень по всьому світу.

У групі пропрієтарних (комерційних) ПС найбільш привабливою виглядає система PatBase [7], яка зазнала значного прогресу практично по всіх сегментах порівняння. Система STN International, одна із старіших систем поряд TotalPatent та Questel, зберігає стабільні показники по всіх Сегментах і проходить саме у цей момент стадію впровадження нової технологічної платформи — STNNext. З економічної точки зору в координатах ціна/якість перевагу вочевидь має система PatBase.

Всі системи, які були згадані у даному дослідженні та Derwent Innovation, або не охоплюють масив українських патентних документів, або пропонують неповну колекцію цих документів. Таку ситуацію можна визнати дискримінаційною з точки зору представленості українських винаходів на світовій арені.

Загальним фактором розвитку більшості систем (за винятком PatentScore) є перевага у використанні патентної класифікації CPC з одночасним збереженням доступності класифікації IPC.

У довготривалій перспективі безумовною є тенденція розширення реалізацій таких методів, як карти цитування та патентні ландшафти (із властивостями асоціативних зв'язків з повними описами ОПІВ). Більшість пропрієтарних ПС вже включили ці можливості у перелік аналітичних процедур.

Безперечною є тенденція використання технологій штучного інтелекту у семантичних процедурах патентних досліджень і патентного пошуку. В цьому сегменті дуже позитивно виглядає PatentScore.

В цілому патентно-інформаційні та патентно-аналітичні системи поступово поєднуються між собою, і, як клас, розвиваються у напрямі максимальної відповідності до вимог комплексних патентних досліджень, менеджменту об'єктів інтелектуальної власності.

Список використаних джерел

1. WIPO. Directory of Intellectual Property Offices. [web list] 2020 [cited 2020 November, 27]; National IP offices; Regional Offices]. Available from: <https://www.wipo.int/directory/en/urls.jsp>.

2. Укрпатент. Адреси вебсайтів відомств інтелектуальної власності та міжнародних організацій. 2020 [cited 2020 Листопад 27]; Available from: <https://ukrpatent.org/uk/articles/addrr-vid>.
3. Singh, V., K. Chakraborty, and L. Vincent, Patent database: Their importance in prior art documentation and patent search. *Journal of Intellectual Property Rights*, 2016. 21(1): p. 42-56.
4. Mehrotra, D., et al., Landscape analysis of patent dataset. *Journal of Intellectual Property Rights*, 2016. 21(4): p. 211-225.
5. України, Д.с., ДСТУ3575-97. Патентні дослідження. Основні положення та порядок проведення. 1997, Держстандарт України: Київ. p. 17.
6. STN_International. STN — the Choice of Patent Experts. 2020 [cited 2020 November 27]; Available from: <http://stn-international.com/>.
7. Minesoft. Patbase. Leading the way in patent searching and analysis. 2020 [cited 2020 November 27]; Available from: <https://mine-soft.com/our-products/patbase/>.
8. Clarivate. Derwent Innovation. 2020 [cited 2020 November 27]; Available from: <https://clarivate.com/derwent/solutions/derwent-innovation/>.
9. Questel. Orbit Intelligence. 2020 [cited 2020 November 27]; Accelerate your patent analysis, and make more informed decisions]. Available from: <https://www.questel.com/business-intelligence-software/orbit-intelligence/>.
10. LexisNexis. LexisNexis TotalPatent One. 2020 [cited 2020 November 27]; The Patent Search Software Tool that Provides Comprehensive Results You Can Rely On]. Available from: <https://www.lexis-nexisip.com/products/totalpatent-one/>.
11. SOFTWARE, M. PatentPulse. 2020 [cited 2020 November 27]; PATENT SEARCH SOLUTION FOR SMES. Patent Pulse is a patent search and analysis platform that is particularly adapted to SMEs that want to exploit technological information. Its outstanding quality/price ratio makes it very affordable and its price is very attractive.]. Available from: <https://www.patent-pulse.com/>.
12. Matheo-Software. MATHEO PATENT. 2020 [cited 2020 November 27]; SEARCH, RETRIEVE AND ANALYZE PATENT DATA.]. Available from: <https://www.matheo-software.com/matheo-patent/>.
13. Cambia. Lens. 2020 [cited 2020 November 27]; The Lens is an open global cyberinfrastructure to make the innovation system more efficient and fair, more transparent and inclusive.]. Available from: <https://www.Lens.org/>.

14. EPO. Espacenet. 2020 [cited 2020 November 27]; Available from: <https://worldwide.espacenet.com/>.

15. WIPO. PatentScope. 2020 [cited 2020 November 27]; Available from: <https://patentscope.wipo.int/search/en/search.jsf>.

16. WIPO, STANDARD ST.9 Bibliographic data on and relating to patents and SPCs. 2013, WIPO. p. 13.

*Андрощук Г. О.,
головний науковий співробітник
НДІ інтелектуальної власності НАПрН України
кандидат економічних наук, доцент
Кваша Т. К.,
завідуюча відділом УкрІНТЕІ*

ПАТЕНТНИЙ ЛАНДШАФТ ЯК ІНСТРУМЕНТ АНАЛІТИКИ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ (НА ПРИКЛАДІ АНАЛІЗУ СФЕРИ ВІЙСЬКОВИХ ТЕХНОЛОГІЙ)

Технологія є фундаментальним фактором соціальних змін, що пропонує нові можливості виробляти, зберігати та поширювати знання. Це особливо стосується військової сфери, основні зрушення в якій часто супроводжуються новаторськими подіями в історії науки та техніки. Якщо спочатку технологія не є результатом військових досліджень та розробок, все одно вона часто знаходить військове застосування. А використання нових технологій і виробництво на їх основі нової продукції збільшує оборонну потужність держави, а продаж військової техніки та послуг приносить значні прибутки для економіки країни.

Минулого року президент Франції Е. Макрон сказав, що технології більше не розглядаються як політично нейтральні: «Битва за технології, яку ми ведемо, полягає в суверенітеті країни. Якщо ми не побудуємо своїх власних чемпіонів у всіх сферах — цифровому, штучному інтелекті — наш вибір буде диктуватися іншими».

Уряди, військові відомства передових країн світу уділяють аналізу розвитку технологій, численних «слабких сигналів», що регулярно виникають на перетині технологічних секторів і галузей наукового знання, і здійснюють довгострокове науково-технологічне прогнозування.

У світовій практиці для технологічного прогнозування все частіше використовується патентний аналіз й аналітика інтелектуальної власності.

Цей метод дає змогу на засадах прогнозу тенденцій розвитку науково-технічних областей та об'єктів техніки обґрунтувати цільові критерії ефективності та вимоги до продукції, оцінювати її технічний рівень. Звіт про патентний ландшафт забезпечує моментальний знімок патентної ситуації в конкретній технології або компанії, в тому чи іншому регіоні, країні або на глобальному рівні. Переробка та візуалізація великих обсягів патентних даних є потужним інструментом аналізу і формування технологічного ландшафту. Адже патенти містять юридично важливу інформацію про винахідників, типи технологій, дату винаходу, пріоритетні дані, відомості про патентні родини, їх географічний розподіл і т. п. За допомогою патентного аналізу можна здійснити планування технологій, визначити тенденції їхнього розвитку та тенденції науки у цільових секторах економіки, провести аналіз технологій конкурентів, отримати розуміння того, чи варто проводити НДДКР і впроваджувати технології [1].

Дослідники зараховують до задач, які розв'язує аналітика інтелектуальної власності, такі:

- виявлення перспектив реалізації продукції, що розробляється;
- виявлення затребуваних розробок, які можуть бути виведені на ринок у ролі товару;
- визначення провідних організацій і країн у досліджуваній сфері, моніторинг напрямів змін у їхній діяльності [2].

Головна перевага патентного ландшафту полягає в можливості оперативного виявлення, порівняння та оцінювання співвідношення між лідерами і аутсайдерами ОВТ, найбільш перспективних учасників ринку або технологій, а також змін перерахованого в часовій динаміці (за роками). Призначення або функція патентного ландшафту — створення з великого обсягу науково-технічної інформації нового знання, доступного для розуміння широким або цільовим колам споживачів інформації про конкурентне середовище і технологічні тренди.

Методологія [3] дослідження базується на 4 етапах:

I. Відбір із усієї бази Derwent Innovation патентів на винаходи, що стосуються сфери «озброєння, військова техніка» — на основі кодів Міжнародної патентної класифікації (МПК) (F41 — озброєння та F42- боеприпаси; вибухові роботи) та ключових слів (military, defense, weapon, enginery, arm ,armament, weaponry, armor, arming, armour, troopsequipment, missile).

II. Визначення світових технологічних напрямів із високими темпами росту патентування винаходів (перспективних напрямів).

III. Аналіз розміщення швидкозростаючих напрямів на патентній ландшафтній карті¹⁶.

IV. Формування переліку найбільш перспективних (пріоритетних), перспективних та популярних технологічних напрямів за критеріями:

I група — пріоритетні напрями — темпи росту патентування більші за 1000 % та розміщення на зелених або голубих ділянках ландшафтної карти значної кількості таких патентів;

II група — перспективні напрями — темпи росту патентування винаходів від 500 % до 1000 % та розміщення на зелених і світло-коричневих ділянках ландшафтної карти значної кількості даних патентів;

III група — популярні напрями — темпи росту патентування винаходів знаходяться в інтервалі 200–500 % і розміщення переважної кількості патентів на коричневих та білих ділянках ландшафтної карти.

I. Система Derwent Innovation за повним запитом (за кодами та ключовими словами) відібрала 523 103 записів (0,4 % загального обсягу опублікованих патентів). Основними світовими патентотримувачами у цій сфері є США, Німеччина, Франція тощо (Рис. 1). Це ті країни, які витрачають найбільше коштів на розробку військової техніки і озброєння та їх патентування.

Серед корпорацій цих країн перші місця за наявністю патентів займають Rheinmetall Waffe Munition GmbH—виробник автомобільних компонентів, систем транспортних засобів оборонного призначення, зброї, боєприпасів, авіації, аеродинамічного обладнання тощо; VoforsAB — шведська компанія, виробник артилерійської продукції; Raytheon — американська компанія, одна з найбільших у країні та світі оборонних та індустріальних корпорацій у царині

¹⁶ Патентний ландшафт (ландшафтна карта) — візуалізація результатів патентного пошуку щодо значущих тенденцій і взаємозалежностей у масиві обраної тематики. При патентному картуванні і описані в документації технічні рішення відображаються на карті у вигляді ізольованих «островів», які показують окремі напрями дослідницької діяльності, найбільш популярні з яких утворюють великі «материки». Ці острови і материки можуть бути білими, коричневими або зеленими:

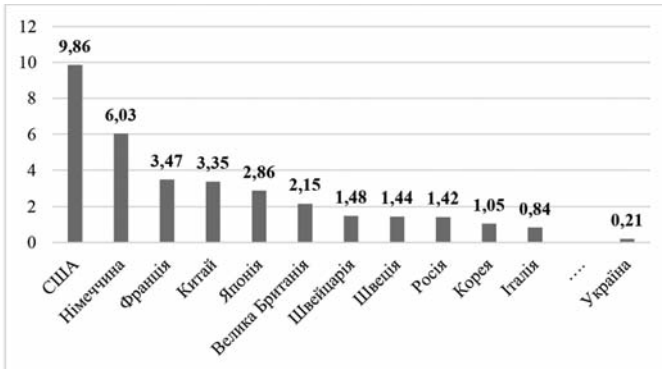
Білий колір — найбільша насиченість патентами і незначна кількість реєстрацій нових патентів (стара область або область уповільнення);

коричневий колір — дещо менша насиченість, нова реєстрація більш активна, але має спадну тенденцію (область уповільнення);

зелений — відбувається активна реєстрація нових патентів (область зростання);

блакитний — нові тематичні області, ще не визначені назви. Ці області можуть стати новими перспективними напрямими і областю зростання або відразу перейти в категорію «область уповільнення» чи зникнути з поля зору.

розробок та вироблення зброї, авіаційної та космічної техніки, електроніки, найбільший виробник керованих ракет у світі та ін.

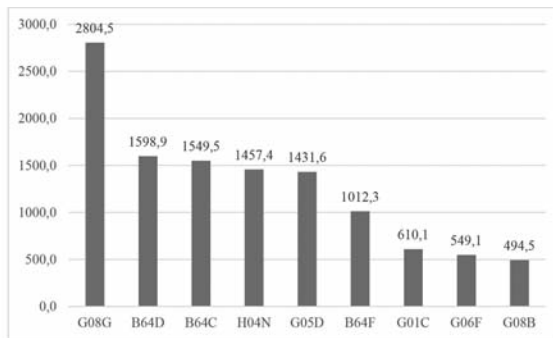


Джерело: Розроблено на основі даних Derwent Innovation

Рис. 1 Частки країн у загальному обсязі отриманих патентів у сфері озброєння та військової техніки за період 2011–2018 рр., %

II. Визначення перспективних світових технологічних напрямів.

За кодами Міжнародної патентної класифікації до топ — напрямів із зростаючою динамікою патентної активності відносяться напрями щодо контролю за рухом транспортних засобів, літаків, вертольотів, злітних палуб, льотного обладнання, сигнальних систем тощо (рис. 2).



Джерело: ClarivateAnalytics

Рис. 2 Топ-класи із найвищими темпами патентування сфери озброєнь та військової техніки (за кодами МПК*)

*Напрями із зростанням патентної активності даного рисунку

G08G	СИСТЕМИ КОНТРОЛЮВАННЯ РУХУ ТРАНСПОРТНИХ ЗАСОБІВ
B64D	ОБЛАДНАННЯ ЛІТАЛЬНИХ АПАРАТІВ; ЛЬОТНІ КОСТЮМИ ДЛІЯ ПІЛОТІВ; ПАРАШУТИ
B64C	ЛІТАКИ; ВЕРТОЛІБОТИ
H04N	ПЕРЕДАВАННЯ ЗОБРАЖЕННЯ
G05D	СИСТЕМИ КЕРУВАННЯ АБО РЕГУЛЮВАННЯ НЕЕЛЕКТРИЧНИХ ЗМІННИХ
B64F	НАЗЕМНІ УСТАНОВКИ АБО УСТАНОВКИ ЗЛІТНИХ ПАЛУБ АВІАНОСЦІВ; ПРОЕКТУВАННЯ, ВИРОБЛЕННЯ, МОНТУВАННЯ, ОЧИЩУВАННЯ, ОБСЛУГОВУВАННЯ АБО РЕМОНТУВАННЯ ЛІТАЛЬНИХ АПАРАТІВ; МАНІПУЛЮВАННЯ, ТРАНСПОРТУВАННЯ, ВИПРОБУВАННЯ АБО ПЕРЕВІРЯННЯ ЕЛЕМЕНТІВ ЛІТАЛЬНИХ АПАРАТІВ
G01C	ВИМІРЮВАННЯ ВІДСТАНЕЙ, РІВНІВ АБО АЗИМУТІВ; ТОПОГРАФІЧНА ЗЙОМКА; НАВІГАЦІЯ; ГІРОСКОПІЧНІ ПРИЛАДИ; ФОТОГРАММЕТРІЯ АБО ВІДЕОГРАММЕТРІЯ
G06F	ОБРОБЛЕННЯ ЦИФРОВИХ ДАНИХ ЗА ДОПОМОГОЮ ЕЛЕКТРИЧНИХ ПРИСТРОЇВ

Більш детальний аналіз кожного класу з рис. 2 виявив, що класи G08G, B64D, G01C, G05D, B64C, B64F, H04N містять по 1–2 напрямків, що відносяться до I (інколи II-ї) групи перспективності (табл. 2). Зокрема, це — літальні апарати спеціального призначення, системи керування рухом дорожнього транспорту, системи радіозв'язку, завантаження або запускання програм тощо.

Технологічні напрями із класів F41 та F42 мають менші темпи зростання патентування — лише один підклас F41A000366 (затворні коробки або рами механізмів казенних частей) входить до технологій II групи за темпами зростання патентування (табл. 3), ще 36-ть відносяться до популярних, але не перспективних напрямків, у т.ч. спускові гачки, механізми для автоматичного відкривання затвора, підривні заряди для утворювання газу під тиском, щити для індивідуального захисту, засоби наступу або оборони, вибухові роботи тощо.

Таблиця 2

Основні характеристики найбільш зростаючих напрямів патентування технологій подвійного призначення

Назва підкласу МПК	Індекс МПК	Кількість документів	Темпи росту, 2017/2011, %
Приспосовування відеопотоку локальної розподіленої мережі до певної локальної мережі, наприклад IEEE 1394 або Bluetooth® -мережі	H04N00214363	162	9100.0
Способи взаємодії, що базуються на графічних інтерфейсах користувача, для контролювання особливих функцій або операцій, наприклад вибирання об'єкта або зображення чи маніпулювання ним, встановлювання величини параметра або вибирання діапазону	G06F00030484	136	6800.0
Сполучання локальної розподіленої мережі, наприклад з'єднання з іншою STB або всередині приміщення	H04N0021436	127	5900.0
Способи взаємодії, що базуються на графічних інтерфейсах користувача та на особливих властивостях відображеної взаємодії об'єктів або модельного представлення середовища, наприклад взаємодії з елементами робочого столу, такими як вікна або іконки чи такими, що супроводжуються зміною поведінки або зовнішнього вигляду курсора	G06F00030481	84	5000.0
Пристрої вводу-виводу для бортових комп'ютерів системи навігації, спеціально приспосовані для навігації в мережі шосейних доріг	G01C002136	78	4800.0
Послуги бездротового зв'язку, в яких використовується інформація про розташування	H04W000402	2343	4248.5
Системи керування рухом дорожнього транспорту	G08G000100	60	3500.0
Протоколи зв'язку	H04N0021643	66	3100.0
Способи взаємодії, що базуються на графічних інтерфейсах користувач та з переліками позицій, які можна вибирати, наприклад меню	G06F00030482	84	2600.0
Літальні апарати спеціального призначення	B64C003902	59	2600.0
Пристрої, що забезпечують багаторазове використання передавального тракту	H04L000500	17194	2394.9
Процедура керування передаванням	H04L002908	6421	2344.4
Інтерфейси між терміналами	H04W009218	2029	2269.8
Керування з'єднанням	H04W007602	8691	2163.5
Системи радіозв'язку, тобто системи, що використовують поле випромінювання на передавальній станції	H04B000706	2181	2144.7
Виведення цифрових даних на індикаторні пристрої	G06F000314	142	2133.3
Керування даними мереж	H04W000800	3084	2032.1

Джерело: розроблено авторами на основі DerwentInnovation

Таблиця 3

Основні характеристики найбільш зростаючих напрямів патентування технологій озброєння та вибухових робіт

Назва підкласу МПК	Індекс МПК	Кількість документів, од.	Темпи росту, 2017/2011, %
Корпуси або спускові коробки затворів; стовбурні коробки	F41A000366	494	708.3
Спускові гачки; кріплення спускових гачків стрілецької або артилерійської зброї	F41A001910	438	445.2
Підривні заряди, тобто гільза і вибухова речовина для утворення газу під тиском	F42B000304	449	414.6
Броня; броньові плити для особистого використання	F41H000508	818	400.0

Джерело: розроблено авторами на основі DerwentImmovation

III. Аналіз розміщення високозростаючих технологічних напрямів на ландшафтній карті.

Всі напрями із найбільш високими темпами росту із табл. 2 розміщуються у переважній кількості на зелених полях ландшафтних карт (області зростання), але кожен з них має патенти і в областях уповільнення.

Наприклад, клас G08G має один підклас I групи перспективності — системи керування рухом дорожнього транспорту — G08G0001 (темпи — 3 500 %). До третьої групи відносяться системи керування рухом повітряного транспорту — G08G0005 (темпи — 325 %). Однак, і третя група має дуже перспективні вузьконаправлені піднапрями (рис. 3).

Області зростання (зелені ділянки) системи керування рухом дорожнього транспорту: передача даних, сигнал передачі, виявлений сигнал, периферійний пристрій, портативна бездротова передача даних, система управління флотилією, ескадрою, дисплейний пристрій; колісний транспортний засіб, безпека користувачів; інформація про навігацію, радіолокаційна система оповіщення про аварійну ситуацію, небезпечний стан, видимість тощо.

Для системи керування рухом повітряного транспорту області зростання характеризуються ключовими словами — навігаційна інформація, система позиціонування, позиційна інформація, головова інформація; криптографічний, червоний криптографічний ключ (рис. 3).

