ISSN 2308-0361

УДК 330.341.1

ШТУЧНИЙ ІНТЕЛЕКТ: ЕКОНОМІКА, ІНТЕЛЕКТУАЛЬНА ВЛАСНІСТЬ, ЗАГРОЗИ*

Геннадій Андрощук,
головний науковий співробітник НДІ інтелектуальної власності НАПрН України, кандидат економічних наук, доцент, судовий експерт
ID ORCID: 0000-0003-0781-9740

У роботі подано економіко-правовий аналіз стану і тенденцій розвитку штучного інтелекту (ШІ), визначено його вплив на економіку, роль інтелектуальної власності (ІВ), подано оцінку ризиків, загроз і небезпек кримінального застосування ШІ, вироблено механізми відповідної протидії. Розглянуто розвиток технологій ШІ як невід'ємної частини «Індустрія 4.0», досліджено основні положення «Білої книги зі штучного інтелекту» ЄС. У правовому регулюванні ШІ розглядається як новий виклик для економіки і правової системи, нове явище, що має мультиплікаційний ефект, правовий феномен у структурі правовідносин, новий об'єкт для правового регулювання. Упровадження ШІ у сферу ІВ формує нові правові та економічні проблеми. Проведено аналіз розглянутих судами справ, по'язаних з проблемою правосуб'єктності ШІ, вивчено законотворчу діяльність з цього питання. Вказано на можливості та небезпеки кримінального застосування ШІ, які проранжовано в порядку рівня їх небезпеки. Окреслено перспективи розвитку ШІ в Україні, проаналізовано Концепцію розвитку штучного інтелекту в Україні. Зроблено висновок про те, що ШІ має стати одним із ключових драйверів цифрової трансформації та загального зростання економіки України.

Ключові слова: штучний інтелект, економічний вплив, інтелектуальна власність, регулювання, кібербезпека, ризики, загрози, національна безпека

Кримінальний потенціал ШІ. Штучний інтелект може бути причетний до злочинів у різний спосіб. Цілком очевидно, що ШІ можна використовувати в якості інструменту для вчинення злочинів з огляду на його можливості полегшення дій проти реальних цілей: прогнозування поведінки людей або установ з метою виявлення і використання вразливостей; створення підробленого контенту для використання в цілях шантажу або заплямування репутації; здійснення дій, до яких злочинці-люди не можуть або не хочуть вдаватися самі через високий рівень небезпеки, фізичні параметри, швидкість реакції тощо. Хоча методи є новими, самі злочини можуть бути традиційного типу — злодійство, вимагання, залякування, терор.

У якості альтернативи системи ШІ можуть самі стати метою злочинної діяльності: обхід систем захисту, що перешкоджають злочину; ухилення від розкриття або переслідування за вже скоєні злочини; приведення до відмови довірених або критичних систем або їх нестійкої поведінки з метою завдаван-

* Продовження. Початок в попередньому номері.

ня збитку або підриву довіри громадськості. ШІ може також просто надати контекст для злочину. Шахрайські дії можуть залежати від того, що жертва вважає, що деякі функції ШІ можливі, навіть якщо це не так, або можливо, але практично не використовується.

Звичайно, ці категорії не виключають одна одну. Для атаки на систему ШІ може знадобитися спрацьовування системи ШІ. Шахрайське моделювання неіснуючих можливостей ШІ може бути виконано з використанням інших методів ШІ.

Злочини дуже різноманітні. Вони можуть бути націлені на приватних осіб або установи, підприємства або клієнтів, власність, уряд, соціальну структуру, суспільний дискурс. Можуть бути мотивовані фінансовою вигодою, набуттям влади або зміною статусу щодо інших. Вони можуть створити або зруйнувати репутацію або відносини, змінити політику або спричинити розлад. Такі ефекти можуть бути самоціллю або сходинками до якоїсь подальшої мети. Вони можуть бути здійснені для пом'якшення покарання або спроби уникнути покарання за інші злочини. Можуть бути спонукувані бажанням помсти, сексуального задоволення або досягненням релігійних чи політичних цілей. Вони можуть висловлювати не що інше, як нігілістичне спонукання до руйнування, вандалізму або насильства заради самих себе.