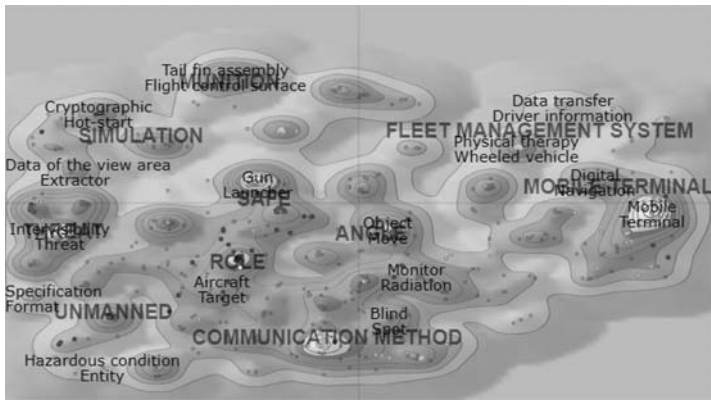
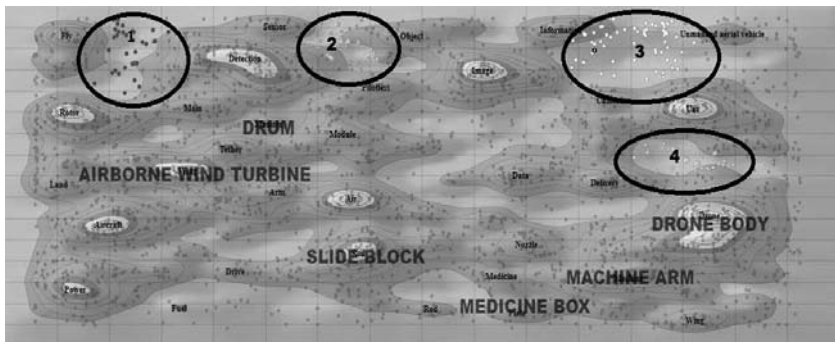


Рис 3. Ландшафтна карта класу G08G із виділенням підкласів G08G0005 (система керування рухом повітряного транспорту — червоні крапки) — та G08G0001 (система керування рухом дорожнього транспорту — зелені крапки).

У класі B64C найбільш перспективними є літальні апарати спеціального призначення (I група). У цій сфері перспективні напрями включають паливо, безпілотні літальні апарати (БПЛА), дрони, гелікоптери, системи керування та стабілізації безпілотних апаратів, системи управління віддаленими транспортними засобами, використання безпілотних апаратів для різних цілей (Рис. 4).



Джерело: розроблено на основі DerwentInnovation

Рис. 4. Розміщення на ландшафтній карті патентів за рубрикою «Літальні апарати спеціального призначення»

(1 — дрони, гелікоптери; 2 — системи, методи управління безпілотними, віддаленими транспортними засобами, ракетами; 3 — системи контролю, комп'ютерна навігація польоту, система стабілізації безпілотних літальних папаратів; 4 — системи, методи управління безпілотними, віддаленими транспортними засобами)

Перспективні напрями в галузі БПЛА:

- їх об'єднання в групи або в рій. Принцип організації рою — кожен дрон управляється власною автоматикою, а поведінкою рою може управляти програма з елементами ШІ або один (кілька) операторів;
- технологія сенсорів для дронів. Сенсори можуть відображати до 2,7 млн кв. миль в одному польоті;
- ринок анти-дронів, серед якого ринок лазерних анти-дронів, за прогнозами, зростатиме найвищими темпами протягом наступних 10 років. Військова і оборонна вертикалі матимуть найбільшу частку ринку анти-дронів, насамперед для контролювання кордонів, контрабанди та шпигунства. Сьогодні країни також надають важливе значення зміцненню заходів боротьби з дронами для моніторингу терористичної діяльності, що сприятиме підвищенню попиту на відповідні системи в найближчому майбутньому.

Ландшафтна карта військових технологій (класи F41 та F42) представляє собою переважно коричневу мапу, тобто, технології озброєння та вибухових робіт у своїй більшості є розробленими і запатентованими, в цих областях має сенс придбувати ліцензії, а нові технології розробляти у нових напрямках.

Детальний аналіз розміщення на ландшафтних картах найбільш високозростаючих напрямів патентування цієї сфери (табл. 3) дав можливість виявити перспективні нові напрямки. Наприклад, у класі F41 такими областями є вогнепальна зброя, індивідуальні системи захисту (рис. 5), а також області з ключовими словами: затворний механізм, затворна камера, флеш-супресор, металний, запалення, задній кінець снаряда тощо.

Відповідний аналіз класу F42 визначив перспективними області з ключовими словами: клапан, модель, газ, інфляційне гніздо труб, вибухові речовини, пістолет, ствол, перфорований пістолет. Наприклад, до цього класу відносяться патенти з голубих ділянок ландшафтної карти — інтегральнийзапальний пристрій, індукований двигуном; пристрій розширювача гарячого випромінювання; метод виготовлення та застосування розширювальної труби, подвійний резервний механізм запору пристрою електро-вибухової речовини; спосіб нейтралізації вибухонебезпечних пристроїв; прилади та спо-

соби перфорації, удосконалення перфораторів та пов'язаних з ними; апарат для виготовлення фасонного заряду тощо.

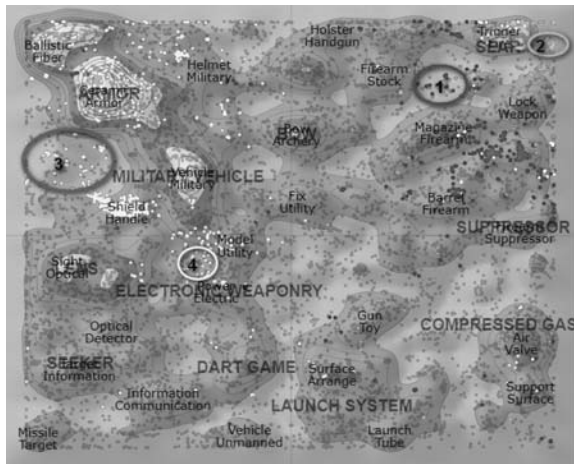


Рис. 5. Ландшафтна карта класу F41 з виділенням областей зростання

1 — Вогнепальна зброя: самонагружуючий пістолет, револьвер з корпусом керування тощо.

2 — Висувна система для вогнепальної зброї, зокрема повітряні гарпуни для стрільби з підводних човнів, багатофункціональний тригерний механізм пістолету тощо.

3 — Портативний екрануючий ефект вибуховості. Мобільний балістичний захисний щит із покращеним захистом користувача.

4 — Багатофункціональний куленепробивний екран, звукозахисний щит, який використовується поліцією, тощо.

Запальний пристрій, індукований двигуном; пристрій розширювача гарячого випромінювання; метод виготовлення та застосування розширювальної труби, подвійний резервний механізм запору пристрою електро-вибухової речовини; спосіб нейтралізації вибухонебезпечних пристроїв; прилади та способи перфорації, удосконалення перфораторів та пов'язаних з ними; апарат для виготовлення фасонного заряду тощо.

IV. Формування переліку найбільш перспективних (проривних), перспективних та популярних технологічних напрямів.

Синтез отриманих результатів дозволив згенерувати кластери найбільш перспективних та просто перспективних технологій військового характеру.

До найбільш перспективних відносяться такі класи та підкласи МПК:

- літальні апарати спеціального призначення (системи, методи управління безпілотними, віддаленими транспортними засобами, ракетами, дрони, гелікоптери, системи контролю, комп'ютерна навігація польоту та система стабілізації для безпілотних літальних апаратів тощо);
- інформаційно-комунікаційні технології, технології систем зв'язку і передавання зображень, систем контролювання руху транспортних засобів;
- вогнепальної зброї (розумна, інтелектуальна, високоенергетична гіперзвукова зброя, боеприпаси з декількома боеголовками);
- радіопеленгація і радіонавігація, індивідуальні системи захисту та системи захисту техніки (броя та інші нові матеріали); вибухові роботи.

Основні напрями подвійних технологій — це авіація та інформаційно-комунікаційна сфера. Основні тренди військових технологій — вогнепальна зброя, системи захисту, навігація, запальні пристрої, нейтралізація вибухонебезпечних пристроїв.

Серед інформаційно-комунікаційних технологій технології штучного інтелекту (ШІ) посилити своє значення, їх визначено як найбільший технологічний виклик, з яким стикаються країни світу, дехто називає ШІ найважливішою технологією, коли-небудь винайденою. Основні технології — біоінспіровані методи навчання (нейронні мережі, глибинне навчання),

У військовій сфері ШІ значно вплине на можливості та сили армій переважно завдяки використанню вбудованого ШІ в інших супутніх технологіях, таких як віртуальна / доповнена реальність; квантові обчислення; автономність, моделювання, простір; дослідження матеріалів; виробництво та логістика; та аналіз великих даних.

Прогноз напрямів розвитку технологій — розширені алгоритми (машинне та глибинне навчання, нейроморфні та імовірнісні обчислення), симбіоз людина-машина (інтерфейс, орієнтований на людину, візуалізація, пояснюваність, командна динаміка), інфопростір (створення зброї за допомогою ШІ, напр., глибокі підробки) та розроблення заходів протидії, напр., підтримка довіри та протидія (вразливості) тощо.

Інший популярний технологічний напрям 2020 р. — робототехніка та автономні системи зброї. До цієї групи відносяться збройні безпілотники та інші автономні системи із зниженим рівнем людського контролю, зокрема БПЛА різного розміру та невеликі рої; робототехнічне сторожове озброєння — гармати, які можуть автоматично виявляти, відслідковувати та (потенційно) атакувати цілі;

керовані боеприпаси, які також називаються розумними бомбами або прецизійними боеприпасами, є вибуховими снарядами, які можуть коригувати початкові цілі або помилки після того, як вони були випущені або запущені.

Прогноз напрямів розвитку технологій — автономні системи, симбіоз людина-машина, автономна поведінка, контрзаходи.

II група — перспективні напрями:

- гвинтокрили;
- передавання зображення (телебачення, відео) — моніторинг процесів або ресурсів, дистанційне керування, оброблення сигналів, телевізійні системи для двостороннього режиму роботи;
- устаткування або способи цифрових обчислень чи обробки даних, пристрої програмної інженерії;
- системи визначення місцеположення транспортного засобу, керування положенням, курсом, висотою або орієнтацією у просторі наземних, водних, повітряних або космічних транспортних засобів, наприклад автоматичне пілотування;
- система озброєння: радіопеленгація, радіонавігація; сигнальні пристрої або пристрої виклику; бойові або броньовані машини; протиповітряні або протиракетні оборонні споруди і системи;
- вибухові роботи: експлуатація шахт і кар'єрів; вибухові роботи спеціального призначення.

Отже, застосування інструментів аналітики інтелектуальної власності надає можливість виявити найбільш перспективні напрями технологічних змін, скорегувати інноваційну політику, вчасно враховувати зміни в широкому діапазоні сфер, щоб отримати потенційні вигоди та мінімізувати ризики і негативні наслідки розвитку нових технологій.

Список використаних джерел

1. Chang P.L. Investigation of technological trends in flexible display fabrication through patent analysis / P. L. Chang, C. C. Wu, H. J. Leu // *Disp.* 33 (2), 2012. — pp. 68–73.

2. Писаренко Т. В. Глобальні технологічні тренди у розрізі окремих Цілей сталого розвитку: монографія / Т. В. Писаренко, Т. К. Кваша, О. Ф. Паладченко та ін. — Київ : УкрІНТЕІ, 2019. — 300 с.

3. Андрощук Г. О. Патентний ландшафт як інструмент прогнозування світових технологічних трендів: сфера озброєння та військової техніки / Андрощук Г. О., Кваша Т. К. // *Наука, технології, інновації.* 2019. № 4 (12). С. 28-40. — DOI: 10.35668/2520-6524-2019-4-04.

Кислий Т. Ф.,
*партнер Arzinger, адвокат, арбітр з розгляду
доменних спорів за процедурою UDRP та доменних
спорів в ccTLD .UA за процедурою UA-DRP
Міжнародного центру з арбітражу та медіації BOIB
(Женева, Швейцарія).*

LEGAL TECH ПРОТИ КІБЕРСКВОТИНГУ: МІЖНАРОДНИЙ ДОСВІД ТА УКРАЇНСЬКІ РЕАЛІЇ

Історія питання. Проблема реєстрації доменних імен з чужою торговельною маркою (кіберсквотинг) існує вже стільки ж років, як і самі доменні імена.

Нагадаємо, що прообраз доменних імен був впроваджений ще у далекому 1983 р. і спершу вони використовувались у комп'ютерній мережі APRANET Міністерства оборони США. З часом їх функціонал змінився на більш традиційний для нас і вже у 1985 р. було за-реєстроване перше доменне ім'я в зоні .com у звичному для нас розумінні.

З того часу доменний простір розпочав свій бурхливий розвиток, який триває і дотепер. В другій половині дев'яностих років минулого століття питання організації і впорядкування доменного простору набуло таких масштабів, що стала очевидною необхідність створення організації, яка б взяла на себе ці функції.

Так у 1998 р. з'явилась Інтернет-корпорація з присвоєння імен та номерів (англ. Internet Corporation for Assigned Names and Numbers, або ICANN), що являє собою міжнародну некомерційну організацію, яка була створена за участю уряду США для регулювання питань, пов'язаних з доменними іменами, IP-адресами і іншими аспектами функціонування Інтернету. У своїй роботі ICANN відповідає за стабільність та безпечність функціонування мережі Інтернет, керує архітектурою та розвитком доменного простору, авторизує реєстраторів, які реєструють та делегують доменні імена.

Однією з основних проблем, яку мало розв'язати ICANN був конфлікт між торговельною маркою та доменним іменем (відомий як «Trademark Dilemma»), і, відповідно ефективні механізми врегулювання таких конфліктів. Для вирішення даного питання ICANN звернулось за експертною оцінкою до Всесвітньої організації інтелектуальної власності (англ. World Intellectual Property Organization, або WIPO). WIPO є одним із спеціалізованих агентств Організації Об'єднаних Націй, яке було створене для просування та вдосконалення захисту прав інтелектуальної власності у світі.

Результатом співпраці ICANN та WIPO стало створення Єдиної політики вирішення доменних спорів стосовно доменних імен (англ. Uniform Domain-Name Dispute-Resolution Policy, або UDRP).

UDRP запровадив обов'язкову адміністративну процедуру розгляду спорів, які виникають при конфлікті доменного імені та торговельної марки. У своєму розвитку ця процедура пройшла етапи від формального документу до системи технологічних рішень, які роблять її однією з найуспішніших та найефективніших у світі серед позасудових механізмів вирішення спорів.

В чому ж була необхідність створення саме позасудової системи вирішення доменних спорів і чим не влаштував традиційний судовий розгляд у національних судах.

Недоліки судового розгляду доменних спорів. В українському суспільстві існує часом небезпідставна думка про низьку ефективність державної судової системи. Слід зазначити, що таку думку поділяють у більшості країн світу, якщо йдеться про вирішення доменних спорів, і таке критичне ставлення почало формуватись вже з часу створення самих доменних імен.

В першу чергу, це пов'язано із мультиюрисдикційністю доменних спорів. Справа в тому, що власник доменного імені (імовірний порушник), власник торговельної марки (ініціатор спору) та реєстратор доменного імені (безпосередньо має виконати рішення) в переважній більшості випадків знаходяться у різних країнах. Тому виникає безліч питань на кшталт до суду якої країни звертатись із позовом, як належним чином повідомити іноземних учасників спору про судову справу, як таким учасникам спору організувати належне представництво у суді, як виконати судові рішення на території іноземної держави і таке інше.

Всі ці питання неймовірно ускладнюють вирішення навіть самого простого доменного спору і мають своїм наслідком довгий та процесуально складний шлях навіть за умови, якщо всі залучені юрисдикції мають зразкову та супер ефективну судову систему.

Також не останню роль відіграє необізнаність рядового суду із питаннями доменних імен. За звичайних умов доменний спір може трапитись у практиці того чи іншого судді вперше і востаннє. Тобто досвіду у розгляді такого спору пересічний суддя не матиме. Як наслідок, необхідний додатковий час, який має витратити суд, щоб розібратись у справі. Також годі говорити про якийсь усталений підхід та єдину практику, а також передбачуваність рішення при розгляді спору за подібних обставин.

Все вищенаведене призводить до дуже тривалого, дорогого та непередбачуваного за результатом розгляду справи. І все це геть не

годиться для такої динамічної сфери як правовідносини у сфері Інтернет.

Давайте розглянемо як з цими викликами впоралися такі не в повній мірі звичні для України інструменти як положення UDRP, медіація WIPO та рішення legaltech.

Переваги розгляду доменних спорів у WIPO. Отже, для розгляду доменних спорів за UDRP було вирішено створити незалежних провайдерів, які б адміністрували процес. На сьогодні таких провайдерів п'ять від більш популярного до менш популярного:

- Центр арбітражу та медіації WIPO (англ. WIPO Arbitration and Mediation Center);
- Національний арбітражний форум (англ. National Arbitration Forum, або NAF);
- Чеський арбітражний суд, Арбітражний центр інтернет спорів (англ. Czech Arbitration Court, Arbitration Center for Internet Disputes);
- Азійський центр вирішення доменних спорів (англ. The Asian Domain Name Dispute Resolution Centre, або ADNDRC);
- Арабський центр вирішення спорів (англ. The Arab Center for Dispute Resolution, або ACDR).

Як бачимо, найбільш популярним провайдером, через якого вирішуються доменні спори є Центр арбітражу та медіації WIPO. І секрет його успіху стоїть на трьох китах: стандартизації, автоматизації та узагальненні.

Дійсно, саме Центр арбітражу та медіації WIPO провів величезну роботу спрямовану на стандартизацію процесів, які відбуваються під час розгляду доменних спорів.

В першу чергу, йдеться про наявність типових документів, які спрощують роботу сторін спору, його адміністратора та адміністративної комісії. Такі документи викладені всіма мовами, якими ведеться розгляд доменних спорів.

Так, на сайті Центру арбітражу та медіації WIPO сторонам спору доступні типові проекти процесуальних документів (скарга, відзив та ін.). Таким чином досягається єдиний підхід при підготовці таких документів, практично виключаються випадки подання неповних або невірно оформлених документів. Вже не кажучи про спрощення роботи самих сторін під час підготовки документів.

Процедура розгляду спору має етапи, які проходять всі справи. Для кожного етапу створений шаблон, який доступний на інтра-сайті Центру арбітражу та медіації WIPO для адміністратора відповідної справи. Це значно пришвидшує рух справи і дозволяє адміністратору реагувати на розвиток справи в дуже стислі терміни.

Так само розроблені шаблони процесуальних документів, які видає адміністративна комісія. Доступ до таких шаблонів забезпечується через адміністратора справи і значно полегшує та пришвидшує роботу адміністративної комісії, а також робить її рішення стандартизованими та більш придатними для аналізу при використанні у наступних подібних спорах.

Для роботи адміністративної комісії з матеріалами справи створений інтрасайт із обмеженим доступом, яким можуть скористатись адміністратор справи та адміністративна комісія, яка її розглядає. Такий доступ адміністративна комісія має як під час розгляду справи, так і після вирішення спору.

Всі рішення у доменних спорах знаходяться в загальному доступі, окрім обмеженої групи конфіденційних рішень. Такий доступ організовано на веб сайті Центру арбітражу та медіації WIPO, при цьому забезпечується широкий вибір інструментів пошуку необхідного рішення.

І, напевно, найбільшою конкурентною перевагою Центру арбітражу та медіації WIPO є узагальнення практики вирішення доменних спорів у вигляді «Огляду WIPO позицій адміністративних комісій WIPO щодо окремих питань UDRP» (англ. WIPO Overview of WIPO Panel Views on Selected UDRP Questions). В даному документі проаналізовані рішення у доменних спорах, які розглядались у WIPO за попередні роки, та викладена позиція по кожному біль менш значущому питанню, якої дотримувались адміністративні комісії. Такий огляд є у вільному доступі на сайті WIPO та дозволяє переглянути кожне рішення на підставі якого сформована та чи інша позиція. Наразі використовується вже третя оновлена версія огляду.

Так, звертаючись до WIPO заявник викладає скаргу з використанням єдиного шаблону та доступу до всіх рішень у подібних справах. Адміністратор справи веде листування також використовуючи шаблони процесуальних документів. Адміністративна комісія розглядаючи справу має у своєму розпорядженні згаданий огляд WIPO і при вирішенні спору слідує підходам, застосованим у попередніх рішеннях.

У підсумку маємо систему адміністративних та технологічних інструментів, які дозволяють розглянути справу у дуже стислі строки (біля 80 днів від подання скарги до виконання рішення), з витратами в рази нижчими судового чи повноцінного арбітражного розгляду (1500 доларів США), та з передбачуваним стабільним результатом.

Ще однією перевагою UDRP є те, що такі рішення потім не переглядаються у державних судах. Такого підходу дотримуються пере-

важно юрисдикції із зрілою судовою системою. Так, наприклад, суди Великобританії у справі YOYO.EMAIL проти Royal Bank of Scotland прийшли до висновку, що рішення адміністративної комісії у доменному спорі розглянутому за UDRP не підлягає оскарженню і перегляду судом.

UA-DRP спори в Україні. Що ж до України, то наша держава також приєдналась до процедури UDRP у 2019 р., надавши змогу зацікавленим сторонам розглядати таким чином доменні спори щодо доменних імен у зонах .UA та .COM.UA через WIPO. Україна, відповідно, тепер може скористатись всім масивом технологічних рішень, що забезпечують тепер швидкий та ефективний розгляд спорів щодо українських доменних імен. Статистика українських справ, яких вже більше 30 за менш ніж рік повноцінного функціонування системи, свідчить про її популярність та перспективність в Україні. Будемо сподіватись, що найближчим часом сфера застосування UDRP розшириться і на решту українських доменних імен.

Зараз Україна може скористатись всім масивом технологічних рішень, що забезпечують тепер швидкий та ефективний розгляд спорів щодо українських доменних імен.

Наразі доменні спори за UA-DRP може розглядати 5 арбітрів, які за основним місцем роботи є українськими приватно практикуючими юристами.

Статистика українських справ, яких вже більше 30 за менш ніж рік повноцінного функціонування системи, свідчить про її популярність та перспективність в Україні. Найбільш типовим порушенням є використання чужої торговельної марки у доменному імені для створення враження пов'язаності домену із власником оригінального бренду, приваблювання споживачів до веб-сайту порушника та отримання ним незаконної вигоди. Всі ці справи були швидко та ефективно розглянуті із відновленням законних прав відповідної сторони. Зі сторони реєстраторів спірних доменних імен наразі повне сприяння як під час розгляду спору, так і під час виконання рішення у справі.