Ступінь, у якому ця різноманітність злочинних дій може бути збільшена за рахунок використання ШІ, значною мірою залежить від того, наскільки вони вбудовані в обчислювальне середовище: робототехніка стрімко розвивається, однак ШІ буде ефективнішим для участі в банківському шахрайстві, ніж у банальній бійці. Сучасне суспільство залежить від складних обчислювальних мереж, причому не тільки у сфері фінансів і комерції, а й політики, новин, роботи і соціальних відносин. Нині люди проводять значну частину свого життя в Інтернеті, отримують більшу частину інформації звідти, і їхні дії в Інтернеті можуть створювати та руйнувати їхню ж репутацію. Ця тенденція, імовірно, збережеться в найближчому майбутньому. Таке онлайн-середовище, у якому дані є власністю, а інформація - сила, ідеально підходить для використання у злочинній діяльності з допомогою ШІ, яка може мати серйозні наслідки в реальному світі. Більше того, на відміну від багатьох традиційних злочинів, злочини в цифровій сфері часто дуже високо тиражовані: одного разу розроблені методи можуть бути поширені, повторені та навіть продані, що створює потенціал для маркетингу кримінальних методів або надання «злочину як послуги». Це може призвести до зниження технологічних бар'єрів, оскільки злочинці зможуть передати на аутсорсинг більш складні аспекти своїх злочинів з використанням ШІ.

ШІ — одна з найбільших потенційних загроз у найближчому майбутньому. Попри величезні перспективи, що відкриваються з використанням ШІ, багато експертів звертає увагу громадськості на ризики, пов'язані з його розвитком. Так, понад 8 тис. відомих учених, розробників і промисловців, серед них астрофізик Стівен Хокінг і засновник компанії Tesla і SpaceX Ілон Маск, діяльність яких так чи інакше пов'язана з розробкою або використанням ШІ, підписали відкритий лист із закликом приділяти більш пильну увагу питанням безпеки та суспільної корисності робіт у сфері ШІ [16]. Один із розробників Skype Яан Таллінн визначив, що є трьома найбільшими загрозами існуванню людства в цьому столітті. За його словами, це штучний інтелект, синтетична біологія і так звані невідомі змінні, при цьому «зміна клімату не буде являти собою серйозну небезпеку». Синтетична біологія — це проектування і створення нових біологічних частин, пристроїв і систем, у той час як невідомі змінні — це «речі, про які ми, можливо, в принципі не можемо зараз знати»,