Окремо слід зазначити, що великого значення набуває кваліфікований юридичний супровід доменного спору. Від правильного підбору та інтерпретації доказів, а також знань прецедентної бази UDRP та UA-DRP багатов чому залежить результат розгляду справи. І, звісно, представники мають володіти англійською та українською мовами, оскільки матеріали справи практично завжди містять документи обома мовами, так само прецедентна база переважно викладена англійською, та й позицію у справі треба бути готовим викласти на будь-якій із цих мов.

Українська практика. Розглянемо як на практиці вирішується український доменний спір на прикладі справи № DUA2020-0005, Хармен Інтернешнл індастріз, Інк. (Harman International Industries, Inc.) проти Александра Колегаєва (у додатку).

Ця справа стосувалась доменного імені jbl.com.ua. Позивач у справі — американська компанія відома як виробник аудіо обладнання та власник бренду JBL. На спірному доменному імені було розташовано веб-сайт, де пропонувались до продажу товари під брендом JBL та продукція інших виробників. Справа була розглянута українською мовою, оскільки реєстраційна угода була викладена українською мовою, і у справі були відсутні обставини на користь іншої мови розгляду. При вирішенні доменного спору має бути досліджено три елементи: (i) схожість або тотожність спірного доменного імені та відповідної торговельної марки, (ii) права або законні інтереси щодо спірного доменного імені, (iii) недобросовісна реєстрація або використання спірного доменного імені.

За першим елементом було враховано, що спірне доменне ім'я повністю включає торговельну марку Позивача, при цьому домен верхнього рівня не враховується при порівнянні. На цій підставі адміністративна комісія прийшла до висновку про тотожність спірного доменного імені та торговельної марки Позивача для цілей UA-DRP.

За другим елементом було враховано, зокрема, невідповідність спірного доменного імені вимогам, які висуваються до веб-сайтів реселерів та дистриб'юторів, відомі також як Oki Data тест. Так, на веб-сайті за спірним доменним іменем пропонувались до продажу не тільки товари під брендом Позивача, а й інші товари. Також при цьому не розкривалась інформація про те який насправді зв'язок існує із Позивачем. З врахуванням цього адміністративна комісія встановила відсутність прав та законних інтересів Відповідача на спірне доменне ім'я.

При дослідженні третього елемента було встановлено, що використовуючи доменне ім'я, Відповідач навмисне намагався з комерційною метою привабити користувачів Інтернету на свого веб-сайту, створюючи оманливу подібність із брендом Позивача в контексті джерела, спонсорства, приналежності або схвалення такого веб-сайту. Крім того, використання спірного доменного імені для торгівлі продукцією під брендом Позивача вказувало на його обізнаність з таким брендом і відповідними правами на час реєстрації спірного доменного імені. За таких обставин адміністративна комісія дійшла висновку про недобросовісну реєстрацію та використання спірного доменного імені.

Оскільки всі три зазначені елементи були підтверджені, вимога Позивача про передачу йому спірного доменного імені була задоволена з подальшим виконанням рішення реєстратором.

Загалом від подання скарги і до винесення рішення пройшло близько 5 місяців із кількомісячною перервою для спроби укладення мирової угоди.

Таким чином, дана справа може слугувати прикладом переваг розгляду доменних спорів за UA-DRP, який, як вже зазначалось, має з часом поширитись і не решту українських доменних імен.

Додаток

WIPO Arbitration and Mediation Center
РІШЕННЯ АДМІНІСТРАТИВНОЇ КОМІСІЇ
Хармен Інтернешенл Індастріз, Інк. (Harman International Industries, Inc.) проти Александра Колегаєва
Справа № DUA2020-0005

1. Сторони

Позивачем є Хармен Інтернешенл Індастріз, Інк. (Harman International Industries, Inc.), США, якого представляє Petošević, Україна.

Відповідачем є Александр Колегаєв, Україна.

2. Доменне ім'я та Реєстратор

Спірне доменне ім'я <jbl.com.ua> зареєстроване через Товариство з обмеженою відповідальністю «Інтернет Інвест» (*imena.ua*) (далі — «Реєстратор»).

3. Історія процесу

Позов було подано до Центру з арбітражу та медіації ВОІВ (далі — «Центр») 5 лютого 2020 р. 6 лютого 2020 р. Центр надіслав електронною поштою запит до Реєстратора для встановлення реєстранта оспорюваного доменного імені. 10 лютого 2020 р. Реєстратор електронною поштою надав Центру відповідь, в якій надав інформацію щодо реєстранта та його контактних даних, які відрізнялись від вказаних у Позові. 10 лютого 2020 р. Центр повідомив ім'я та контактні дані Позивачу та запропонував йому внести відповідні зміни до Позову. 11 лютого 2020 р. Позивач надав Позов, який був змінений з врахуванням наданого імені реєстранта та його контактних даних.

Центр встановив, що Позов та змінена скарга відповідає формальним вимогам Єдиної політики вирішення спорів щодо доменних імен в домені .UA (далі — «Політика .UA»), Правил Єдиної політики вирішення спорів щодо доменних імен в домені .UA (далі — «Правила .UA»), а також Додаткових правил Єдиної політики вирішення спорів щодо доменних імен в домені .UA Всесвітньої орга-

нізації інтелектуальної власності (далі — «Додаткові правила ВОІВ»).

Відповідно до Правил .UA, параграф 4(с), Центр формально повідомив Відповідача про Позов, і провадження було відкрито 17 лютого 2020 р. Відповідно до Правил .UA, параграф 5(а) та з врахуванням зупинення провадження на час переговорів щодо мирової угоди Відповідь слід було надати до 22 липня 2020 р. Відповідач не надав ніякої Відповіді. Відповідно, 23 липня 2020 р. Центр повідомив про пропуск строку Відповідачем.

24 липня 2020 р. Центр призначив Тараса Кислого у якості одноосібного члена Комісії у цій справі. Комісія встановила, що вона була призначена належним чином. Комісія надала Заяву про прийняття та Декларацію про неупередженість та незалежність, як цього вимагає Центр на виконання Правил .UA, параграф 7.

4. Фактичні обставини

Позивач є американською компанією, яка випускає як професійне акустичне обладнання та електроніку для кінотеатрів, студій звукозапису, концертних залів, так і аудіотехніку для приватного використання, зокрема, динаміки, аудіо колонки, у тому числі портативні, тощо. Позивач є власником торговельної марки JBL, яка отримала охорону в багатьох країнах світу, в тому числі в Україні було видане свідоцтво № 37005, дата реєстрації 15 січня 2004 р.

Спірне доменне ім'я було зареєстроване 11 лютого 2004 р. вело до веб-сайту, де пропонувалась до продажу продукція під Торговельною маркою Позивача та продукція інших виробників. На час розгляду Позову спірне доменне ім'я перенаправляє до доменного імені <jbl-harman.in.ua>, яке веде до веб-сайту, де пропонується до продажу продукція під Торговельною маркою Позивача.

5. Доводи Сторін

А. Позивач

Спірне доменне ім'я є тотожним або схожим до ступеню змішування з Торговельною маркою Позивача. Спірне доменне ім'я повністю включає в себе Торговельну марку Позивача. Частина доменного імені, що відноситься до доменної зони (.com.ua), не береться до уваги при оцінці тотожності або схожості до ступеня змішування між доменом і торговельною маркою.

Відповідач не має прав або законних інтересів стосовно спірного доменного імені. Позивач не надавав жодних повноважень, дозволів або ліцензій на використання своїх торговельних марок, у тому числі торговельної марки JBL, об'єктів авторського права у спірному доменному імені, на комерційному сайті за даним ім'ям та на сторінках соціальних мереж магазину «www.jbl.com.ua». Відпові-

дач не відомий загалу за спірним доменним іменем. Відповідач використовує спірне доменне ім'я стосовно комерційного веб-сайту, а саме онлайн-магазину. Таким чином, використання торговельних марок Позивача не носить некомерційний характер. Дії Відповідача не можуть розцінюватись як *bona fide* використання спірного доменного імені, оскільки при цьому Відповідач не розкриває точно та однозначно характер своїх взаємовідносин з Позивачем, а також оскільки Відповідач на веб-сайті за спірним доменом пропонував до продажу також продукцію інших виробників.

Спірне доменне ім'я було зареєстроване або використовується недобросовісно. Відповідач знав про Торговельну марку Позивача під час реєстрації спірного доменного імені та свідомо його реєстрував з комерційною метою для приваблення користувачів Інтернету за рахунок репутації Позивача. Відповідач мав на меті перешкодити Позивачу відобразити його Торговельну марку у відповідному доменному імені. Реєструючи спірне доменне ім'я Відповідач мав на меті порушити звичний хід бізнесу Позивача як свого конкурента. Відповідач є власником доменного імені, де також використано торговельну марку третьої особи, що свідчить про усталену недобросовісну модель поведінки Відповідача. Відповідач не надав змістовної відповіді на звернення Позивача стосовно неправомірного використання спірного доменного імені. Відповідач публічно пропонував спірне доменне ім'я для продажу.

V. Відповідач

Відповідач не надав відповіді щодо позиції Позивача.

6. Обговорення та висновки

Відповідно до параграфу 4(а) Політики .UA позивач для обґрунтування своїх вимог повинен довести кожен з наступних елементів:

- (i) доменне ім'я є ідентичним або оманливо подібним до торговельної марки, на яку позивач має права; і
- (ii) у відповідача немає прав або законних інтересів щодо доменного імені; і
- (iii) доменне ім'я зареєстроване або використовується недобросовісно.

Політика .UA є варіацією Єдиної політики вирішення спорів щодо доменних імен в домені ("UDRP") і ці документи співпадають щодо більшості положень. Хоча UDRP не передбачає суворої доктрини прецедентного підходу, для підтримання загальної довіри до системи UDRP є важливим, щоб сторони могли очікувати передбачуваний результат розгляду своєї справи. Тому комісії при розгляді спорів за процедурою UDRP прагнуть дотримуватись однакових підходів при подібних ключових факторах або обставинах справи. Узагальнення

усталених підходів комісій у застосуванні UDRP при розгляді доменних спорів детально розкриті у Огляді Всесвітньої організації інтелектуальної власності позицій комісій Всесвітньої організації інтелектуальної власності щодо окремих питань UDRP, третє видання (Огляд ВОІВ 3.0). З врахуванням цього Комісія у даній справі вважає за доцільне, щоб її висновки узгоджувались не лише з положеннями Політики .UA, а й з відповідними попередніми рішеннями комісій за процедурою UDRP, та з відповідними узагальненнями таких рішень, які викладені в Огляді ВОІВ 3.0, де це доречно.

У даній справі позов було подано приблизно через 16 років після реєстрації спірного доменного імені. З цього приводу слід зазначити, що сам факт значного розриву в часі між реєстрацією доменного імені та поданням позову не є перешкодою ні для ініціювання справи, ні для її потенційного виграшу. При розгляді справ за Політикою .UA йдеться радше про припинення порушення, аніж відшкодування, і основною метою є зупинення триваючого порушення або запобігання наступним зловживанням чи шкоді. Не слід очікувати, що власники торговельних марок будуть постійно моніторити кожне можливе зазіхання на їх торговельну марку, або ж миттєво вживати заходи щодо захисту своїх прав, як тільки вони дізнаються про їх порушення, в той час як кібер-сквотери практично позбавлені фінансових та організаційних перепон для масових реєстрацій доменних імен. Відповідно, Комісія не бачить підстав для застосування концепцій на кшталт позовної давності чи аналогічних концепцій у даній справі. В той же час, Комісія допускає, що в деяких справах затримка з поданням позову може ускладнити позивачу обґрунтування своєї позиції по суті спору, зокрема, коли відповідач може продемонструвати негативні наслідки такої затримки. Аналогічна позиція також висловлена у розділі 4.17 Огляду ВОІВ 3.0.

А. Тотожний або схожий до ступеню змішування

Комісія встановила, що Позивач має права на свою Торговельну марку.

У доменному імені загальний домен верхнього рівня (наприклад, «.ua», «.com.ua») є стандартною реєстраційною вимогою, і як такий не має значення для встановленні схожості за першим елементом, який має довести позивач у справі. Враховуючи наведене, Комісія не бере до уваги домен «.com.ua» при вирішенні питання про схожість спірного доменного імені та Торговельної марки Позивача. Аналогічна позиція також висловлена у *ABElectrolux проти Захаров Евгений, справа ВОІВ № DUA2020-0006*.

У справах, де доменне ім'я повністю включає торговельну марку, таке домене ім'я за звичайних обставин доцільно вважати тотож-

ним або схожим із такою торговельною маркою для цілей Політики .UA. Комісія у даній справі встановила, що спірне доменне ім'я повністю включає Торговельну марку Позивача. Аналогічна позиція також висловлена у АВ *Electrolux проти Захаров Евгений*, справа VOIB № DUA2020-0006.

Враховуючи вищенаведене Комісія прийшла до висновку, що спірне доменне ім'я є тотожним із Торговельною маркою Позивача, на яку Позивач має права і, відповідно, Позов відповідає вимогам параграфу 4(а)(і) Політики .UA.

В. Права або законні інтереси

Відповідно до параграфу 4(с) Політики .UA наявність або відсутність прав або законних інтересів відповідача стосовно доменного імені встановлюється з врахуванням будь-яких із наступних обставин (включно але без обмежень):

- (і) перед отриманням будь-якого повідомлення щодо спору, відповідач використовував або демонстративно готувався до використання доменного імені або імені, що стосується доменного імені, у зв'язку з добросовісним наданням товарів або послуг; або
- (іі) відповідач (як фізична особа, суб'єкт господарської діяльності або інша організація), відомий загалу за доменним іменем, навіть якщо відповідач не набував жодних прав на торговельні марки; або
- (ііі) відповідач використовує доменне ім'я з некомерційною метою або правомірно без наміру отримати комерційну вигоду шляхом оманливого приваблювання споживачів або завдання шкоди репутації торговельної марки.

Загалом тягар доказування за процедурою Політики .UA покладено на позивача. В той же час слід визнати, що доведення відсутності у відповідача прав чи законних інтересів щодо доменного імені може являти неможливе для виконання завдання «доведення зворотного», що часто вимагає в першу чергу інформації, яка є у розпорядженні чи контролюється відповідачем. Тому, коли позивач *prima facie* заявляє, що у відповідача немає прав або законних інтересів, тягар доказування перекладається на відповідача, який має надати відповідні докази, що демонструють права або законні інтереси щодо доменного імені. Якщо відповідач не надає такі докази, то має вважатись, що позов відповідає вимогам щодо другого елемента доказування. Аналогічна позиція також висловлена у АВ *Electrolux проти Захаров Евгений*, справа VOIB № DUA2020-0006.

У даній справі Позивач *prima facie* стверджує про відсутність прав або законних інтересів Відповідача щодо спірного. Відповідач не надав ніяких доказів стосовно цього питання.

Обставини справи свідчать, що Позивач не надавав ліцензію і ніяким іншим чином не надавав згоди на використання Відповідачем раніше зареєстрованої Торговельної марки Позивача, тому Комісія встановила, що ніяке дійсне або гіпотетичне добросовісне або законне використання спірного доменного імені не може бути з розумним ступенем вірогідності заявлене у цій справі. Аналогічна позиція висловлена також комісіями у попередніх справах .UA (див., наприклад, АВ *Electrolux проти Name Servis, Александр Шевчук, справа ВОІВ № DUA2020-0011*).

Обставини справи свідчать, що Відповідач не відомий загалом за спірним доменним іменем.

Також обставини справи свідчать, що Відповідач використовує спірне доменне ім'я з наміром отримати комерційну вигоду шляхом оманливого приваблювання споживачів пропонуючи для продажу, в тому числі, продукцію під Торговельною маркою Позивача.

Слід однак зазначити, що реселери, дистриб'ютори або надавачі послуг, які використовують доменне ім'я із торговельною маркою позивача для здійснення продажів або ремонту товарів чи щодо відповідних послуг позивача можуть добросовісно пропонувати товари або послуги і, відповідно, мати законний інтерес щодо доменного імені. Комісія проте приходиться до висновку, що для цього мають виконуватись всі наступні умови:

- (i) відповідач має насправді пропонувати відповідні товари або послуги;
- (ii) відповідач має використовувати відповідний веб-сайт лише для продажу товарів або послуг із торговельною маркою позивача;
- (iii) відповідний веб-сайт має правдиво та явно розкривати характер взаємовідносин реєстранта із власником торговельної марки; та
- (iv) відповідач не має намагатись «застовпити» доменні імена, які відображають відповідну торговельну марку.

При цьому наведене не має застосовуватись, коли існувала пряма чи опосередкована домовленість між сторонами щодо дозволу чи заборони реєстрації або використання доменного імені, що включає торговельну марку позивача. Аналогічна позиція також висловлена у розділі 2.8 Огляду ВОІВ 3.0 і відома загалом як *Okі Data* тест.

У даній справі Комісія встановила, що дії Відповідача не відповідають, принаймні, (ii) та (iii) вищенаведеним критеріям, оскільки Відповідач пропонував на своєму веб-сайті також продукцію інших виробників, окрім продукції Позивача, а також ніде не вказував,

що не є авторизованим партнером Позивача. Відповідно, Відповідач не має законного інтересу щодо спірного доменного імені.

Крім того, з врахуванням природи спірного доменного імені, яке є тотожним із торговельною маркою Позивача, виникає високий ризик його сприйняття як потенційно афілійованого з Позивачем. В цілому використання Відповідачем спірного доменного імені не може розцінюватись як «добросовісне», якщо таке використання оманливо вказує на афілійованість із власником торговельної марки (див., наприклад, *Google LLC проти Александр Дмитрович Бутенко*, справа ВОІВ № DUA2020-0009).

Враховуючи все вищенаведене, Комісія прийшла до висновку, що Відповідач не має прав або законних інтересів стосовно спірного доменного імені. Відповідно, Позов відповідає вимогам параграфу 4(a)(ii) Політики .UA.

С. Зареєстроване або використовується недобросовісно

Відповідно до параграфу 4(b) Політики .UA зазначені далі обставини (включно, але без обмежень) у разі виявлення їх Комісією вважаються доказом недобросовісної реєстрації або використання доменного імені:

(i) обставини, що вказують на те, що ви зареєстрували або придбали доменне ім'я в першу чергу з метою продажу, здавання в оренду або передачі реєстрації доменного імені іншим чином позивачеві, який є власником знака для товарів та послуг, або конкурентові такого позивача, за ціною, що перевищує ваші документовані витрати, безпосередньо пов'язані з доменним ім'ям; або

(ii) ви зареєстрували доменне ім'я, щоб перешкодити власнику знака для товарів та послуг відобразити його знак у відповідному доменному імені, за умови, що ви задіяли схему такої поведінки; або

(iii) ви зареєстрували доменне ім'я в першу чергу з метою порушення звичного ходу бізнесу конкурента; або

(iv) використовуючи доменне ім'я, ви навмисне намагалися з комерційною метою привабити користувачів Інтернету на ваш веб-сайт або інший об'єкт онлайн, створюючи оманливу подібність із знаком позивача в контексті джерела, спонсорства, приналежності або схвалення вашого веб-сайту чи об'єкта, продукту чи послуги на вашому веб-сайті або об'єкті.

Комісія встановила, що у даній справі, мали місце принаймні обставини вказані у п.(iv) вище, що свідчить про недобросовісність.

Також Комісія встановила, що використання Відповідачем спірного доменного імені для пропонування для продажу продукції Позивача свідчить про те, що на час реєстрації спірного доменного

імені Відповідач чітко і ясно знав та націлювався на раніше зареєстровану та знану торговельну марку Позивача, що свідчить про недобросовісність. Аналогічна позиція також висловлена комісіями у попередніх справах UDRP (див., наприклад, MichaelKors (Switzerland) InternationalGmbH. проти MinakovaMaria, справа BOIB № DUA2020-0002).

Враховуючи все вищенаведене, Комісія прийшла до висновку, що оспорюване доменне ім'я було зареєстроване та використовується недобросовісно. Відповідно, скарга Заявника відповідає вимогам параграфу 4(a)(iii) Політики .UA.

7. Рішення

Враховуючи вищенаведене, відповідно до параграфів 4(i) Політики .UA та 15 Правил .UA Комісія вирішила, що спірне доменне ім'я <jbl.com.ua> має бути передделеговане Позивачу.

Тарас Кислий

Одноосібний член Комісії

Дата: 2 серпня 2020 р.

Список використаних джерел

1. Role of the Domain Name System (DNS), J.C. Klensin, J. Klensin (February 2003).

2. ICANN CEO Talks About the New Affirmation of Commitments, інтерв'ю, URL:<https://www.icann.org/news/announcement-2009-09-30-en>.

3. «Management of Internet Names and Addresses». United States Department of Commerce — via ICANN.org.

4. «What are UN specialized agencies, and how many are there?». Dag Hammarskjöld Library, 11 March 2018.

5. «Management of Internet Names and Addresses». United States Department of Commerce — via ICANN.org.

6. «Uniform Dispute Resolution Policy (UDRP) Complaints», Adlex Solicitors, URL:<https://www.adlexsolicitors.co.uk/what-we-do/disputes/domain-names/udrp/>. WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Third Edition («WIPO Jurisprudential Overview 3.0»). URL:<https://www.wipo.int/amc/en/domains/search/overview3.0>.