вважає Таллінн. Естонський програміст, який допомагав створити платформу для обміну файлами Kazaa в 90-х і службу відеодзвінків Skype у 00-х, останніми роками все більше стурбований саме ШІ. «*Зміна клімату не стане ризиком для існування, якщо не буде неконтрольованого сценарію*», — зазначив він через Skype. Із трьох загроз, які найбільше турбують Таллінна, є ШІ. Науковець витрачає мільйони доларів, щоб спробувати гарантувати безпечний розвиток технології. Це включає в себе ранні інвестиції в лабораторії ШІ, такі як Deep Mind (частково для того, щоб він міг стежити за тим, що вони роблять) і фінансування досліджень безпеки ШІ в таких університетах як Оксфорд і Кембридж. Посилаючись на книгу оксфордського професора Тобі Орда, Таллінн зауважив, що ймовірність того, що люди не виживуть у цьому столітті, становить один із шести. Однією з найбільших потенційних загроз у найближчому майбутньому є саме ШІ, а ймовірність того, що зміна клімату призведе до вимирання людства, становить менше 1 %. Коли справа стосується ШІ, ніхто не знає, наскільки розумними стануть машини, і спроби вгадати, наскільки просунутим буде ШІ у наступні 10, 20 або 100 років, є марними. Такі спроби передбачення ускладнюються тим, що системи ШІ починають створювати інші системи ШІ без участі людини. Наскільки потужно і як саме розвиток ШІ впливатиме на розробку ШІ? Якщо виявиться, що ШІ не дуже успішний у створенні інших ШІ, тоді, на думку Таллінна, нам не варто надто непокоїтися, оскільки буде час для «розосередження і розгортання» можливостей. Однак, якщо ШІ уміє створювати інші ШІ, то «дуже виправдано турбуватися ... про те, що станеться далі», — наголосив науковець. Він пояснив, що є два основні сценарії, які розглядають фахівці з безпеки ШІ. Перший — це нещасний випадок у лабораторії, коли дослідницька група залишає систему ШІ, щоб тренуватися на деяких комп'ютерних серверах увечері, а «вранці світу більше немає». У другому випадку дослідницька група створює прототипну технологію, яка потім приймається і застосовується в різних галузях, «де вони в кінцевому підсумку призводять до небажаних наслідків». Дослідник зазначив, що він більше зосереджений на першому, оскільки менше людей думають про такий сценарій. За його словами, деякі компанії ставляться до безпеки ШІ більш серйозно, ніж інші. Deep Mind, наприклад, підтримує регулярні контакти з дослідниками безпеки ШІ в таких місцях, як Інститут майбутнього людства в Оксфорді. У ньому також працюють десятки людей, зосереджених на безпеці ШІ. На іншому кінці шкали такі корпоративні центри як Google Brain і Facebook AI Research, що менше залучені до співтовариства з безпеки ШІ.

Оцінка ризиків і загроз ШІ. Як зазначалося на Всесвітньому економічному форумі 2020 року, поряд з макроекономічними ризиками, геополітичними та геоекономічними загрозами і напруженістю, екологічними і кліматичними ризиками, біологічними загрозами глобальними визнаються і технологічні ризики. Технології продовжують відігравати важливу роль у формуванні глобального ландшафту ризиків. Технологічні загрози пов'язані з шахрайством щодо персональних даних і кібератаками на них, що спричинило посилення законодавства про персональні дані у Європі та інших країнах світу, де було виявлено низку технологічних вразливостей. Очікується, що ризики, пов'язані з фейковими новинами і крадіжкою особистих даних, будуть і надалі збільшуватися. Це супроводжується також загрозами для конфіденційності корпоративних і державних даних та інформації. Виявлені масові витоки даних, загрози програмного забезпечення показали потенційне використання ШІ для розробки більш потужних кібератак. Отримано додаткові докази того, що кібе-

ратаки створюють ризики для критично важливої інфраструктури, що спонукало країни посилити контроль за транскордонними угодами і кооперацією з міркувань національної безпеки. Дослідники Cybersecurity Ventures прогнозують, що світові втрати через кіберзлочинність зростатимуть на 15 % щорічно до 2025 року і сягатимуть 10,5 трлн дол., тоді як у 2015 році цей показник становив 3 трлн доларів.

Із розвитком інтернет-простору в Україні активізувалася кіберзлочинність, особливо під час карантину, коли в онлайн масштабно перейшли робота, покупки, зустрічі. Шахрайства з платіжними картками, крадіжки грошей з банківських рахунків, розповсюдження комп'ютерних вірусів, викрадення хакерами персональних даних громадян, онлайн-торгівля наркотиками, протидія піратству та поширенню протиправного контенту — це далеко не повний перелік злочинів, які розслідувала кіберполіція. Загалом, за даними Національної поліції України, у 2020 році було зареєстровано понад 5 тис. кіберзлочинів, вдалося оперативно затримати 106 фігурантів кримінальних проваджень [17].