7. Blog — 23/05/2016. Intellectual Property. Court Confirms Principles to be Applied in Domain Name Cases URL:<https://www.edwin-coe.com/blogs/main/court-confirms-principles-applied-domain-name-cases>.

Коноваленко В. В.,
директор ГО «Товариство популяризації знань
про інтелектуальну власність»

ЕЛЕКТРОННА СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ «KNOWLEDGE TO ROYALTY CONVERTER»: ВІД ПОСЛУГ ДО РОЯЛТІ

*Хто весь день працює, тому ніколи заробляти гроші.
Джон Рокфеллер*

Більшість наукових (науково-педагогічних) працівників, юристів та інші фізичних осіб, які володіють професійними знаннями в сфері інтелектуальної власності, прочитавши цей вислів Джона Рокфеллера, не відразу зрозуміють про що йде мова, оскільки вважають, що чим більше будуть працювати, надаючи послуги, тим більше будуть заробляти.

Але поміркувавши над цими мудрими словами, зрозуміють головне, що праця повинна створювати активи, які дозволяють отримувати пасивний дохід від його використання, наприклад, твір, за використання якого виплачується авторська винагорода (рояліті).

Запинимось на традиційному способі надання онлайн послуг у сфері інтелектуальної власності.

Зазвичай онлайн послуги здійснюються шляхом письмового звернення клієнта через зворотний зв'язок з питанням, на який дається письмова відповідь.

У зв'язку з тим, що питання ставить клієнт, який не є фахівцем в сфері інтелектуальної власності, то для підготовки відповіді на поставлене питання доводиться задавати додаткові питання, щоб з'ясувати суть проблеми. На все це потрібен час.

Такі онлайн консультації мають наступні недоліки.

У зв'язку з тим, що така онлайн консультація є індивідуальною, то вона не може використовуватися багаторазово.

Крім того, є складність з оплатою таких онлайн консультацій і тому така форма роботи з клієнтом використовується в основному як інструмент пошуку потенційних клієнтів, з якими укладається договір для надання повноцінних юридичних послуг.

Онлайн консультування як об'єкт авторського права.

Для того щоб отримувати пасивний дохід у вигляді рояліті, онлайн консультацію треба перетворити в об'єкт авторського права і організувати збір коштів.

Для вирішення цих задач використовується електронна система підтримки прийняття рішень (ЕСППР) «Knowledge to royalty converter», в якій можна створювати онлайн консультації двох видів:

- онлайн консультацію, основним елементом якої є онлайн тести;
- онлайн консультацію, основним елементом якої є конструктор документів.

Зупинимось на онлайн консультаціях, основним елементом яких є онлайн тести.

Результати тестування виводяться на дисплей у табличній формі, в якій відображені поставлені запитання і вибрані відповіді, а також даються рекомендації щодо усунення наявних проблем. Ця таблиця є об'єктом авторського права.

Слід зазначити, що один тест може мати сотні результатів тестування, оскільки на будь-яку комбінацію питань і відповідей на поставленні питання користувач має отримати консультацію.

Так, онлайн консультація «Уточнення особи, яка має право подати заявку на отримання патенту на службовий винахід (корисну модель)» [1] має 120 варіантів результатів тестування, що дозволяє охопити 100 процентів винахідників та їх роботодавців у питанні приналежності права на подачу заявки на отримання патенту на службовий винахід (корисну модель).

Приклад результатів тестування наводиться.

Результати тестування

Дата: 21.11.2020 р. 13:18:31

№ варіанта: 86

В онлайн консультації може бути будь-яка кількість онлайн тестів.

Слід зазначити, що на відміну від послуги, онлайн консультація як об'єкт авторського права створює монополію, яка дозволяє правовласнику онлайн консультації отримувати пасивний дохід у вигляді роялті.

З прикладами таких онлайн консультацій в сфері інтелектуальної власності можна ознайомитися на вебсайті «Територія інтелектуального капіталізму» [2].

Питання	Відповідь	Результати тестування
Питання 1. При яких умовах створено службовий винахід (корисна модель)?	Винахід (корисна модель) створено у зв'язку з виконанням службових обов'язків або доручення роботодавця	У зв'язку з тим, що в трудовому договорі нічого не записано про належність майнових прав на винахід (корисну модель), то майнові права на винахід (корисну модель) належить винахіднику і роботодавцю спільно (частина 2 ст. 429 Цивільного кодексу України). Це означає, що одним із заявників має бути винахідник. Якщо винахідник не передав третій особі права на реєстрацію винаходу (корисної моделі), то його права порушені.
Питання 2. Яку форму має трудовий договір (контракт), укладений з винахідником?	Трудовий договір має форму заяви про прийом на роботу і наказу про зарахування в штат підприємства	Використовуючи право на реєстрацію винаходу (корисної моделі), винахідник може стати співвласником патенту, домовившись з третьою особою, або подавши позовну заяву про включення його до заявники на реєстрацію винаходу (корисної моделі). Якщо винахідник передав третій особі права на реєстрацію винаходу (корисної моделі), то його права не порушуються.
Питання 4. Які дії здійснив роботодавець протягом 4 місяців після одержання від винахідника повідомлення про створення винаходу (корисної моделі)?	Роботодавець передав право на реєстрацію винаходу (корисної моделі) третій особі	У зв'язку з тим, що третя особа не подала заявку на реєстрацію винаходу (корисної моделі), то права винахідника та роботодавця можуть бути порушені. Необхідно перевірити, чи не порушує третя особа умов договору, за яким йому передані права на реєстрацію винаходу (корисної моделі). В разі порушень умов договору, прийняти відповідні заходи.
Питання 5. Чи подала третя особа заявку на реєстрацію винаходу (корисної моделі)?	Ні	У зв'язку з тим, що роботодавець не уклав договір про виплату винагороди у встановлений законом строк, то у відповідності з частиною 4 статті 9 Закону України «Про охорону прав на винаходи і корисні моделі» до винахідника перейшло право на реєстрацію винаходу (корисної моделі). Користуючись тим, що роботодавець порушив права винахідника на реєстрацію винаходу (корисної моделі), він може запропонувати роботодавцю внести зміни в договір про виплату винагороди.
Питання 6. Чи використовується третьою особою винахід (корисна модель)?	Ні	У тому разі, якщо роботодавець відмовиться внести зміни в договір про виплату винагороди, то слід звернутися до суду з відповідною позовною заявою.
Питання 9. В який термін роботодавець уклав з винахідником договір про виплату винагороди?	Після чотирьох місяців з дати отримання повідомлення про створення винаходу (корисної моделі)	

Онлайн консультація, основним елементом якої є конструктор документів.

В онлайн консультації може бути будь-яка кількість конструкторів документів, кожен з яких дозволяє створити, відредагувати, зберегти в файл і роздрукувати договір або будь-який інший документ в інтерактивному режимі.

Конструктор договорів охороняється авторським правом як комп'ютерна програма.

З прикладами конструкторів договорів з авторського права можна ознайомитися на вебсайті «Територія інтелектуального капіталізму» [3].

Кабінет редактора — місце для творчості.

В ЕСППР є кабінет редактора, в якому вчені, юристи та інші професіонали конвертують знання в об'єкти авторського права.

В кабінеті редактора містяться інструментальні засоби для створення онлайн консультацій та відображається інформація про передплату на онлайн консультації, її вартість, розмір винагороди, яку отримує автор за використання об'єктів авторського права, та інша корисна інформація, яка дозволяє автору контролювати грошовий потік від надання онлайн консультацій.

Базовими мовами створення онлайн консультацій є українська та російські мови, з машинним перекладом відповідно на російську і українські мови з подальшим редагуванням тексту.

Існує можливість ілюструвати питання і відповіді на них малюнками і фотографіями та підключити до редагування онлайн консультації літературного редактора.

Онлайн консультація може створюватися декількома авторами, які стають співавторами твору.

ЕСППР підтримує роботу колл-центру, з якого автор або особи, яких автор реєструє в кабінеті редактора, можуть вести обговорювання результати тестування в режимі інтернет-чату з користувачами онлайн консультацій.

Модель бізнесу, яку підтримує ЕСППР [4].

ЕСППР підтримує модель онлайн бізнесу, суб'єктами якого є автори-юристи (створюють онлайн консультації українською або російською мовами), партнери (залучають авторів-юристів для створення онлайн консультацій і здійснюють передплату), посередники (надають партнеру послуги з передплати), передплатники.

Керує таким онлайн бізнесом партнер, який є суб'єктом підприємницької діяльності (СПД) і до якого стікаються всі грошові потоки, які він розподіляє між правовласником ЕСППР, авторами-юристами і посередниками.

Схема генерації пасивного доходу у вигляді роялті.

Пасивний дохід генерується за рахунок надання СПД платних онлайн консультацій.

ЕСППР підтримує два види передплати на онлайн консультації.

1) Передплата онлайн консультацій для однієї особи.

Такі онлайн консультації мають невелику ціну (декілька сотень гривень) і стають доступними користувачеві з дати оплати рахунку, сформованого під час оформлення передплати, через систему LiqPay.

2) Передплата онлайн консультацій для групи осіб.

Такі онлайн консультації можуть використовувати до 20 найманих працівників особи, яка здійснила передплату на онлайн консультації. Онлайн консультація стає доступною користувачеві з дати оплати, здійсненої відповідно до умов договору.

Передплату можна здійснювати на термін від 1 до 12 місяців.

У схемі генерації пасивного доходу задіяні:

- автори (вчені, юристи та інші професіонали), які створюють онлайн консультації;
- СПД (здійснюють передплату на онлайн консультації),
- посередники (надають СПД послуги з передплати на онлайн консультації),
- передплатники (використовують онлайн консультації).

Зупинимося на договірних відносинах між суб'єктами онлайн бізнесу, створеному на базі ЕСППР.

Між правовласником ЕСППР і партнерами укладається договір на надання послуг, відповідно до якого правовласник ЕСППР здійснює адміністрування онлайн консультацій. За надані послуги правовласнику ЕСППР виплачується винагорода у відсотках від вартості підписки на онлайн консультації.

Договір на надання послуг також укладається між правовласником ЕСППР і вченим (юристом), відповідно якого фахівець отримує доступ до кабінету редактора.

Договірні відносини між партнером і авторами онлайн консультацій.

У зв'язку з тим, що створення онлайн консультацій не входить в коло службових обов'язків наукових (науково-педагогічних) працівників, то виключні майнові права на онлайн консультації належать авторам.

Онлайн консультації можуть створюватися науковими (науково-педагогічними) працівниками в порядку особистої ініціативи або за договором про створення за замовленням і використання об'єкта права інтелектуальної власності. Цей договір автор може укладати з будь-яким партнером.

Онлайн консультації створені в порядку особистої ініціативи використовуються згідно ліцензійних договорів, який партнер укладає з авторами.

За використання онлайн консультацій автору виплачується винагорода, розмір якої визначається у договорі у відсотках від вартості підписки на онлайн консультацію.

Між партнером і посередниками укладається договір на надання послуг з підписки на онлайн консультації. За надані послуги посереднику виплачується винагорода у відсотках від вартості підписки на онлайн консультації.

Користувач використовує онлайн консультації відповідно до ліцензійного договору.

Загальна схема договірних відносин між суб'єктами бізнесу, підтримуваного ЕСППР наводиться.



Список використаних джерел

1. Вебресурс: <https://konovalenko.zp.ua/tests/user/tests.php?cat=308&anid=1&lid=1>.
2. Вебресурс: <https://konovalenko.zp.ua/tests/subscribe.php?key=KWXSzKW0>.
3. Вебресурс: <https://konovalenko.zp.ua/tests/subscribe.php?key=Krk0jwC>.
4. Гуйтур М.М., Коноваленко В.В., Коловський А.С. Як науковим (науково-педагогічним працівникам) перетворити свої знання на пасивний дохід у вигляді роялті. // Вища школа. Київ, 2017. №8. ст. 112-123.

*Лавренчук Т. М.,
юрист, адвокат АО «ІНПРАКСІ»*

ЕЛЕКТРОННІ ДОКАЗИ: ТРАНСФОРМАЦІЯ МЕТОДІВ ТА СПОСОБІВ ДОКАЗУВАННЯ

В епоху цифрових технологій та постійного розвитку засобів комунікації трансформуються і методи та способи доказування обставин в ході судового процесу. Зокрема значного поширення набирає доказування з використанням електронних доказів.

Водночас, розвиток процесуального законодавства в частині регулювання електронних доказів не є достатньо стрімким та відповідним усім вимогам сучасного суспільства.

Електронними доказами згідно з актуальним процесуальним законодавством України є інформація в електронній (цифровій) формі, яка містить дані про обставини, що мають значення для справи, зокрема:

- електронні документи (в т. ч. текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо);
- веб-сайти (сторінки);
- текстові, мультимедійні та голосові повідомлення;
- метадані, бази даних;
- інші дані в електронній формі.

Такі дані можуть зберігатися, зокрема на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в т. ч. в мережі Інтернет).

Процесуальний закон допускає подання електронних доказів учасниками процесу в таких формах:

- в оригіналі;
- в електронній копії, засвідченій електронним цифровим підписом, прирівняним до власноручного підпису відповідно до Закону України «Про електронний цифровий підпис» або іншому порядку, передбаченому законом;
- в паперовій копії, посвідченій в порядку, передбаченому законом.

Втім не всі процесуальні кодекси містять положення, що регулюють питання пов'язані з електронними доказами. Зокрема, в КПК України відповідні питання не врегульовані, натомість такі докази віднесені до категорії документів, в т. ч. матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у т. ч. електронні), порядок їх посвідчення при цьому відсутній.

Інші ж процесуальні закони, всупереч наявності відповідних положень містять низку недоліків, що істотно впливають на практику застосування такої форми доказів та їх юридичну силу.

Так, Закон України «Про електронний цифровий підпис» [1], на який міститься посилання у всіх чинних процесуальних кодексах в частині встановлення форми подання електронної копії електронних доказів, втратив чинність на підставі Закону України «Про електронні довірчі послуги» [2].

Водночас, діючі процесуальні кодекси не приведені у відповідність до вказаних законодавчих змін.

Проблемним є й відмежування оригіналу електронного доказу від його копії.

В розумінні ст. 7 Закону України «Про електронні документи та електронний документообіг» [3] кожний з електронних примірників вважається оригіналом електронного документа. Отже, копія документа, що міститься на різних носіях інформація фактично є її оригіналом.

Електронна копія ж згідно з процесуальним законом має бути засвідчена кваліфікованим електронним підписом.

Якщо подано копію (паперову копію) електронного доказу, суд за клопотанням учасника справи або з власної ініціативи може витребувати у відповідної особи оригінал електронного доказу. Якщо оригінал електронного доказу не подано, а учасник справи або суд ставить під сумнів відповідність поданої копії (паперової копії) оригіналу, такий доказ не береться судом до уваги.

Зважаючи на вищевикладене, на практиці часто виникають труднощі доказування з використанням електронних доказів.

В рамках цієї статті вважаю за доцільне окреслити тенденції судової практики, що склалися в умовах не достатньої регламентації питання щодо використання електронних доказів для доказування фактичних обставин справи.

Електронне листування

Поширеною є судова практика відхилення електронного листування як неналежного доказу у зв'язку з відсутністю електронного цифрового підпису як обов'язкового реквізиту електронного документа.

Так, Верховний Суд в постанові від 28.12.2019 р. по справі № 922/788/19 [4] дійшов висновку, що роздруковка електронного листування не може вважатись електронним документом, зважаючи на те, що електронний підпис є обов'язковим реквізитом електронного документа, який використовується для ідентифікації автора та/або підписування електронного документа іншими суб'єктами електронного документообігу.

Аналогічні висновки містяться в постановках Верховного Суду від 11.06.2019 р. у справі № 904/2882/18, від 24.09.2019 р. у справі № 922/1151/18.

Так само в постанові Верховного Суду від 16.03.2020 р. по справі № 910/1162/19 [5] містяться такі висновки: «надані позивачем копії документів не є електронними документами в розумінні положень Закону України «Про електронні документи та електронний документообіг», отже, не можуть мати юридичної сили як доказу».

Отже, з метою мінімізації ризиків відхилення судом електронного листування в якості доказу рекомендується впровадження практики використання електронного цифрового підпису в господарській діяльності та взаємовідносинах з контрагентами.

При здійсненні оцінки щодо належності та допустимості електронного листування в якості доказу використання електронного цифрового підпису не є єдиним критерієм, який береться до уваги судами.

Так, Верховний Суд в постанові від 07.11.2019 р. при розгляді справи № 908/1264/18 [6] вказав на недопустимість доказів у зв'язку з тим, що документи, які надходили на електронну скриньку позивача не містять електронного цифрового підпису особи, яка їх відправила, а електронна адреса відправника не є офіційною електронною адресою, тому ідентифікувати особу, яка є відправником електронних документів неможливо; умовами договору не передбачено листування або обміну документами засобами електронного зв'язку.

В постанові від 14.01.2020 р. по справі № 925/1082/18 [7] Верховним Судом прийнято в якості належних доказів електронні листи, направлені на офіційну електронну пошту, яка зазначена в укладеному між сторонами договорі.

В постанові Верховного Суду від 11.06.2019 р. по справі № 904/2882/18 [8] вказано на те, що для надання електронному листуванню юридичної сили в якості доказу необхідним є погодження сторонами договору порядку електронного документообігу з погодженням відповідних адрес для електронного листування та переліку осіб, уповноважених вести зазначене листування.

У зв'язку з вищевикладеним, альтернативним варіантом надання доказової сили електронному листуванню є врегулювання учасниками договірних правовідносин порядку електронного документообігу безпосередньо в укладеному між ними договорі шляхом встановлення офіційної електронної пошти, уповноважених на листування осіб та порядку документообігу.

Месенджери

Складніша ситуація з наданням доказової сили листуванню, що здійснюється з використанням месенджерів, таких як Viber,

Telegram, Whatsapp, Skype, що широко використовуються як засіб комунікації в повсякденному житті.

Верховний Суд в постанові від 04.12.2019 р. по справі № 756/11258/17 [9] при оцінці доводів щодо домовленості сторін про встановлення розміру відсотків за договором позики вказав на те, що переписка у мобільному додатку «Viber» не є належним та допустимим доказом у цій справі відповідно до статей 76–81 ЦПК.

Так само, Верховний Суд в постанові від 16.12.2019 р. по справі № 922/3128/18 [10] вказав на те, що наявні роздруківки з мобільного додатку «Viber», що містяться в матеріалах справи не є належними та допустимими доказами у розумінні ст.ст. 76–77 ГПК України.

В той же час, поширеною є й практика прийняття в якості доказів скріншотів листування в месенджерах для підтвердження повідомлення про обставини, що входять до предмету доказування по справі.

В постанові Верховного Суду від 17.04.2020 р. по справі № 905/2319/17 [11] визнано належними доказами обміну інформацією між учасниками справи скріншоти з месенджера Viber.

Верховний Суд в постанові від 25.03.2020 р. по справі № 570/1369/17 [12] вважав належними доказами скріншоти листування сторін через засоби Інтернет — зв'язку Skype та у мережі Viber.

При кваліфікації таких дій, як домашнє насильство Верховний Суд вважає належними та допустимими доказами скріншоти повідомлень з телефону та планшету, роздруківки з Viber (Постанова Верховного Суду від 13.07.2020 р. по справі № 753/10840/19 [13]).

В окремих випадках суди приймають в якості доказу факту належності особі номеру телефону, з якого було здійснено дзвінок, скріншот соц-мережі «Viber», на якому є фотокартка особи, якій належить телефон (Постанова Верховного Суду від 27.11.2019 р. по справі № 1540/3778/18 [14]).

Проблемним в застосуванні скріншотів листування, що здійснювалось з використанням месенджерів є те, що переважна їх більшість мають функцію видалення повідомлень у обох співрозмовників, що може призвести до неможливості підтвердження достовірності відповідних доказів шляхом їх огляду в судовому порядку.

Для уникнення таких ситуацій рекомендовано застосування процесуального права на подання заяви про забезпечення доказів шляхом їх огляду, яка може бути подана до суду як до, так і після подання позовної заяви.

Водночас, для задоволення такої заяви судом необхідним буде підтвердження належності телефонного номера особі, з якою велось відповідне листування. Такими доказами зокрема можуть бути відо-

мости з державних реєстрів, будь-які відкриті джерела, а також заяви та документи, долучені учасниками справи до матеріалів справи.

Так само, суд за заявою учасника справи чи з власної ініціативи може оглянути веб-сайт (сторінку), інші місця збереження даних в мережі Інтернет з метою встановлення та фіксування їх змісту. У разі необхідності для проведення такого огляду суд може залучити спеціаліста.

Крім того, суд може призначити експертизу для встановлення та фіксування змісту веб-сайту (сторінки), інших місць збереження даних в мережі Інтернет за умови, якщо це потребує спеціальних знань і не може бути здійснено судом самостійно або із залученням спеціаліста.

Соціальні мережі

Проблеми доказування виникають і при використанні скріншотів з соціальних мереж, у зв'язку з неможливістю ідентифікації особи, якою здійснено ту чи іншу публікацію.

Розглядаючи скріншоти з соціальних мереж в якості доказу суди часто приходять до таких висновків: «в соціальних мережах може зареєструватися будь-яка людина і під будь-яким іменем. Перевірити таку інформацію неможливо, а тому вона є недопустимим та неналежним доказом» (Постанова Верховного Суду від 27.11.2019 р. по справі 667/266/15-ц [15]).

Як і у випадку з скріншотами з месенджерів, дієвим способом фіксації змісту веб-сторінки та протидії видаленню запису, розміщеного в соціальній мережі для приховування доказів може бути огляд відповідного доказу судом в порядку забезпечення доказів, або ж проведення судової експертизи.

Невідповідність змісту скріншота веб-сторінки може бути самостійною підставою для проведення експертизи з метою визначення факту внесення змін до інформації, розміщеної на відповідній веб-сторінці або ж фальсифікації скріншота, наданого в якості доказу по справі.

Аудіо- та відеозаписи

Аудіозаписи в якості електронних доказів також мають ряд недоліків пов'язаних з труднощами доказування.

Учасники процесу мають бути готові до того, що у разі наявності заперечень інших учасників та сумнівів щодо факту належності голосу, зафіксованого на пристрої запису конкретній особі — ідентифікація особи, якій належить такий голос може бути здійснена виключно шляхом проведення експертизи.

Верховний Суд в постанові 22.08.2019 р. по справі № 712/8320/15-к [16] погодився із висновками судів про відсутність

достатніх і допустимих доказів, якими б підтверджувалися ті факти, що голос на аудіозаписах належить особі, у зв'язку з тим, що судова фоноскопічна експертиза, клопотань про призначення такої експертизи заявлено не було.

Поряд з цим, особа, що заперечує факт належності конкретній особі голосу, запис якого наданий в якості доказу, має вчиняти певні процесуальні дій, необхідні для спростування відповідного доказу.

Так, згідно постанови Верховного Суду від 25.08.2020 р. № 553/1268/15-ц [17] визнання аудіозапису речовим доказом є правомірним у разі відсутності переконливих аргументів і доказів, які б ставили під сумнів допустимість аудіозапису як доказу та не заявленні учасниками справи клопотань про призначення у справі фонетичної експертизи для спростування відповідного доказу.

Більше того, нерідко виникають випадки, в яких учасниками справи заперечується достовірність аудіозаписів наданих в якості доказу та вказується на їх фальсифікацію шляхом монтажу. Для спростування вказаних обставин також проводиться судова експертиза.

Складнощі виникають і з використання аудіозапису телефонної розмови в якості доказу.

Вирішуючи питання про допустимість аудіозаписів телефонних розмов суди керуються висновками, що містяться в Рішенні Конституційного суду України у справі за конституційним поданням Служби безпеки України щодо офіційного тлумачення положення ч. 3 ст. 62 Конституції України № 12 – рп/2011 від 20.10.2011 р. [18] та оцінюють відповідні докази як такі, що є недопустимими та порушують встановлене ст. 32 Конституції України [19] право на таємницю телефонних розмов.

Так, Другий апеляційний адміністративний суд у постанові від 27.09.2019 р. по справі № 520/5474/19 [20] вказав на те, що здійснення звукового запису голосу особи без її згоди порушує право на охорону інтересів особи. Голос фізичної особи належить до прояву особистого характеру, що охороняється, його звуковий запис можна здійснювати або використовувати тільки з відома фізичної особи.

Відеозаписи в якості електронних доказів аналогічно до аудіозаписів мають свої недоліки.

Як підтверджується постановою Верховного Суду від 12.06.2018 р. по справі № 908/1120/17 [21] для оцінки належності відеозапису як доказу береться до уваги наявність в ньому необхідних реквізитів електронного доказу, таких як фіксація дати та часу зйомки, місця події.

Питання щодо автентичності відеозапису та відсутності в ньому монтажу вирішується шляхом призначення судової експертизи.

На практиці часто виникають проблеми з неможливістю виявити ознаки монтажу навіть шляхом проведення судової експертизи у разі, якщо використовується копія аудіозапису чи відеозапису, а не їх оригінал (Постанова Верховного Суду від 31.10.2019 р. по справі № 404/700/17 [22]).

Новим способом забезпечення електронної доказової бази в рамках судового спору може стати нова онлайн-система WIPO PROOF [23], запроваджена Всесвітньою організацією інтелектуальної власності (ВОІВ) в травні 2020 р., в рамках якої генерується захищене від несанкціонованого доступу свідоцтво, яке підтверджує існування цифрового файлу в конкретний момент часу, а також факт його незмінності з відповідного моменту, що називається токен WIPO PROOF. До цього часу судової практики з використанням такої доказової бази не сформовано.

Зважаючи на вищевикладене, процесуальне законодавство потребує адаптації до умов сьогодення та більш детальної регламентації з метою усунення значної кількості прогалин, що ускладнюють процес доказування фактичних обставин шляхом використання електронних доказів.

Список використаних джерел:

1. Про електронний цифровий підпис: Закон України від 22.05.2003 року// Офіційна інтернет-сторінка Верховної Ради України. URL: <https://zakon.rada.gov.ua/laws/show/852-15#Text>.
2. Про електронні довірчі послуги: Закон України від 05.10.2017 року [Електронний ресурс] // Офіційна інтернет-сторінка Верховної Ради України. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>.
3. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 року// Офіційна інтернет-сторінка Верховної Ради України. URL: <https://zakon.rada.gov.ua/laws/show/851-15#Text>.
4. Постанова Верховного Суду від 28.12.2019 року по справі №922/788/19. URL: <https://reyestr.court.gov.ua/Review/86717260>.
5. Постанова Верховного Суду від 16.03.2020 року по справі №910/1162/19. URL: <https://reyestr.court.gov.ua/Review/88244984>.
6. Постанова Верховного Суду від 07.11.2019 року по справі №908/1264/18. URL: <https://reyestr.court.gov.ua/Review/85470804>.
7. Постанова Верховного Суду від 14.01.2020 року по справі №925/1082/18 URL: <https://reyestr.court.gov.ua/Review/87056348>.
8. Постанова Верховного Суду від 11.06.2019 року по справі №904/2882/18. URL: <https://reyestr.court.gov.ua/Review/82426143>.

9. Постанова Верховного Суду від 04.12.2019 року по справі №756/11258/17. URL: <https://reyestr.court.gov.ua/Review/86435419>.
10. Постанова Верховного Суду від 16.12.2019 року по справі №922/3128/18. URL: <https://reyestr.court.gov.ua/Review/86619089>.
11. Постанова Верховного Суду від 17.04.2020 року по справі №905/2319/17. URL: <https://reyestr.court.gov.ua/Review/88842957>.
12. Постанова Верховного Суду від 25.03.2020 року по справі №570/1369/17. URL: <https://reyestr.court.gov.ua/Review/88602149>.
13. Постанова Верховного Суду від 13.07.2020 року по справі №753/10840/19. URL: <https://reyestr.court.gov.ua/Review/90385050>.
14. Постанова Верховного Суду від 27.11.2019 року по справі №1540/3778/18. URL: <https://reyestr.court.gov.ua/Review/85934103>.
15. Постанова Верховного Суду від 27.11.2019 року по справі 667/266/15-ц. URL: <https://reyestr.court.gov.ua/Review/86207417>.
16. Постанова Верховного Суду 22.08.2019 року по справі №712/8320/15-к. URL: <https://reyestr.court.gov.ua/Review/84092501>.
17. Постанова Верховного Суду від 25.08.2020 року по справі №553/1268/15-ц. URL: <https://reyestr.court.gov.ua/Review/91260411>.
18. Щодо офіційного тлумачення положення частини третьої статті 62 Конституції України: Рішення Конституційного Суду України від 20.10.2011 № 12-рп/2011// Офіційна інтернет-сторінка Верховної Ради України. URL: <https://zakon.rada.gov.ua/laws/show/v012p710-11#Text>.
19. Конституція України: Закон України від 28.06.1996 // Офіційна інтернет-сторінка Верховної Ради України. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>.
20. Постанова Другого апеляційного адміністративного суду у постанові від 27.09.2019 року по справі №520/5474/19. URL: <https://reyestr.court.gov.ua/Review/83957142>
21. Постанова Верховного Суду від 12.06.2018 року по справі №908/1120/17. URL: <https://reyestr.court.gov.ua/Review/74671049>.
22. Постанова Верховного Суду від 31.10.2019 року по справі №404/700/17. URL: <https://reyestr.court.gov.ua/Review/85390646>.
23. WIPO PROOF: TRUSTED DIGITAL EVIDENCE FOR YOUR INTELLECTUAL ASSETS// Офіційна інтернет-сторінка ВОІВ. URL: <https://wipoproof.wipo.int/wdts/>.

*Логвиненко М. І.,
к.ю.н., доцент кафедри АГПФЕБ ННІ права
Сумського державного університету*
*Диковець А. В.,
аспірантка кафедри АГПФЕБ ННІ права
Сумського державного університету*

ЗАХИСТ ОБ'ЄКТІВ АВТОРСЬКОГО ПРАВА ЗА ДОПОМОГОЮ ТЕХНОЛОГІЇ BLOCKCHAIN

Інтернет та цифрові технології створили новий онлайн — світ, який має як позитивну, так і негативну сторону. З позитивної сторони, Інтернет відкриває нові ринкові можливості, серед яких вільне розповсюдження автором результатів своєї інтелектуальної діяльності, але з іншої сторони, більшість авторів піддаються дуже високому ризику неконтрольованого копіювання результатів їхньої творчої діяльності та використання інформації без їх згоди.

Сьогодні, інтелектуальна власність стає доступною для кожного, хто має на меті скопіювати, відтворити або скопіювати об'єкт інтелектуальної власності (наприклад, твір). Оскільки, з появою Всесвітньої мережі Інтернет, змінився і спосіб взаємодії користувачів із об'єктами права інтелектуальної власності. Раніше, ми, як споживачі певної продукції, мали змогу здійснити покупку лише в звичайному магазині або скориставшись послугами, які надає Інтернет — магазин. Тепер, той самий продукт, а саме об'єкт інтелектуальної власності, можна замовити зовсім безкоштовно за допомогою веб — мережі на свої гаджети: комп'ютери, смартфони або планшети.

Захист та охорона прав авторів завжди були досить складним явищем в сфері інтелектуальної власності, а поява онлайн — світу ще більше ускладнила цей «взаємозв'язок». Це пояснюється тим, що більшість прав авторів, або ігнорувалися, або піддавалися порушенню. Серед таких порушень часто зустрічаються:

1. Несанкціоноване копіювання тексту або зображення. Досить поширеною формою порушення авторських прав є пряме несанкціоноване копіювання захищених текстових або графічних зображень у творі, який поширюється серед публіки. Законодавство про авторське право дозволяє часткове копіювання, але якщо користувач цитує матеріал та зазначає у своєму творі автора тексту чи зображення. Незаконне копіювання як одна з проблем захисту авторського права завдає значної шкоди авторам книг, фільмів, авторам та виконавцям музичних творів, оскільки перешкоджає їм

отримувати доходи за їхню діяльність та утримує їх відподальшого інвестування в творчу діяльність, що може навіть підірвати розвиток тієї чи іншої сфери творчої діяльності [1, с. 236].

2. Завантаження на веб-ресурс твору без дозволу автора. Інтернет надає безліч можливостей для легкого порушення авторських прав. Окрім безпосереднього копіювання тексту або зображень на іншу веб-сторінку, кожен, хто завантажує зображення для власного користування або завантажує до своєї веб-сторінки, також порушує авторські права. Щоб уникнути порушення авторських прав, другий користувач повинен отримати дозволу від автора твору на використання тексту, зображення чи іншого об'єкта.

3. Цифрове відтворення та відображення. Несанкціоноване завантаження матеріалів, захищених авторським правом, є ще однією загальною формою порушення авторських прав. У той час як музичні та відеофайли продаються через Інтернет для особистого користування, копіювання, продаж або розповсюдження файлу без дозволу являє собою порушення авторських прав. Це правда, незалежно від того, чи ви платите за роботу. Будь-яке відображення зображення чи тексту з захищеної авторським правом твору для рекламних цілей також є порушенням авторських прав, як і використання цього матеріалу в рекламі, футболці або банері.

4. Ксерокопіювання. Використання фотокопії для відтворення книги, журнальної статті чи будь-якого іншого друкованого матеріалу, захищеного авторським правом, є порушенням авторських прав, крім випадків, коли копіювання виконується для суто особистого використання. Наприклад, законодавство про авторське право дозволяє обмежувати копіювання матеріалу для використання в освітніх цілях, наприклад, поширення матеріалу з книги під час лекції студентам [2].

Нелегальний обмін об'єктами авторського права, використання захищеного авторським правом контенту завжди залишалося і залишається серйозною проблемою. Тому, виникає питання, чи може ця проблема, знайти своє вирішення завдяки використанню технології «blockchain»?

Blockchain — це децентралізована система зберігання даних або цифровий реєстр транзакцій, угод, контрактів [3].

Blockchain працює наступним чином: усі транзакції за допомогою складних математичних алгоритмів об'єднуються в «блоки», які потім зв'язуються криптографічно і хронологічно в «ланцюг» та мають певний хеш (цифровий пароль) попереднього блоку. Транзакція при цьому здійснюється лише тоді, коли вважається підтвердженою [4].

Blockchain може слугувати певним захистом від хакерів, які мають на меті проникнути в систему. Захист полягає в тому, що для проникнення в систему побудовану на «blockchain» необхідно мати доступ до баз даних на всіх комп'ютерах одночасно, а це в даному випадку нереально.

М. Свон виділяє три умовні сфери застосування технології блокчейн:

1. blockchain 1.0 — валюта;
2. blockchain 2.0 — контракт;
3. blockchain 3.0 — додатки, що працюють за рамками фінансових транзакцій і ринків (поширюються на сфері державного управління, охорони здоров'я, науки, освіти та ін.) [5, с. 20].

Прикладом використання контракту, як одного із сфер застосування «blockchain» є сам «smart-contracts» (контракт), який містить умови щодо використання цифрового об'єкта авторського права, наприклад, фотографії. Використанням валюти в зазначеній сфері може слугувати «bitcoin». За рахунок використання зазначеної криптографічної валюти, платформа може здійснювати виплату роялті. Завдяки цифровому кодуванню прав автора, виплата роялті є більш надійною та ефективною. Наприклад, у випадку виникнення спору з приводу невиплати роялті, дані щодо проведення платежів, які знаходяться в «blockchain», можуть бути використані як доказ підтвердження здійснених платежів або ж навпаки, свідчити про їх відсутність.

Вже сьогодні існують платформи з продажу музичних творів, побудовані на системі «blockchain», такі як PeerTracks, Bittunes і UjoMusic. Peertracks використовує дану технологію для створення системи торгівлі акціями для виконавців, Bittunes мають за мету створити музичний ринок, вільний від посередників, а UjoMusic має намір розробити систему для вирішення проблем, пов'язаних зі схемою розподілу гонорарів і ліцензування [6]. Перелічені організації вважають, що в майбутньому виконавці будуть розміщувати аудіофайли з особистим ID (ідентифікатором) в «blockchain», точно так, як зараз це відбувається з криптовалютами. Реалізація даної платформи дозволить автору самостійно відстежувати число завантажень твору та контролювати виплату винагороди без посередників.

Не можна не погодитися з думкою науковців, які вважають, що технологія Blockchain може слугувати підтвердженням авторського права на твір, який незареєстрований в порядку, передбаченому законодавством. Оскільки, завантаження твору з певною інформацією про автора в «blockchain» вже є фіксацією авторства. На практиці це здійснюється так: за допомогою спеціального сервісу, на-

приклад, «ProofofExistence», завантажений файл з твором хешується, а результат (унікальний відбиток хеш — файлу) заноситься в blockchain. В такому записі зберігаються тимчасові мітки (time-stamps), в які неможливо внести зміни. Неможливість внесення змін в ланцюгу, є підтвердженням того, що файл (наприклад, твір) був завантажений реальним автором в конкретний момент часу.

Отже, можна стверджувати, що в порівнянні з депонуванням творів, технологія «blockchain» спрощує та скорочує процедуру фіксації факту авторства. Крім того, запис, залишений автором в «blockchain» залишається в реєстрі незалежно від існування організації — депозитарію.

Однак, виникає питання, чи українські судові органи зможуть прийняти таке підтвердження авторства як доказ?

Наприклад, у східно-китайському місті Гуанчжоу було створено Інтернет-суд, який займатиметься питаннями та суперечками, пов'язаними з Інтернетом. Нова структура буде використовувати блокчейн для боротьби з плагіатом в інтернет-авторів.

На думку китайського судді WangJiangqiao, децентралізований характер Blockchain гарантує цілісність даних, оскільки розподілений реєстр безпечно зберігає всі записи та цифрові сліди, включаючи авторство, час створення, зміст та докази порушення прав. Зважаючи на незмінність Blockchain, ці записи можуть мати правовий вплив [7].

Деякі компанії вже почали використовувати технологію Blockchain. Наприклад, веб-сайт Binded, створений компанією із Сан-Франциско, дозволяє художникам захищати створені ними оригінальні зображення. Художник повинен просто зареєструватися та завантажити свої роботи. Потім робота зберігається на блокчейні. Також художник отримує сертифікат, що підтверджує справжність зображення. Однак завантаження зображення на веб-сайт і отримання сертифіката не реєструє роботу художника в Бюро авторських прав США. Художникові все одно доведеться виконати певні формальності, щоб виграти відшкодування збитків у судовому процесі в США [8].

На нашу думку, технологія «blockchain» — це одна з революційних технологій, яка матиме неабиякий вплив на наше життя в найближчі роки і десятиліття, а особливо в сфері захисту інтелектуальної власності.

Як нова технологія, з можливістю перевірки, збереження та відстеження цифрових даних, а також забезпечення платформи для низьких витрат та прозорості для транзакцій у глобальному масштабі, вона має можливість революціонізувати обмін цифровими акти-

вами. Проте, для реалізації такого захисту необхідно здійснити ряд дій, серед яких і створення відповідної нормативно-правової бази.

Список використаних джерел

1. Підпригора О.А., Святоцький О.Д. Основи правової охорони інтелектуальної власності в Україні: підручник. Київ: Концерн «Видавничий Дім «Ін Юре», 2003. 236 с.

2. Логвиненко М. І., Каріх І.В., Диковець А. В. Проблеми захисту об'єктів авторського права в мережі Інтернет. Правові горизонти. 2019. № 15 (28). С.23.

3. What is Blockchain Technology? A Step by Step Guide For Beginners. URL: <https://blockgeeks.com/guides/whatisblockchaintechology/>

4. What is Blockchain Technology?. URL: <http://www.coindesk.com/information/whatisblockchaintechology>.

5. Блокчейн. Схема новой экономики. Москва, 2017. 240 с.

6. Блокчейн меняет музыкальную индустрию. URL: <https://forklog.com/blokchejn-menyuet-muzykalnuyu-industriyu/>.

7. Китай обирає блокчейн в якості захисту проти онлайн-плагіату. URL: <http://coinews.io/ua/category/1-cry/article/3622-kitaj-obira%D1%94-blokchejn-vyakost%D1%96-zahistu-proti-onlajn-plag%D1%96atu>.

8. How can Blockchain protect Intellectual Property rights? URL: <https://www.avocats-mathias.com/technologies-avancees/blockchain-intellectual-property-rights>.

Сердюк О. В.,

патентний повірений України

MisterRegister- ПАТЕНТНИЙ ПОВІРЕНИЙ У СМАРТФОНІ: ОНЛАЙН СЕРВІС ДЛЯ ПОШУКУ, МОНІТОРИНГУ ТА РЕЄСТРАЦІЇ ТОРГОВИХ МАРОК

Юристи довгий час залишались за бортом автоматизації, але за останні декілька років ситуація змінилась. Разом із відкриттям державних реєстрів (відкритих даних) та появою законів про електронні документи та електронний документообіг, багато державних установ почали працювати через Інтернет. Все це обумовило бум українського legal-tech. Почали з'являтися різноманітні боти та автоматизовані сервіси, які беруть на себе рутинні процеси юристів та суттєво зменшують їх витрати часу. Не стала виключенням і сфера інтелектуальної власності.

Відкриття Укрпатентом реєстрів об'єктів інтелектуальної власності та створення системи електронної взаємодії закладу експертизи (СЕВ ЗЕС) надало учасникам ринку можливість створювати власні технологічні рішення для автоматизації діяльності патентного повіреного. Так, у кінці 2019 р. було створено прототип сервісу Mister Register, який автоматизував створення та подання електронної заявки на знак для товарів і послуг до закладу експертизи, а також проводив пошук схожих позначень серед зареєстрованих та поданих на реєстрацію знаків для товарів і послуг за національною та мадридською процедурами.

Прототип сервісу взаємодіє із користувачем через Telegram бота. Бот збирає необхідні дані, передає на сервер, який після обробки даних повертає через бота посилання на веб-сторінку із результатом обробки — результати пошуку або створену заявку на знак.

Відмінності MisterRegister від існуючих рішень (на момент написання статті).

Завдяки автоматизації більшості процесів та унікальним технічним рішенням, Mister Register зможе надати послуги швидше, дешевше, а іноді взагалі безкоштовно. Деякі послуги (наприклад пошук) Mister Register надасть якісніше, а деяких послуг в існуючих рішеннях зовсім немає. Для наглядності приводимо порівняльну таблицю.