За даними американської компанії Specops Software, яка досліджує питання кіберзахисту та кібербезпеки, Україна увійшла до десятки країн, *проти яких здійснювалися найбільш небезпечні кібератаки*. *Нещодавно Рада* національної безпеки і оборони України повідомила, що у 2021 році в країні зафіксовано вже майже 14 млн інцидентів у сфері кібербезпеки, однак масштабних кіберзагроз не зафіксовано. Водночас світова тенденція за останній місяць свідчить про збільшення випадків фішингу і продажу великих баз даних. В Україні більшість атак були спрямовані на державний сектор, а це понад 75 % усіх атак. Загалом протягом місяця найбільша кількість інцидентів була пов'язана з несанкціонованим доступом до комп'ютерних систем (70 % випадків), скануванням ресурсів (10 % випадків) і здійсненням атак типу brute-force (7 % випадків). До того ж окремо можна виділити фішингові атаки, яких було зафіксовано понад 400 тисяч [18]. Фахівці Національного координаційного центру кібербезпеки при РНБО України працюють над розробленням Стратегії кібербезпеки України.

Проблеми регулювання ШІ. Автори, що розробляли «Білу книгу зі штучного інтелекту. Європейський підхід до досконалості і довіри» визначають високоризикове застосування ШІ як таке, що впливає на права людей та компаній, створює загрозу травми, смерті або значної шкоди. Окремі застосування ШІ підпадатимуть під нове регулювання безвідносно до сектору, наприклад ті, що стосуються працевлаштування та прав робітників, дистанційної біометричної ідентифікації, наприклад за ходою, і технологій спостереження [3, 19]. Виділяють дві ключові групи ризиків. Перша група — ризики для основних прав, таких як право на свободу слова та зібрань, право на гідність, недискримінацію, захист персональних даних та конфіденційність, право на ефективну юридичну допомогу та справедливий суд і захист споживачів. Ці ризики можуть породжуватися недоліками загальної конструкції систем або використанням даних без виправлення можливих упереджень. ШІ збільшує також можливості відстежування й аналізу поведінки громадян та деанонімізації шляхом опрацювання і встановлення зв'язків між наборами великих даних, які самі по собі не містять персоніфікованої інформації. Вказується на важливу відмінність ШІ від людини в контексті ухвалення рішень: відсутність соціального контролю. Через особливості ШІ, такі як непрозорість («ефект чорної скриньки»), складність, непрогнозованість та часткова самостійність, складно перевірити дотримання законодавства ЄС, спрямованого на захист прав людини. Органам влади та громадянам може бути складно з'ясувати, як було ухвалене те чи інше рішення за

участю ШІ та чи були дотримані відповідні правила. Це може завадити ефективному доступу до правосуддя постраждалим від дій та рішень систем ШІ. Друга група — ризики для безпеки та ефективного функціонування режиму відповідальності. Це ризики для користувачів продуктів та послуг із вбудованим ШІ. Наприклад, хиба системи розпізнавання об'єктів в автономному авто може спричинити аварію з травмами та матеріальною шкодою.

Європейський інспектор із захисту даних Войцех Вівьоровський підтримав ризик-орієнтований та людиноцентричний підхід Єврокомісії, однак зазначив, що нова регуляторна база для ШІ повинна захищати від негативних наслідків не лише індивідів, а й спільноти та суспільство загалом; варто мати більш надійну та конкретну схему класифікації ***ризиків***, щоб кожна значна потенційна загроза від ШІ мала відповідні контрзаходи; необхідно чітко визначити прогалини в законодавстві, які потрібно заповнити; потрібно уникати накладок між наглядовими органами та містити механізм співпраці. Він підтримав також ідею мораторію на запровадження в Євросоюзі автоматизованих систем розпізнавання людських рис. Причому не лише облич, а й ходи, відбитків пальців, ДНК, голосу, натиску на клавіатуру та інших біометричних і поведінкових сигналів — принаймні, поки не буде запроваджено необхідну юридичну базу, яка гарантувала б пропорційність застосування відповідних технологій.