Функція	MisterRegister	Інші
Моментальне подання заявки на ТМ без спеціальних знань та участі спеціаліста	✓	✗
Інструмент для самостійного ведення діловодства за заявками на знаки без спеціальних знань	✓	✗
Моментальний пошук ТМ по всіх базах: національна та мадридська процедури, зареєстровані ТМ та подані на реєстрацію	✓	✗
«Розумний» пошук: співзвучні, подібні, транслітеровані позначення	✓	✗
Моніторинг появи схожих ТМ за алгоритмом «розумного» пошуку	✓	✗
Моніторинг знаків певного заявника	✓	✗
Безкоштовне нагадування про закінчення терміну дії свідоцтв та патентів	✓	✗
онлайн продовження терміну дії свідоцтв та патентів в кілька кліків	✓	✗
Підбір класів МКТП за нестандартними формулюваннями	✓	✗

Розглянемо функції, які вирішує MisterRegister, більш докладно. Пошук ТМ

«Розумний» пошук дозволяє протягом кількох секунд виявити не лише ідентичні, але й співзвучні, подібні та транслітеровані знаки.

Наприклад, за запитом «фото» MisterRegister знайде не тільки «фото», а й «foto» та «photo».

Запит «атоксил» через Сервіс Mister Register виявить «atoksil», «atoks», «атоксіл», «atoxil», «atosil», «амоксил» та ін.

Пошук буде проведено не лише по базі національних заявок та реєстрацій, але й по базі заявок та реєстрації, поданих за Мадридською процедурою.

Таким чином Mister Register збереже час на формування варіацій пошукового запиту та пошук за різними джерелами.

Автоматизовані моніторинги.

Моніторинг за ключовим словом працює за алгоритмом «розумного» пошуку та повідомлятиме про всі новоподані в Україні заявки (за національною та міжнародною процедурою) на ідентичні та схожі знаки. Це дасть можливість правовласникам та їх представникам оперативно реагувати на порушення з боку третіх осіб, зокрема, вчасно подавати до Укрпатенту заперечення проти реєстрації таких знаків.

Моніторинг за певним заявником / власником — дозволить отримувати інформацію про те, заявки на які знаки подає ваш конкурент, а отже ви будете знати які товари чи послуги він планує вивести на ринок.

Це надасть можливість правовласникам та їх представникам оперативно реагувати на порушення з боку третіх осіб, зокрема, вчасно подавати до Укрпатенту заперечення проти реєстрації таких знаків.

Моніторинг термінів дії — ця послуга дозволить не пропускати щорічні терміни підтримання чинності патентів на винаходи, корисні моделі, промислові зразки та не забути про продовження термінів дії свідоцтв на знаки.

Подання заявки на знак

Mister Register надає можливість моментального прямого подання заявки на знак до Укрпатенту з використанням власного електронного цифрового підпису (ЕЦП) або ЕЦП представника — патентного повіреного, який є партнером сервісу. На відміну від подання електронних заявок безпосередньо через системи електронного подання заявок Укрпатенту, процедура не потребує спеціальних знань та є набагато простішою, зокрема при створенні переліку товарів і послуг або при накладанні ЕЦП.

Mister Register значно скорочує час на подання заявки: за 4 хвилини професійний користувач зможе ввести всі необхідні дані та отримати розписку про прийняття заявки Укрпатентом.

Додаткові переваги при поданні заявки:

- Мінімізація помилок та часу при введенні даних заявника: Mister Register отримує адресу та найменування заявника з державного реєстру (для ФОП або юридичних осіб);
- Створення зображення знаку з тексту;
- Адаптація зображення знаку для заявки, наприклад зміна розміру або конвертація кольору у градації сірого;
- Можливість платити державні збори та мито онлайн;
- діловодство за заявкою: Mister Register отримує всі документи від Укрпатенту, нагадує про строки відповіді чи сплати збору, та надає посилання для онлайн сплати збору.

Користувачі

Для власників малого та середнього бізнесу, науковців і винахідників — це своєрідна таблетка від головного болю, адже відтепер все незрозуміле, заплутане і складне, таке, що вимагає спеціальних знань процедури та строків і постійної уваги, аби їх не пропустити, стає простим та легким.

Для власників чинного свідоцтва на знак, промисловий зразок або патенту на винахід чи корисну модель — це нагода доручити боту відстежувати терміни дії охоронних документів, попереджати про їх закінчення та можливість продовження чинності.

Сервіс є незамінним помічником і для професійних користувачів — патентних повірених, юристів, адвокатів, судових експертів, суддів, маркетологів, дизайнерів, адже він скорочує до 80 % часу на рутинні процеси, такі як подання заяви на знак або пошук знаку на схожість, та нагадує про всі терміни, що особливо важливо при великій кількості об'єктів.

Водночас, деякі патентні повірені негативно сприймають ботів та автоматизовані сервіси, вбачаючи в них конкурентів або через консервативні погляди. Варто зазначити, що сьогодні ані Mister Register ані інші автоматизовані сервіси та боти ще не здатні повністю замінити патентного повіреного. Навпаки, використання останніми ботів та інших інструментів автоматизації може значно спростити діяльність та стати конкурентною перевагою. Наприклад, Mister Register вже має партнерів-патентних повірених, які вже відчули переваги автоматизації рутинних процесів.

Вартість послуги. Базова версія Mister Register безкоштовна. У ній можна тричі на місяць провести пошук і 1 раз на місяць подати заявку на реєстрацію, а також контролювати 1 знак та 1 власника, отримуючи необмежені нагадування про дію ваших торгових марок. Платити за це не потрібно. Якщо хочете реєструвати більше однієї торгової марки щомісяця, прискорювати проходження заявки, бачити висновки щодо пошуку — обирайте окремі платні послуги (від 50

грн) або передплату від 600 грн. Тобто все просто: додаєте бота @misterregisterbot в Telegram і серед його функцій обираєте ті, що хочете йому доручити. В тому числі підключити людину-консультанта за потреби. Але скоріш за все це не потрібно буде. Бот достатньо розвинений і добре «знає» свою справу. Тим, хто звик до онлайн-банкінгу, віддаленої роботи та переваг гаджетів, спілкування з ботом буде навіть зручнішим, аніж з «аналоговим» спеціалістом.

Перспективи удосконалення цифрової платформи

Сервіс MisterRegister створювався в першу чергу для звичайних користувачів, які не знайомі з нюансами пошуку, реєстрації, моніторингу торговельних марок. Тому всі процеси в ньому спрощені. Через відсутність повноцінного веб інтерфейсу, MisterRegister не здатен стати повноцінною платформою автоматизації діяльності патентного повіреного або юридичної компанії із практикою інтелектуальної власності. Але це перший крок українського LegalTech до створення української платформи управління об'єктами інтелектуальної власності, які вже багато років існують на іноземних ринках, але в Україні не використовуються через відсутність локалізації та адаптації до українського ринку.

На момент написання статті, на базі функцій Mister Register вже ведеться розробка такої удосконаленої платформи під назвою «Lexberry».

Платформа lexberry вже буде мати повноцінний веб інтерфейс та можливість керувати не тільки знаками для товарів і послуг, а й всіма видами об'єктів інтелектуальної власності, такими як промислові зразки, винаходи, корисні моделі, об'єкти авторського права. Під керуванням мається на увазі додавання та облік існуючих об'єктів, подання електронної заявки на реєстрацію нових, діловодство та обмін електронними документами із відомством, контроль всіх строків (відповідей на запити експертизи, сплати зборів, тощо).

Також lexberry дозволить реєструвати та керувати доменними іменами. Завдяки інтеграції з реєстром знаків для товарів та послуг, lexberry зможе автоматично реєструвати домени в зоні UA в день публікації відповідного знаку для товарів та послуг.

Окремою перевагою платформи lexberry слід виділити функцію пошуку позначень при реєстрації знаків для товарів та послуг. Алгоритми «розумного» пошуку будуть знаходити частково схожі позначення, аналогічно сервісу Mister Register, що було описано вище. Але пошук буде проводитись не тільки по зареєстрованим та поданим на реєстрацію знакам для товарів та послуг за національною та мадрридською процедурами, а й по ряду інших баз, таких як:

- реєстр юридичних осіб;

- добре відомі знаки;
- географічні назви;
- медичні префікси;
- абрєвіатури міжнародних організацій.

Пошук будуть проводитись за лічені секунди. Функція такого пошуку стане у нагоді не лише заявниками та їх представникам, а й експертам закладу експертизи.

Платформа lexberry буде синхронізуватись з реєстрами об'єктів інтелектуальної власності, автоматично оновлювати дані та виділяти різницю (наприклад порівнювати переліки МКТП).

Окрім функцій пов'язаних із об'єктами інтелектуальної власності, lexberry буде мати інші необхідні для повноцінної роботи модулі, такі як: біллінг, менеджмент задач, кабінет клієнта, кабінет агента (субпідрядника), шаблон і затор документів, конструктор звітів та багато іншого. Таким чином, lexberry стане інструментом автоматизації діяльності від самозайнятого патентного повіреного до крупної юридичної компанії із практикою інтелектуальної власності або компанії-власника портфелю торговельних марок чи патентів, а гнучкі тарифи будуть враховувати потреби клієнтів будь-якого розміру.

Після підключення патентних повірених до платформи lexberry, в подальших планах є створення маркетплейсу патентних повірених із повною статистикою, рейтингом та відгуками по кожному, де користувачі зможуть обрати представника у справах інтелектуальної власності та з легкістю передавати справи від одного представника іншому.

Також планується інтеграція lexberry із платформою Дія.

Взагалі, поява такого сервісу як «Mister Register» — це ще один крок до створення прозорого та здорового бізнес-середовища в Україні. Це ті самі відкриті дані, що є найактуальнішим глобальним трендом.

Нагороди. Необхідність професіоналів в подібному сервісі підтверджується і тим, що Mister Register здобув перемогу у конкурсі стартапів для юридичного бізнесу AEQUO Legal Tech Challenge 2019 р. Тож варто користуватися кращими технологічними інструментами, випереджати конкурентів та розвивати інновації!

Деякі іноземні платформи для управління інтелектуальною власністю

Назва платформи	Опис
AalbunIP	Створена індійськими розробниками на базі SugarCrm. Платформа має складний інтерфейс. В ній відсутні функції автоматичного обчислення строків та зборів для різних юрисдикцій. Також немає інтеграцій з реєстрами ОІВ та патентними відомствами країн. Компанія має власний штат помічників юристів, які вручну можуть вести додані на платформу об'єкти. Не локалізована для України
webTms	Платформа із США. Досить стара платформа, яка з'явилась у 1998 р. Має багато функцій, але незручна, має застарілий інтерфейс та дуже повільна. Інтегрується з реєстрами та відомствами деяких країн. Не локалізована для України
tmCloud	Платформа із США. Створена засновником webTms у 2006 р. Має багато функцій, в тому числі інтегрується з реєстрами та відомствами деяких країн. Має застарілий інтерфейс, незручна та складна у використанні. Не локалізована для України

Список використаних джерел:

1. Сердюк О. Патентний повірений у смартфоні: онлайн-сервіс для швидкої реєстрації ТМ // Інтелектуальна власність в Україні 2020.-№ 10.- С. 38-41.

2. Патентний повірений у смартфоні: запущено онлайн-сервіс для швидкої реєстрації ТМ. URL: <https://yur-gazeta.com/golovna/patentniy-povireniy-u-smartfoni-zapushcheno-onlajnservis-dlya-shvidkoyi-reestraciyi-tm.html>.

3. Платформа lexberry. URL: <https://lexberry.com.ua>.

Фонарьова Т. А.,

к.е.н., доц., докторант,

ORCIDID: 0000-0001-7726-6999

Петренко В. О.,

д.т.н., проф.,

ORCIDID:0000-0001-5017-1674

Бушуев К. М.,

аспірант, здобувач

ORCIDID:0000-0001-8321-4124

Національна металургійна академія України, м. Дніпро

НЕЙРОННІ МЕРЕЖІ В ІНФОРМАЦІЙНО-ТЕХНОЛОГІЧНОМУ ОБСЛУГОВУВАННІ ЮРИДИЧНОЇ ДІЯЛЬНОСТІ

Актуальність. Людство вступило до ери диджиталізації. Цифрова економіка диктує нові вимоги до планування й організації бізнес-процесів у всіх сферах діяльності вітчизняних підприємств. В наданні юридичних послуг, як і в інших видах бізнесу, постає необхідність прийняття рішень, які базуються на інформаційних, інтелектуальних ресурсах та знаннях персоналу компаній. Отже, в умовах глобальної інформатизації суспільства все більшу роль відіграє «LegalTech» (юридичні технології) — онлайн-посередництво між замовником та юридичною фірмою як для надання інструментів юридичного самообслуговування, так й задля звернення до професійних юристів. Для ефективного впровадження LegalTech, слід **враховувати специфіку організації бізнес-процесів в наданні юридичних послуг.**

З одного, боку юридичні фірми виступають суб'єктами ринкових відносин, а це означає, що менеджмент повинен будуватися на принципах маркетингу, який в свою чергу, включає моніторинг та вивчення зовнішнього середовища, дослідження та прогнозування ринку юридичних послуг, аналіз внутрішнього середовища фірми, формування цінової та рекламної політики просування юридично-правових послуг. Всі ці напрями діяльності не можливо здійснити без впровадження маркетингової інформаційної системи, яка б забезпечувала потребу у всебічній, своєчасній інформації та підтримувала прийняття рішень задля ефективної роботи з клієнтами та створення, таким чином, конкурентних переваг в умовах ринкових відносин.

З іншого боку, при розробці та впровадженні новітніх ІТ-технологій в сфері юридичної діяльності, слід враховувати специфічні ознаки юридичної послуги, а саме, те, що юридична послуга

стає такою тільки при тісній взаємодії професійного юриста та клієнта, тобто знання, досвід, інформаційні ресурси фахівця з права поєднуються з тією інформацією яку надає клієнт, його досвід, навички, дії щодо застосування порад юриста, у сумі, й створюють юридичну послугу, як інтелектуальний продукт, який має унікальність, мінливість якості, неоднорідність, комерційну таємницю [1].

Таким чином, зрозуміло, що результат юридичного обслуговування залежить не тільки від професіоналізму юриста, якостей замовника, а й від забезпеченості всього процесу потрібною й достовірною інформацією. Застосування **LegalTech** роблять юридичну послугу інноваційною, тобто здатною забезпечити новизну прийомів, методів у рішенні проблем клієнта.

Виклад основного матеріалу. Ефективна діджиталізація дозволяє застосовувати мобільні та цифрові технології, які розширюють досвід користувачів. Використання новітніх технологій у маркетинговому середовищі підприємства здійснюється в таких напрямках. По-перше, процес діджиталізації починається з перебудови інформаційної системи підприємства та створення відповідної інфраструктури. Важливо не просто знати про існування окремих інновацій в ІТ-технологіях, а аналізувати і розуміти, яким чином вони можуть взаємодіяти та адаптуватися одна до одної. По-друге, — отримання доступу до інновацій. Мається на увазі можливість інтегрувати власні розробки з придбаними готовими рішеннями. По-третє, врахування законодавства та прав інтелектуальної власності. Важливо, щоб нормативно-правовий механізм дозволяв їх впроваджувати та була можливість забезпечити захист інтелектуальної власності. Тільки так можна забезпечити швидке впровадження технологій та інновацій та швидко комерціалізацію результатів інтелектуальної діяльності і отримання конкретних економічних ефектів. По-четверте, наявність та мотивація персоналу, здатного працювати з цифровими технологіями в умовах діджиталізації. Створення умов для кар'єрного та професійного росту повинно будуватися на розробці програм інвестування в розвиток індивідуального людського капіталу кожного окремого працівника. Ці заходи запобігають процесу старіння персоналу, створюють необхідні умови розвитку та справедливої оцінки праці [2].

На погляд авторів, головним фактором успішного впровадження LegalTech, є удосконалення інформаційної системи юридичної фірми за рахунок впровадження інтелектуальної системи підтримки прийняття рішень (ІСППР) із застосуванням нейронної мережі та розгляд її можливостей в юридичній діяльності.

Застосування можливостей нейронних мереж (НМ) ще не достатньо вивчено та не набуло поширення в практиці професійних юристів. НМ стрімко завойовують все більше напрямків для їх застосування, особливо в економічній сфері. Цьому сприяє їх гнучкість, здатність до навчання, що надає розробникам велику кількість можливостей для прогнозування та моделювання різних альтернативних сценаріїв розвитку ситуації в мінливому середовищі. Отже, вони здатні навчатися на попередньому досвіді, використовуючи великі масиви інформації, моделювати тенденції й підходи і на цій основі підтримувати фахівця в прийнятті відповідних рішень.

Як відомо, засновниками штучних нейронних мереж являються В. Мак-Калох і В. Пітс, які довели, що за допомогою порогових нейронних елементів можна реалізувати обчислення будь-яких логічних функцій. Д. Хебб розробив математичну основу для навчання ряду нейронних мереж. Ф. Розенблатт запропонував і дослідив модель нейронної мережі, яку він назвав перцептроном. У 1969 р. М. Мінський і С. Пайперт опублікували монографію «Перцептрони», в якій було дано математичний аналіз перцептрона, і показані обмеження, властиві йому. Т. Кохонен розробив і дослідив як самоорганізуються нейронні мережі. Ряд авторів Д. Руммель-Харт, Д. Хінтон і Р. Вільямс запропонували алгоритм зворотного поширення помилки, саме він представляє найбільший інтерес, так як є ефективним засобом для навчання багатосарових нейронних мереж прямого поширення.

Основне призначення нейромереж полягає в тому, що на підставі аналізу великих обсягів інформації, яка відображає окремі випадки, визначаються загальні закономірності для розпізнання нових випадків. Знання, зафіксовані як ваги декількох сотень меж-нейронних зв'язків, зовсім не піддаються аналізу й інтерпретації людиною. Найвідоміші програмні продукти для реалізації нейромережових систем — BrainMaker фірми CaliforniaScientificSoftware, NeuralWorksProfessional фірми NeuralWare, ANSim фірми SAIC [3].

Адже, аналіз наукових праць дозволяє зробити висновок про наявний широкий спектр можливих застосувань нейронних мереж, а юридична діяльність — ще один напрямок їх застосування, який потребує наукового дослідження.

Основний елемент нейронної мережі — це формальний нейрон, здійснюючий операцію нелінійного перетворення суми добутоків вхідних сигналів на вагові коефіцієнти. Для навчання мережі використовуються різні алгоритми навчання та їх модифікації. Дуже важко визначити, який навчальний алгоритм буде найшвидшим

при вирішенні того чи іншого завдання. Як зазначено вище, найбільший інтерес представляє алгоритм зворотного поширення помилки, так як є ефективним засобом для навчання багат шарових нейронних мереж прямого поширення. Алгоритм мінімізує середньоквадратичну помилку нейронної мережі. Для цього з метою налаштування синоптичних зв'язків використовується метод градієнтного спуску в просторі вагових коефіцієнтів і порогів нейронної мережі. Для прискорення процедури навчання замість постійного кроку навчання варто використовувати адаптивний крок навчання, з ним мережа працює в 4 рази швидше. На кожному етапі навчання мережі він вибирається таким, щоб мінімізувати середньоквадратичну помилку мережі [4].

Розглянемо більш детально напрями та перспективи використання в LegalTech нейронних мереж.

1. Попередження конфліктів. Удосконалення інформаційної системи господарюючих суб'єктів за рахунок впровадження інтелектуальної системи підтримки прийняття рішень (ІСППР) із застосуванням нейронної мережі дозволить уникнути конфліктних ситуацій, завдяки аналітичним та обліковим можливостям, як вбудований програмний додаток, на централізованих платформах, прогнозу проблемних місць в виробничій та фінансовій діяльності. Прийняття своєчасних управлінських рішень по ліквідації негативних факторів забезпечує випуск якісної продукції виконання договірних зобов'язань і зменшує кількість конфліктів, пов'язаних з виконанням контрактів.

2. Підвищення правової грамотності населення. Створюється програмне забезпечення, що дозволяє без допомоги професійних юристів аналізувати і готувати правові документи, а також майже автоматизувати процес прийняття рішень з юридичних питань, складати договори, заповіти та інші документи. Головним чином, це стосується малого бізнесу, який не має власного юридичного відділу, і кінцевих споживачів. Здатність до навчання, яке демонструють сучасні НМ, спроможні оцінювати обставини справи, та надавати користувачу всі можливі варіанти рішення, таким чином, це дозволить збільшити рівень правової обізнаності зацікавленої частини населення. Згідно з підсумками опитування, проведеного в 2018 р. Національної юридичної службою АМУЛЕКС і Аналітичним центром НАФД, індекс правової грамотності склав 54 п.п з 100 можливих. Опитування показало, що все більша кількість людей бажає підвищити свій рівень правових знань [5]. В Україні LegalTech свій активний розвиток почав лише на початку 2016 р. Адже, дуже важливо, вивчати його можливості, доводити цю інфор-

мацію до користувачів, задля зміни кута зору українців на надання юридичних послуг, для розуміння ними, що багато юридичних питань кожен вже може вирішити онлайн, економлячи при цьому час та кошти.

3. Підвищення ефективності роботи професійних юристів. НМ, на основі даних довідкових правових інформаційних ресурсів, здатні аналізувати великі масиви інформації щодо попередньої судової практики максимально схожих за обставинами справ. Це зменшує трудомісткість роботи професійних юристів по пошуку необхідної інформації, по підготовці й оцінці правових вимог, тобто економить час, що іноді являється головною перевагою в успішному вирішенні справи. Програмні продукти та додатки на основі НМ дозволяють вивчати юридичну англійську мову, у перспективі такі юристи зможуть брати участь у міжнародних конференціях, розуміти англомовні договори і працювати з ними, особливо у сфері ІТ, що, в свою чергу, може бути підґрунтям кар'єрного зросту, отримання кращої посади, яка вимагає володіння саме професійною лексикою.

4. Пошук альтернативних засобів вирішення спорів. Використання LegalTech з вбудованою НМ робить можливим моделювання вирішення спорів на основі схожих примірних процедур, що дозволяє заздалегідь оцінити перспективи судового розгляду справи. НМ навчається на матеріалах аналогічних справ, а потім, після введення в опитувальник даних користувачем, надає альтернативні можливі варіанти вирішення спорів та пропонує послуги з представництва в суді за відсоток від суми, одержуваної при виграші справи.

5. Підвищення ефективності правосуддя. Використання НМ, як програмного додатку вбудованого в інформаційну систему, дозволяє підвищити ефективність роботи суддів, наприклад, за рахунок використання програмного забезпечення, що допомагає виділити ключові моменти і правові питання спору, а також пошуку рішень у справах, в яких висувалися подібні або ідентичні аргументи для повторного використання їх тексту. Хоча повністю «комп'ютерне» прийняття судових рішень навряд чи буде прийнято суспільством в осяжний період, цілком можливою є автоматизована підготовка їх чорнових варіантів з наданням сторонам можливості ознайомитися з ними і, можливо, відмовитися від позову, уникнувши судових витрат [5].

6. Вбудовані НМ в ІСППР як — інновації в правовому захисті бізнесу. В мінливих умовах сьогодення важливим завданням є захист бізнесу не тільки від економічних проблем, а й від фізичного впливу, наприклад, неправомірних дій зі сторони контролюючих і правоохоронних органів. Так, інноваційні зміни в інформаційній системі, тобто впровадження ІСППР на основі НМ,

підтримують керівників, які не є юридично грамотними, в прийнятті рішень щодо безпеки бізнесу, допомагають знайти юридичну інформацію з інформаційних баз для захисту себе та фірми у разі перевірки контролюючого органу, бути в курсі усіх державних реєстрів з метою попередження рейдерських захоплень, фінансових махінацій тощо. Завдяки інноваціям користувач має можливість отримати доступ до найактуальнішого законодавства, завантаживши собі невеличкий додаток на смартфон та організувавши доступ до Інтернету.

7. Роль та місце ІСППР та інноваційних програмних додатків в адвокатському захисті. Зрозуміло, що існує частина юридичного супроводження та захисту, яка не доступна роботам та програмному забезпеченню — це адвокатський захист посадових осіб та співробітників, або підприємства в цілому, в ході розслідування кримінальних проваджень правоохоронними органами. Важливим фактором захисту є швидкість реакції на негативний вплив та прибуття кваліфікованого адвоката на слідчу дію та вжиття ним необхідних заходів правового опору в рамках слідчої дії. І саме використання інтелектуальних систем підтримки прийняття рішень з вбудованими НМ мають змогу допомогти у швидкому інформуванні кваліфікованих спеціалістів у необхідності їх професійних вмінь та навичок.

Але слід враховувати і роль ботів, а саме, наприклад, OblavaBotце Telegram-бот, який допомагає здійснити швидкий та якісний пошук кримінального адвоката на слідчу дію. Система сервісу у вигляді агрегатора дає змогу підібрати адвоката з переліку адвокатів відповідно до спеціалізації та/або територіального положення [5].

8. Нейронні мережі у створенні ботів-юристів — це реальність. Яскравий приклад — бот-юрист DoNotPay. За допомогою штучного інтелекту додаток визначає випадки, коли водієві не потрібно оплачувати штраф за паркування. За перші кілька місяців роботи бот заощадив користувачам 3 млн дол. Після успішного запуску функціонал бота розширили. Він став розбиратися у понад однієї тисячі галузей права. Тепер бот може відповісти на питання, як заповнити форму для виходу в декрет або як бути, якщо орендодавець порушив договір [5].

Результати дослідження. Досліджуючи певний час МІС українських підприємств, автори прийшли до висновку, що здебільшого вони мають маркетингову інформаційну систему відкритої архітектури і підтримують стратегію поступового нарощування її функціональних можливостей. Але, на думку авторів, це може призвести до втрати конкурентних переваг, прибутку та взагалі до банкрутства підприємства. Нова економічна реальність невід'ємно пов'язана з

нестачею часу та підвищенням швидкості вироблених операцій, саме тому технології штучного інтелекту перетворюються у віртуальне середовище, в якому здійснюється не тільки процеси купівлі-продажу, а й процеси обміну знаннями, владою і капіталом, отже, з розподілу економічних ресурсів. Таким чином, маркетингова інформаційна система повинна знаходитися в постійному оновленні відповідно до розвитку сучасних ІТ-технологій, віртуального середовища та штучного інтелекту.

Спираючись на [6], автори намагаються розв'язати вказані проблеми. Цьому повинна сприяти удосконалена інформаційна система, яка зображена на рисунку 1.



Рис. 1. Удосконалення інформаційної системи фірми з надання юридичних послуг

Як видно з рисунку, для розширення можливостей системи авто-рами запропоновано удосконалити її підсистему аналізу та моделювання шляхом будови інтелектуальної системи підтримки прийняття рішень (ІСППР) з використанням НМ.

Апробація запропонованого удосконалення проводилася у декількох напрямках, але кожен з них підтверджує можливості застосування як в умовах діючих підприємств та й в умовах юридичних фірм.

По-перше, була вирішена одна із складних задач для підприємств з надання інжинірингових послуг, а саме, розрахована прогнозна вартість проекту з автоматизації, що здатна забезпечити вихід на зовнішній ринок.

По-друге, сформована опитувальна форма для обліку та оцінки кредитоспроможності клієнтів банку або іншого підприємства, яке здійснює такий аналіз та надання підтримки в прийнятті рішення щодо надання кредиту або відмові.

У першому напрямку, автори, за допомогою побудованої НМ, здійснили розрахунок прогнозної вартості за надані інженерно-консультаційні послуги (див. рис. 2). Після навчання нейронної мережі на даних за попередні роки користувач мав можливість здійснити перехід за допомогою кнопок меню на форму вхідних даних. У наступній вкладці користувач вводить нові вхідні дані та отримує прогнозне значення вартості проекту [4].

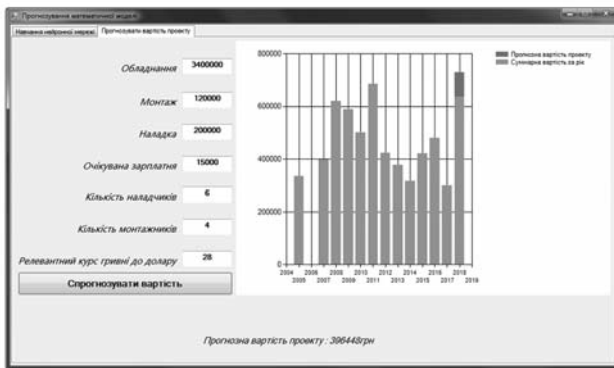


Рис. 2. Приклад визначення прогнозної вартості проекту на навченій нейронній мережі [4].

Проведена апробація показала, що ІСППР з навченою нейронною мережею, надала користувачеві вичерпну інформацію щодо майбутнього проекту. Отже, в підсумку, завдяки використанню НМ

формується договір на отримання тендеру, що запобігає виникненню непорозумінь та конфліктів між замовником та підприємством. НМ навчається на матеріалах аналогічних справ та проєктів, а потім, після введених в розроблену форму даних надає користувачу відповідний варіант рішення.

Другий напрямок апробації вдосконаленої інформаційної системи із застосуванням нейронних мереж був здійснений на прикладі заповнення опитувальної форми для прийняття кредитного висновку щодо клієнту підприємства. Після запуску програмного продукту користувачу дається можливість обрати тип алгоритму навчання та структури нейронної мережі, тобто налаштувати програмний продукт. Для зручності користувачу також демонструється форма даних та основні параметри, які характеризують клієнтів (див. рис. 3) [6].

Вік	Сума на кредит поточ рахунок	Залишок на кредит поточ рахунок	Кількість записів	Термін кредит	Ставка	Потом на поточ кредит	Ставка на поточ мови робота	Провайзер компю	Кредит рейтинг	Кредит історія	Наличність житла	Тип запису	Сума на поточ рахунок	Власник	Ціль кредит	Залишок на депозит та ошля-раром	
22	5951	10000	1	48	2	1	3	1	0	1	2	3	2	3	1	3	1
49	20960	20000	2	12	2	1	4	1	0	4	2	2	1	3	1	6	1
49	20960	20000	2	12	2	1	4	1	1	1	2	2	1	3	1	6	1
49	20960	20000	2	12	2	1	4	1	1	1	2	2	1	3	1	6	4
49	20960	20000	2	12	2	1	4	1	1	1	2	2	1	3	1	6	4
49	20960	20000	2	12	2	1	4	1	1	1	2	2	1	3	1	6	4
25	20000	0	2	12	2	1	4	1	0	4	2	2	1	3	1	6	4
25	4000	5000	2	2	12	1	3	1	0	2	2	3	1	3	1	1	4
25	4000	5000	2	2	12	1	3	1	0	2	2	3	1	3	1	1	4
25	4000	5000	2	2	12	1	3	1	0	2	2	3	1	3	1	1	4
25	4000	5000	2	2	12	1	3	1	0	2	2	3	1	3	1	1	4

Рис. 3. Структурна форма даних для нейронної мережі [6]

Після того як параметри обрані, активується кнопка вкладки «Додати дані до навчальної вибірки». Дані для навчання отримуються з інформаційної системи. Для побудови моделі використовувалась скорочена вибірка анонімізованих соціо-демографічних та агрегованих даних рахунків клієнтів підприємства. У дослідженні вводилось 50 даних клієнтів, які вже отримали, чи не отримали кредит. Отже, вибірка даних містить дані, отримані як із внутрішніх джерел, так і з зовнішніх. Крім того, більшість даних представлені у вигляді дискретних груп значень, що робить модель більш точною та дозволяє легко інтерпретувати результати і взаємозв'язки. Після натискування на кнопку додати до бази даних та кнопки «Навчити мережу», здійснюється навчання мережі. Після того, як мережа навчена, користувач отримує графік навчання НМ. Після цього, користувач переходить до вкладки «Надання кредиту так/ні». Вводяться дані в форму представлену на рис. 4 [6].

Вік (Age)	34	Кредитний рейтинг (Good, bad)	1. Надійний класик
Сума кредиту (грн) (Amount)	50000	Градієнт впливляє компанії (Company)	016
Залишок на поточному рахунку (грн) (Checkbook)	1000	Навчання життя (Housing)	2. Власник
Кількість заложених осіб (Persons)	1	Ставка (Interest)	20%
Термін кредиту (Головний)	12	Тип застави (Job)	3. Прямий спеціаліст
Стаж на роботі (Employment)	4.4 м... < 7 років	Самий стан / стать (Marital)	1. Чоловічий розлучений
Кількість поточних непогашених кредитів (своїх)	0	Інші види розстрок (Other)	2. Розстрок за товари
Кредитна історія (History)	1. Всі кредити цього	Власність (Property)	1. Нерухомість
Ціль кредитування (Purpose)	9. Бізнес	Залишок на депозиті (Savings)	2. 10000 € - < 50000

Рішення щодо надання кредиту: Так, 926976978778839

Очистити Кредитний висновок

Рис. 4. Форма для вхідних даних та для формування рішення [6]

Розроблений програмний продукт, на основі нейромережі, дає змогу підтримки в прийнятті рішення щодо кредитного висновку для клієнту підприємства [6].

Отже, в інформаційній системі циркулюють значні обсяги різнобічної інформації, але мета полягає в підтримці рішень стосовно клієнтів, надання інформації достатньої для прийняття рішень. Система забезпечує обробку інформації для подальшого навчання нейронної мережі. Водночас можна користуватися базою даних для деталізації окремих розрахунків та іншими програмними продуктами для зміни вхідних даних чи методів розв'язання задач. Схема такої системи підтримки рішень з використанням нейронної мережі представлена на рис. 5.

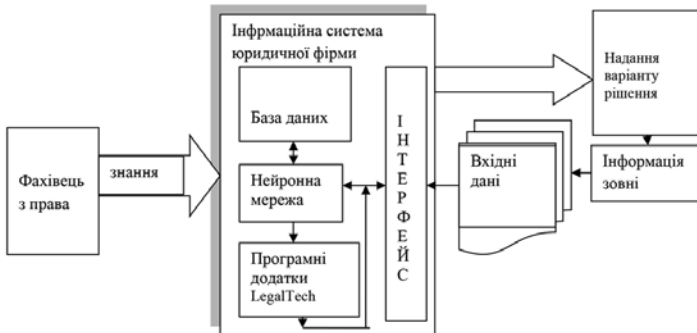


Рис.5. Системи підтримки рішень з використанням нейронної мережі

Отже, використання НС в ІСППР в цілому показали гарний результат, але головна проблема полягає в тому, що використана НС потребує досить багато часу й великої кількості даних, які служать як приклад для навчання. Такий існуючий підхід називають навчання з учителем і він має ряд обмежень: передбачає пряму демонстрацію бажаного результату; копіювання демонстрації, а не креативність; результати не покращує в порівнянні з демонстрацією. Отже, постає питання, чи зможуть НС у подальшому обійти ці обмеження? Відповідь на це запитання надають спеціалісти Google вже сьогодні. Нова робота Google пропонує архітектуру нейронних мереж, здатних імітувати вроджені інстинкти і рефлексії живих істот, з подальшим донавчанням протягом життя. На жаль, існуючі алгоритми оптимізації структури мережі, такі як NeuralArchitectureSearch (NAS), оперують цілими блоками. Після додавання або видалення яких, нейросеть доводиться навчати заново з нуля. Це ресурсномісткий процес і не в повному обсязі розв'язує проблему. Тому дослідники запропонували спрощену версію, яка отримала назву «WeightAgnosticNeuralNetworks» (WANN) [7]. Ідея полягає в тому, щоб замінити всі ваги нейромережі одною «загальною» вагою. І в процесі навчання підбирати не ваги між нейронами, як в звичайних нейромережах, а підбирати структуру самої мережі (кількість і розташування нейронів), яка з однаковими вагами показує найкращі результати. А після ще й оптимізувати її, щоб мережа добре працювала з усіма можливими значеннями цієї загальної ваги (загальним для всіх з'єднань між нейронами). В результаті це дає структуру нейронної мережі, яка не залежить від конкретних значень ваг, а працює добре з усіма. Тому що працює за рахунок загальної структури мережі.

Побічним позитивним ефектом такого підходу є значне зменшення числа нейронів в мережі (так як залишаються лише найбільш важливі сполуки), що збільшує її швидкодію. Це схоже на те, як навчаються тварини. Маючи при народженні близькі до оптимальних інстинкти, і використовуючи цю задану генами структуру мозку як початкову, в процесі свого життя тварини донавчають свій мозок під конкретні зовнішні умови. Як підсумок, запропонований дослідниками з Google спосіб пошуку початкової архітектури оптимальної нейромережі не тільки імітує навчання тварин (народження з вбудованими оптимальними інстинктами і донавчання протягом життя), але також дозволяє уникнути симуляції усього життя тварин з повноцінним навчанням всієї мережі в класичних еволюційних алгоритмах, створюючи відразу прості і швидкі мережі. Які досить лише злегка довчити, щоб отримати повністю оптимальну нейромережу [7].

Висновки. Отже, змінюється уявлення щодо бізнес-середовища підприємства. На перший план виходять такі аспекти як довіра споживачів, імідж, цілісність сприйняття корпоративної культури. Стратегічне планування стає, за таких умов, замкнутим циклом, безперервним, завдяки зворотному зв'язку з ринком, а саме з клієнтами-споживачами юридичних послуг. Прийняття рішень ґрунтується на всебічному аналізі великих масивів даних за допомогою моделювання, впровадження величезної кількості прогнозних та аналітичних інструментів, що дозволяють фахівцям з правабути озброєними в умовах невизначеності, але й вимагають від них здатності до безперервного навчання, освоєнні новаторських бізнес-технологій.

Підсумовуючи, важливо розуміти, що впровадження ІСППР та новітніх ІТ-технологій в кожному окремому підприємстві унікальна, тут не має шаблону дій, універсального сценарію. Переможцями у конкурентній боротьбі будуть ті фірми, які здатні докорінно змінювати внутрішні процеси, безперервно взаємодіють з клієнтом, на всіх рівнях і етапах роботи підтримують контакти з ним, створюють нові можливості з кваліфікованим персоналом і новими бізнес-процесами, діють швидко, щоб отримати перемогу у конкурентній боротьбі на ринку юридичних послуг. LegalTech, нейронні мережі, інші програмні додатки дають новітні можливості, використовуються безліччю способів, тим самим створюючи потенціал для нової цінності юридичної послуги.

Список використаних джерел

1 Вступ до маркетингу: концепт лекцій / Авт. Л.С. Шевченко, О. А. Грищенко та ін.; за ред. Л.С. Шевченко. – Харків: Нац. юрид. акад. України, 2008. – 71 с. URL: <https://ukr-pravo.at.ua/index/0-697> (дата звернення 28.11.2020).

2 Управління інноваціями підприємства у контексті дігіталізації/ Петренко В.О., Савчук Л.М., Бушуєв К.М., Фонарьова Т.А. // XVII Міжнародної науково-практичної конференції «Управління проектами в умовах дігіталізації суспільства» 15–16 травня 2020 р. Київ: КНУБА, 2020.

3. Modern aspects of investment and approaches to its assessment / V. Petrenko, T. Fonarova, K. Bushuiev // Intelligent computer-integrated information technology in project and program management [Text]: Collective monograph edited by I. Linde, I. Chumachenko, V. Timofeyev. Riga: ISMA, 2020. 324 p. P. 225-240.

4. Застосування нейронних мереж в системах підтримки та прийняття рішень маркетингової інформаційної системи підприємства /

В.О. Петренко, К.М. Бушуєв, Л.М. Савчук, Т.А. Фонарьова // Управління проектами та розвиток виробництва: Зб. наук.пр. – К: вид-во СНУ ім. В. Даля, 2018. – №3(67). – С. 43-52.

5. Слепченко К. LEGALTECH В УКРАЇНІ / К. Слепченко // ФББ-201, КНЕУ, 2019. URL: <https://www.businesslaw.org.ua/legal-tech-in-ukraine/> (дата звернення 28.11.2020).

6. Modern aspects of construction of information system with the use artificial intellectual on the basis of neural networks / V.O. Petrenko, T.A. Fonarova, K.M. Bushuiev // Information system and innovative technologies in project and program management [Text]: Collective monograph edited by I. Linde, I. Chumachenko, V. Timofeyev. – Riga: ISMA, 2019. – P. 227-237.

7. Технології штучного інтелекту на прикладі застосування нейронних мереж в менеджменті підприємства / В.О. Петренко, Л.М. Савчук, Т.А. Фонарьова, К.М. Бушуєв // Матеріали XVIII Міжнародної науково-практичної конференції, Київ, 19-20 вересня 2019 р. [Електронний ресурс] «Побудова інформаційного суспільства: ресурси і технології». - МОН України, УкрІНТЕІ [та ін.].

*Троцька В. М.,
завідувачка сектору суміжних прав
відділу авторського права і суміжних прав
НДІ інтелектуальної власності НАПрН України,*

ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ТЕКСТУ ТА ДАНИХ В УМОВАХ ФОРМУВАННЯ ЄДИНОГО ЦИФРОВОГО РИНКУ: ПРАВОВІ АСПЕКТИ

З розвитком цифрового середовища, накопиченням значного обсягу знань та інформації, все частіше даністають комерційним ресурсом. Говорять: «дані — це нова нафта, що породжує капітали» [1]. Отримання результатів дослідження на основі аналізу даних дає змогу мати цінні знання та інформацію, використання яких сприяє розвитку цифрової економіки в світі, а для бізнесу — бути конкурентоздатним за рахунок створення та впровадження інновацій. Для здійснення досліджень неприбутковими організаціями необхідно, щоб тексти та дані були відкритими та доступними. В інакшому випадку існуватиме інформаційний вакуум, що негативно позначатиметься на проведенні досліджень. Тому, в умовах форму-

вання єдиного цифрового ринку існує потреба в усуненні бар'єрів на шляху відкритості та доступності до текстів і даних. Одним з бар'єрів вважають авторські права. Відповідно до законодавства про авторське право використання таких об'єктів як твори та бази даних допускається з дозволу правовласників та виплатою їм винагороди, крім винятків, що передбачають обмеження майнових прав правовласників, спрямовані на забезпечення балансу публічних і приватних інтересів у суспільстві (далі — винятки та обмеження). За наявності відповідних положень у законодавстві допускається вільне використання об'єктів авторського права. Норми про винятки та обмеження з метою інтелектуального аналізу тексту та даних передбачені в законах окремих іноземних країн та в регіональному законодавстві, а саме: Директиві Європейського Парламенту та Ради про авторське право і суміжні права в єдиному цифровому ринку, прийнятій у 2019 р.¹⁷ (далі — Директива ЄС) [2]. З огляду на підвищення уваги до питань секторальної інтеграції України до єдиного цифрового ринку ЄС, а також враховуючи законопроектні роботи у сфері авторського права і суміжних прав, що тривають у нашій державі, виникає потреба в детальному дослідженні винятків та обмежень з метою інтелектуального аналізу тексту та даних, їх осмисленні щодо доцільності врахування відповідних норм у національному законодавстві.