Права ІВ у галузі розвитку технологій ШІ. Європейський парламент 20 жовтня 2020 року прийняв Резолюцію про права ІВ у галузі розробки технологій ШІ (Intellectual property rights for the development of artificial intelligence technologies) (2020/2015 (INI)) [20]. Ось деякі основні положення цього документа. Оскільки правова база ЄС у сфері ІВ призначена для заохочення інновацій і творчості, а також доступу до знань та інформації; оскільки технології ШІ можуть утруднити ідентифікацію прав ІВ та їх застосування до продуктів, створених на основі ШІ, тим самим перешкоджаючи справедливій компенсації творцям людям, чиї оригінальні твори використовуються для управління такими технологіями, Європейський парламент бере до відома Білу книгу Європейської комісії зі штучного інтелекту — європейський підхід до досконалості та довіри і європейську стратегію обробки даних; підкреслює, що викладені тут підходи можуть допомогти розкрити потенціал ШІ, орієнтованого на людину, в ЄС; зазначає проте, що захист прав ІВ в контексті розвитку ШІ і пов'язаних з ним технологій не було взято до уваги ЄК, незважаючи на ключове значення цих прав; наголошує на необхідності створення Єдиного європейського простору даних і вважає, що його використання буде відігравати важливу роль в інноваціях і творчості економіки ЄС, які слід заохочувати; зазначає, що Союз повинен відігравати фундаментальну роль у визначенні основних принципів розробки, використання і застосування ШІ. Зазначає, що збалансований захист прав ІВ для технологій ШІ і багатовимірний характер такого захисту мають ключове значення, при цьому підкреслюється важливість забезпечення високого рівня захисту прав ІВ, забезпечення правової визначеності та створення необхідної довіри, заохочення інвестицій у ці технології та забезпечення їх довгострокової рентабельності та використання споживачами. Вважає, що технологічна творчість, породжена технологіями ШІ, має бути захищена правами ІВ для заохочення інвестицій в цю форму творчості та підвищення правової визначеності для громадян, підприємств і винахідників, які на сьогодні є одними з найбільш частих користувачів технологій ШІ. Вважає, що твори, створені самими штучними об'єктами і роботами, можуть не підпадати під захист авторських прав, щоб поважати принцип оригінальності, пов'язаний з людиною, оскільки термін

«інтелектуальна творчість» належить до особистості автора. Закликає Європейську комісію просувати горизонтальний, заснований на фактах і технологічно нейтральний підхід до загальних єдиних правил авторського права, які можуть застосовуватися до творів, вироблених ШІ у Союзі, якщо встановлено, що такі твори можуть бути захищені авторським правом; рекомендує, щоб усі права власності надавалися тільки фізичним або юридичним особам, які законно створили твір, і тільки за згодою правовласника, якщо використовується матеріал, захищений авторським правом, якщо не застосовуються виключення або обмеження авторського права.

Перспективи розвитку ШІ в Україні. Усі основні економіки світу (понад 30 країн) уже розробили національні стратегії розвитку штучного інтелекту. Так, зокрема, Канада, Китай, Росія, Франція, США, Японія, Фінляндія та Об'єднані Арабські Емірати мають чіткий план дій. Найкращі стратегії були підготовлені Францією, США, Китаєм, Японією та Фінляндією [21]. Україна поки що спромоглася лише на концепцію. Кабінет Міністрів України 2 грудня 2020 року затвердив Концепцію розвитку штучного інтелекту в Україні [22]. Документ використовує основні принципи Керівних принципів Організації економічного співробітництва і розвитку (ОЕСР) з питань штучного інтелекту (Recommendation of the Councilon Artificial Intelligence), до яких Україна приєдналася у 2019 році. Серед основних принципів розвитку та використання технологій ШІ визначено такі: ШІ має приносити користь людям і планеті, сприяючи інклюзивному зростанню, сталому розвитку та добробуту; системи ШІ розробляються та використовуються лише за умови дотримання верховенства права, а їх використання повинно забезпечуватися відповідними гарантіями, зокрема, можливістю безперешкодного втручання людини у процес функціонування системи, забезпеченням прозорості та відповідального розкриття інформації про системи ШІ; організації та особи, які розробляють, упроваджують або використовують системи ШІ, несуть відповідальність за їх належне функціонування відповідно до вищезазначених принципів. Мета концепції — вироблення стратегії для стимулювання розвитку і перетворення галузі ШІ на один з ключових драйверів цифрової трансформації та загального зростання економіки України. Концепція передбачає широке використання передових технологій ШІ у сфері освіти, економіки, соціального управління, кібербезпеки, оборони та інших сферах з метою зростання довгострокової конкурентоспроможності України на міжнародному ринку.