Правові аспекти інтелектуального аналізу тексту та даних відповідно до європейського законодавства розглядалися в наукових роботах таких авторів як: Christian Geib, Eleonora Rosati, Stephen Khan, Maria Daphne Papadopoulou, Margieta Roukana, Michael W. Carroll, Severine Dusollier, Teresa Nobre, Joao Pedro Quintais, Г. О. Андрощук, Ю. М. Капіца, Д. А. Мотовілова та ін. Наукові дослідження переважно стосувалися загального аналізу норм Директиви ЄС або відповідних норм законів про авторське право іноземних країн. Детального дослідження норм Директиви ЄС в частині винятків та обмежень з метою інтелектуального аналізу тексту та даних та водночас аналізу нових законопроектних ініціатив, запропонованих в Україні, на дату написання цієї статті не здійснювалося. Тому існує потреба заповнити цю прогалину.

Поняття «цифрова економіка» тісно пов'язане з використанням даних. У класичному розумінні «цифрова економіка» означає діяльність, в якій основними засобами (факторами) виробництва є цифрові (електронні, віртуальні) дані як числові, так і текстові [3].

¹⁷ Директива ЄС набрала чинності 7 червня 2019 р. Положення цієї Директиви мають бути імplementовані в національне законодавство Держав-учасниць ЄС до 7 червня 2021 р.

Нові технології, як зазначено в п. 8 преамбули Директиви ЄС, дозволяють автоматизувати обчислювальний аналіз та обробляти значні обсяги інформації в цифровій формі, з метою отримання нових знань і відкриттів. Однак, на практиці організації та установи зіштовхуються з правовою невизначенністю. Зокрема, пошук тексту та даних часто включає дії, пов'язані з відтворенням творів, баз даних, охоронюваних авторським правом, чи з відтворенням та вилученням вмісту неоригінальних баз даних, що охороняються в країнах ЄС правом особливого роду «*sui generis*» (далі — право *sui generis*). Це означає, що за відсутності винятків у законодавстві, для використання тексту та даних, зокрема й у процесі науково-дослідної роботи, необхідно отримувати дозвіл у правовласників, а також виплачувати їм винагороду. Так, доступ до нових наукових статей і звітів про результати досліджень у багатьох іноземних виданнях є платним, або можливий на основі відкритого доступу. Проте, навіть в останньому випадку умови ліцензії можуть виключати право на вільне використання тексту та даних у відповідних цілях.

Дії, пов'язані з аналізом текстів, часто передбачають отримання інформації з наукових статей. Існує також термін «інтелектуальний аналіз тексту наукових статей». Під цим терміном розуміються процеси, за допомогою яких інформація відбирається, виокремлюється та інтерпретується з сотень статей та синтезується в причинно-наслідковій моделі [6]. Технології аналізу дозволяють відкрити нові напрямки досліджень та виявити нові кореляції та закономірності з отриманої інформації, які в іншому випадку не можливо було б виявити. Для проведення належного дослідження потрібен доступ до значного масиву інформації, зокрема й до наукових статей, в яких міститься така інформація. Цифрова обробка інформації, відображеної в тексті, дозволяє економити час та уникати зайвих витрат при дослідженні, що є особливо цінним для неприбуткових науково-дослідних організацій в сучасних умовах масштабного поширення цифрового контенту.

До «науково-дослідних організацій» належать університети, їх бібліотеки, науково-дослідні інститути або інші неприбуткові установи, основна мета яких полягає в проведенні наукових досліджень або освітньої діяльності, пов'язаної зі здійсненням наукових досліджень (далі — організації) (ст. 2 (1) Директиви ЄС). Важливою умовою поширення винятків та обмежень на дії, пов'язані з аналізом текстів і даних такими організаціями, є їх неприбутковість. Комерційні організації чи підприємства для цілей цієї Директиви ЄС, не розглядаються.

Під «аналізом тексту та даних» («Textanddatamining») розуміється будь-який автоматизований аналітичний метод, спрямований на аналіз тексту та даних в цифровій формі з метою отримання інформації, яка включає, але не обмежується моделями, тенденціями та кореляціями (ст. 2 (2) Директиви ЄС).

Відразу, варто звернути увагу, що винятки та обмеження стосуються аналізу текстів і даних. При цьому, права на тексти можуть охоронятися авторським правом, або ні. Як відомо, законодавство про авторське право не охороняє інформацію як таку, навіть якщо вона виражена, описана, пояснена, проілюстрована в творі. Охорона поширюється лише на форму вираження твору. Тому використання при аналізі вмісту тексту як звичайної інформації, є вільним.

Що стосується охорони прав на бази даних, то в порівнянні з текстами, існують наступні особливості. Згідно з Директивою Європейського Парламенту та Ради № 96/9/ЄС від 11 березня 1996 р. про правовий захист баз даних (далі — Директива про бази даних) [4], права на бази даних охороняються авторським правом, а права на неоригінальні бази даних — правом *sui generis*. Відтак, використання як оригінальних, так й неоригінальних баз даних потребує отримання дозволу та виплати винагороди правовласникам, крім винятків, визначених у законодавстві. Розрізняють бази даних високого (BigData) й низького рівнів. Зокрема, вчені CaspersM., GuibaultL. розмежовують дані наступним чином. Дані високого рівня включають вміст, такий як: статті в газетах чи журналах, книги, музика, фотографії, кінематографічні твори. До даних низького рівня належать «необроблені» дані, такі як генетична інформація, дані вимірювань у будь-якій галузі науки, імена та адреси, GPS координати, телефонні номери або фінансові дані [5]. Як бачимо, вміст баз даних може включати об'єкти авторського права, а права на самі бази даних можуть охоронятися авторським правом чи правом *sui generis*. Це пояснює той факт, що за відсутності у законодавстві винятків та обмежень, використання будь-яких баз даних, зокрема й з дослідницькою метою, не може бути вільним. Усвідомлюючи це, у законах окремих країн про авторське право (Японії, Великобританії, Німеччини, Франції тощо) введені норми про винятки та обмеження щодо інтелектуального аналізу тексту та даних в дослідницьких цілях.

Винятки та обмеження, передбачені в міжнародному та національному законодавствах про авторське право, стосуються використання творів певними способами. У статтях 3 та 4 Директиви ЄС уточнені способи використання, а саме: відтворення тексту та

даних, вилучення вмісту баз даних. По тексту Директиви ЄС застосовується термін «використання технологій аналізу тексту та даних»¹⁸, сформульованя якого є нечітким та неоднозначним. Фактично визначено про допустимість вільного використання «технологій аналізу», під якими може розумітися комп'ютерне забезпечення дослідження, а не використання тексту та даних з метою їх аналізу.

Аналіз тексту та даних з метою проведення наукового дослідження в сучасних умовах розвитку цифрових технологій, можливий за таких умов. По-перше, потрібно мати доступ до тексту та даних, представлених у цифровій формі. По-друге, допускається їх вільне використання організаціями з метою проведення наукового дослідження.

Щодо першої умови. У Директиві ЄС зазначено, що винятки та обмеження поширюються лише на випадки, коли організація отримала «законний доступ» до тексту та даних. Однак, з появою цифрових технологій доступ до творів ускладнився за рахунок застосування прав власниками технічних засобів захисту. Доступ вважається законним, якщо прав власники не залишили за собою виключного права надавати дозвіл на відтворення, вилучення вмісту даних з метою аналізу, а також надання доступу до тексту та даних. У випадках, коли твір є загальнодоступним у мережі Інтернет, потрібно враховувати метадані, умови використання контенту веб-сайту та послуг, що надаються. Організації можуть отримати законний доступ до тексту та даних, зокрема за допомогою перевірки IP-адреси або аутентифікації адреси чи особи. Цікаво, що відповідно до п. 18 преамбули, ст. 4 (3) Директиви ЄС аналіз тексту та даних може бути здійснений на підставі договорів чи односторонніх заяв (декларацій). Тобто, не зважаючи на те, що в Директиві ЄС введені винятки та обмеження, прав власники все ж вправі залишати за собою виключне право надавати дозвіл на використання твору, чи забороняти подібне використання. За наявності вказаних норм у законодавстві, у прав власників є правові підстави для того, щоб визначати умови поширення твору на основі договірних домовленостей чи декларацій, а також застосовувати технічні засоби захисту. Практично прав власник матиме право обмежувати доступ до тексту та даних, встановлювати умови, зокрема й щодо виплати винагороди, навіть у тих випадках, коли дозволяються вільне використання згідно з встановленими законом винятками та обмеженнями. За таких умов, виникає питання ефективності реалізації прийнятих

¹⁸ Англійською мовою «usesofttextanddataminingtechnologies» (п. 5 преамбули Директиви ЄС).

норм Директиви ЄС, застосування яких не надає беззастережне право на бездогівірне, безкоштовне використання тексту та даних з метою їх аналізу організаціями.

Щодо другої умови. Аналіз тексту та даних вимагає їх відтворення, вилучення вмісту баз даних та, в разі необхідності, збереження. Якщо вказане використання здійснюється організацією з метою проведення наукового дослідження, то для аналізу залежно від задач, які ставляться, доцільно зібрати, ознайомитися зі структурованими чи неструктурованими текстом і даними, отримати (виділити) необхідну інформацію, узагальнити, класифікувати, кластеризувати та застосувати інші методи інтелектуального аналізу тексту і даних для отримання результатів. Дії можуть підпадати під винятки та обмеження, а саме: вільне тимчасове відтворення творів, визначене в ст. 5 (1) Директиви 2001/29/ЄС Європейського парламенту та Ради від 22 травня 2001 р. про гармонізацію певних аспектів авторського права та суміжних прав у інформаційному суспільстві [6]¹⁹. Проте, відтворення може бути не лише тимчасовим. Так, відтворені тексти та дані з метою аналізу можуть зберігатися стільки, скільки це потрібно для цілей дослідження. На відміну від відтворення текстів і даних з метою аналізу, тимчасове відтворення не може передбачати збереження твору більш ніж необхідно в рамках здійснюваного технологічного процесу. Організації можуть, наприклад, для подальшої перевірки результатів наукових досліджень, зберігати копії текстів і даних для цілей аналізу, за умови, що доступ до них захищено (п. 15 преамбули Директиви ЄС).

Формулювання об'єкту правовідносин стосується саме «інтелектуального» аналізу тексту та даних. Вважається, що аналіз передбачає інтелектуальний підхід, а тому виключається поширення норм про винятки та обмеження на здійснення аналізу за допомогою штучного інтелекту. У зв'язку з масштабною автоматизацією всіх процесів у суспільстві, збір та обробка тексту та даних за допомогою комп'ютерних програм стає все більш поширеним явищем.

Вільне використання текстів і даних допускається без виплати винагороди їх правовласникам. Обґрунтовується це тим, що при вільному використанні текстів і даних організаціями, які здійснюють наукові дослідження, будь-який потенційний збиток, нанесе-

¹⁹ Ст. 5 (1) Директиви 2001/29/ЄС Європейського парламенту та Ради від 22 травня 2001 р. про гармонізацію певних аспектів авторського права та суміжних прав у інформаційному суспільстві «1. Тимчасові дії з відтворення, передбачені статтею 2, що мають короткотривалий або епізодичний характер і є невід'ємною і важливою частиною технологічного процесу, єдиною метою яких є забезпечення: (а) передачі в мережі між третіми особами із залученням посередника, або (б) правомірному використанні твору або іншого об'єкта, і які не мають самостійного економічного значення, повинні бути виключені з права на відтворення, передбаченого статтею 2».

ний правовласникам із врахуванням прийнятого в законодавстві винятку та обмеження, є мінімальним (п. 17 преамбули Директиви ЄС). Таким чином, не має потреби у виплаті компенсації (винагороди) правовласникам за використання їх об'єктів авторського права. До того ж при науковому дослідженні існує потреба в обробці великого масиву інформації, що міститься в текстах і даних, тому виплата компенсації (винагороди) може бути не виправдано витратною для неприбуткових організацій.

При реалізації положень Директиви ЄС можуть виникати практичні питання. Зокрема, чи вважатиметься відтворення текстів і даних з метою аналізу, їх цитуванням. Яким чином мають дотримуватися особисті немайнові права авторів щодо зазначення їх імені та джерела запозичення, з огляду на великі масиви обробки текстів і даних, в яких міститься інформація²⁰. Залишається також відкритим питання про права на похідні твори, створені з використанням текстів і даних. Наприклад, коли здійснюється творчий підбір та упорядкування даних, що призводить до створення бази даних, права на яку охороняються авторським правом. Або в разі творчого перекладу тексту, взятого з іноземних джерел, чи виникатимуть виключні права у перекладача надавати дозвіл на відтворення перекладу тексту та отримання винагороди. Не менш дискусійним залишається питання, коли тексти, бази даних створюються штучним інтелектом за допомогою відповідних комп'ютерних програм. Виникає питання, кому мають належати майнові права на такі об'єкти, та відповідно право розпоряджатися майновими правами.

Що ж до України, то в нашій державі процес приведення національного законодавства до законодавства ЄС наразі триває. Міністерством розвитку економіки, торгівлі та сільського господарства України розроблено проект Закону України «Про авторське право і суміжні права», в новій редакції (далі — Проект Закону) [8]. На етапі розробки включені положення про вільне використання творів з метою інтелектуального аналізу тексту та даних. Проте, в подальшому такі положення були виключені, зважаючи на рекомендації міжнародних експертів, озвучені на Семінарі з розвитку законодавства у сфері авторського права і суміжних прав, організованому CLDP спільно з вказаним Міністерством (м. Київ, 12–13 вересня 2019 р.). Зазначено, що регулювання відносин у За-

²⁰ Наприклад, застосування корпусів мови таких як Міжнародний корпус англійської мови і Британський національний корпус BritishNationalCorpus, включають колекцію зі 100 млн слів розмовного та письмового тексту. Корпус української мови — майже 3 млрд слів (Україна, Польща) [7]. Відповідні організації, що спеціалізуються на дослідженні мовознавства за допомогою інформаційно-пошукових систем можуть здійснювати пошук текстових прикладів у корпусі.

коні України «Про авторське право і суміжні права», відображених у положеннях Директиви ЄС, повинне бути відтерміноване доки всі держави-учасниці ЄС не транспонують Директиву ЄС і не вирішать можливі проблеми тлумачення та застосування її положень. Тому, запропоновані положення відкладені для розгляду на майбутнє.

Варто звернути увагу, що в Проекті Закону враховані норми Угоди про асоціацію між Україною та ЄС, Директиви про бази даних. Передбачена правова охорона неоригінальних баз даних правом *sui generis*²¹. Виробнику такої бази даних належатиме виключне право, якщо ним було зроблено якісно та (або) кількісно значний внесок в отримання, перевірку чи подання вмісту бази даних, щоб запобігти вилученню та (або) повторному використанню всього вмісту бази даних чи значної її частини у якісному чи кількісному вимірі. Не вдаючись до подробиць аналізу складності наведених формулювань та їх застосування на практиці, в разі прийняття закону, виробники неоригінальних баз даних отримають виключне право дозволяти відтворення вмісту бази даних або частин в будь-якій формі²². Винятки складатимуть: вільне вилучення для особистих цілей, проте лише вмісту неелектронної бази даних; відтворення творів для ілюстрації в освітній або науковій діяльності, за умови зазначення джерела і якщо це виправдано некомерційною метою цих дій; для громадської безпеки чи для цілей судового, адміністративного або кримінального провадження. Якщо на сьогодні будь-хто може вільно відтворювати неоригінальні бази даних, то з прийняттям вказаних норм, дослідники матимуть право вільно відтворювати бази даних, які не є електронними, а науково-дослідні організації — лише з метою ілюстрації. Дозволені дії щодо вільного відтворення баз даних з метою аналізу при здійсненні наукового дослідження некомерційними організаціями, не передбачені. Відтак, виникатимуть правові бар'єри в доступі до інформації для здійснення наукових досліджень, що може негативно по-

²¹ Права на неоригінальні бази даних передбачені також в Угоді про асоціацію між Україною та ЄС.

²² Як засвідчили неодноразові дослідження, проведені в ЄС, застосування положень Директиви про бази даних в частині права *sui generis* ставиться дослідниками під сумнів. Як засвідчила практика реалізації положень цієї Директиви, ефективні результати запровадження норм відсутні. Підтвердженням цього є звіт: Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases <http://www.technopolis-group.com/wp-content/uploads/2018/07/Study-in-Support-of-the-Evaluation-of-the-Database-Directive-.pdf>; Synopsis report on the responses to the public consultation activities on the evaluation of Directive 96/9/EC on the legal protection of databases <https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-evaluation-directive-969ec-legal-protection-databases>.

значитися на розвитку науки та впровадженні інновацій. Як зазначає Ю. М. Капіца «нові рішення, що пропонуються Директивою ЄС, які передбачається запровадити в Україні, доцільно оцінювати, виходячи з загальних прогнозів розвитку суспільства та реалізації найбільш оптимальної моделі авторського права, що забезпечує стимулювання створення творів та забезпечує баланс інтересів творців, для яких творча діяльність є професійною, медіа, видавничого бізнесу та спільноти» [9, 76]. Положення про охорону прав на неоригінальні бази даних розроблені з урахуванням європейського законодавства. Проте, не зважено на те, що в ЄС запропоновані норми про винятки та обмеження щодо інтелектуального аналізу тексту та даних, вже на основі напрацьованої практики та виявлення прогалин реалізації норм Директиви про бази даних, в якій не передбачені відповідні винятки та обмеження.

З огляду на наведене, при доопрацюванні Проекту Закону можливо залишити запропоновані норми про правову охорону неоригінальних баз даних правом *sui generis* та доповнити положеннями про вільне використання текстів і даних з метою їх інтелектуального аналізу. Проте, в цьому випадку, не будуть враховані рекомендації міжнародних експертів щодо передчасності введення відповідних норм. За таких обставин, вважається за доцільне відтермінувати як введення норм про вказане вільне використання тексту і даних, так й положень про правову охорону неоригінальних баз даних правом *sui generis*, до напрацювання відповідної європейської практики, в тому числі й судової.

Зважаючи на наведене, можливо дійти таких висновків.

Європейські країни шляхом прийняття відповідних законодавчих норм прагнуть забезпечити ефективний розвиток різних секторів економіки, які використовують цифрові технології, сприяють діяльності дослідницької галузі, яка вносить вклад у розвиток інноваційних, креативних та цифрових індустрій. Підтвердженням цього є прийняття Директиви Європейського Парламенту та Ради про авторське право і суміжні права в єдиному цифровому ринку, в якій визначені винятки та обмеження з метою інтелектуального аналізу тексту та даних. Що ж до України, то при внесенні відповідних змін до національного законодавства про авторське право і суміжні права доцільно проводити подальше дослідження не лише європейського законодавства, а й практики його застосування, особливо в частині реалізації норм про охорону прав на неоригінальні бази даних, а також положень про винятки та обмеження, згідно з якими допускається вільне використання таких баз даних.

Список використаних джерел:

1. Блонов Р. Большие данные — это новая нефть URL:<https://vc.ru/flood/51521-bolshie-dannye-eto-novaya-neft>.
2. 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 (Text with EEA relevance.). OJ L 130. 17.5.2019. P. 92-125.
3. Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації» від 17 січня 2018 р. № 67-п URL:<https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text>.
4. Директива Європейського Парламенту та Ради № 96/9/ЄС від 11 березня 1996 року про правовий захист баз даних URL:https://zakon.rada.gov.ua/laws/show/994_241#Text.
5. Caspers, M.; Guibault, L. FutureTDM. Deliverable 3.3 Baseline report of policies and barriers of TDM in Europe URL:<https://www.cric.or.jp/english/clj/cl2.html>.
6. Michael W. Carroll. Copyright and the Progress of Science: Why Text and Data Mining is Lawful URL:https://lawreview.law.ucdavis.edu/issues/53/2/articles/files/53-2_Carroll.pdf.
7. Директива 2001/29/ЄС Європейського парламенту та Ради від 22 травня 2001 року про гармонізацію певних аспектів авторського права та суміжних прав у інформаційному суспільстві (Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society) OJ L 167, 22.6.2001, p. 10–19.
8. Корпусна лінгвістика URL:https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D1%80%D0%BF%D1%83%D1%81%D0%BD%D0%B0_%D0%BB%D1%96%D0%BD%D0%B3%D0%B2%D1%96%D1%81%D1%82%D0%B8%D0%BA%D0%B0.
10. Проект Закону України «Про авторське право і суміжні права» URL:<https://www.me.gov.ua/Documents/Detail?title=ProktZakonuUkrainiproAvtorskePravoISumizhniPrava>.
9. Капіца Ю. М. Директива 2019/790/ЄС про авторське право в єдиному цифровому ринку та питання адаптації законодавства України // ІНФОРМАЦІЯ І ПРАВО. № 3(30)/2019 URL:<http://ippi>.

Наукове видання

**ПИТАННЯ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ**

Випуск вісімнадцятий

Комп'ютерне макетування — *Л. Цикаленко*
Художнє оформлення — *І. Петренко*

Адреса редакції:
вул. Казимира Малевича 11, Київ, 03150
Тел.: 228-21-36; тел./факс: 200-08-76
www.ndiiv.org.ua
e-mail: letter@i.kiev.ua

Формат 60x84/16. Папір офсетний.
Гарнітура SchoolBookСТТ.
Ум.-друк. арк.9,7. Наклад 300 прим.
Видавець: ТОВ «НВП «Інтерсервіс»
м. Київ, вул. Бориспільська, 9.
Свідоцтво: серія ДК № 3534 від 24.07.2009 р.
Виготовлювач: ТОВ «НВП «Інтерсервіс»
м. Київ, вул. Бориспільська, 9.
Свідоцтво: серія ДК № 3534 від 24.07.2009 р.