За даними дослідження Oxford Insights і Міжнародного центру розвитку досліджень Government AI Readiness Index 2020 року, в Україні зосереджена найбільша кількість компаній-розробників технологій ШІ в Східній Європі. Компанії у сфері ШІ з українським корінням уже придбали міжнародні корпорації Snap, Google, Rakuten. Активно використовуються в різних сферах і чатботи. Тому ШІ повинен стати одним з ключових драйверів цифрової трансформації та загального зростання економіки України. Розвиваючи сферу ШІ, ми забезпечуємо конкурентоспроможність України на міжнародному ринку. Одне із завдань, яке ставить уряд, — увійти до топ-10 країн з високим розвитком ШІ у світі (AI Readiness Indexby Oxford Insights, AI Indexby Stanford University). Основні напрями Концепції включають таке: удосконалення середньої, вищої освіти та підвищення кваліфікації з метою підготовки кваліфікованих фахівців та фахівчинь у сфері ШІ; стимулювання наукових досліджень у галузі, зокрема за допомогою грантів; стимулювання підприємництва в галузі ШІ, а також розробка методу перекваліфікації кадрів, які можуть втратити роботу через автоматизацію за 5–10 років; робота з підвищення рівня кібербезпеки, удоскона-

лення законодавства у сфері кіберзахисту; застосування технологій ШІ в оборонній сфері та публічному управлінні; розв'язання проблем роботи держреєстрів; використання ШІ в правосудді, зокрема для попередження небезпечних явищ завдяки аналізу наявних даних. На розробку та впровадження перших етапів концепції необхідно понад 14 млн грн у 2021–2023 роках.

З метою оцінки ефективності результатів реалізації рішень за пріоритетними напрямами, передбаченими в Концепції розвитку сфери штучного інтелекту в Україні, використовуються такі статистичні критерії результативності: використання технологій ШІ на підприємствах, у роботі державних органів; актуальність існуючих навчальних програм з технологій зі ШІ у закладах вищої освіти; створення нових навчальних курсів та освітніх програм про технології зі ШІ; створення нових робочих місць; кількість публікацій у виданнях провідних галузевих конференцій (CVPR\ICCV\ECCV — для комп'ютерного зору, NeurIPS, ICML, ICLR — для машинного навчання тощо) і провідних рецензованих виданнях, індекси цитування; міжнародні рейтинги (AI Readiness Indexby Oxford Insights, AI Indexby Stanford University тощо), індекси цитування. Передбачається також проведення моніторингу процесу реалізації рішень за пріоритетними напрямами, вказаними в Концепції розвитку сфери штучного інтелекту України, динаміки основних показників, досягнення прогнозованих результатів Міністерством цифрової трансформації України статистичним методом. Реалізація положень Концепції розвитку штучного інтелекту дасть змогу: здобути Україні відповідний сегмент світового ринку технологій ШІ та провідні позиції в міжнародних рейтингах (як результат — прихід іноземного інвестора в галузь); створити умови для участі України в діяльності міжнародних організацій та реалізації ініціатив щодо формування стратегій розвитку, регулювання та стандартизації ШІ у світі; упровадити технології ШІ у сфері освіти, економіки, публічного управління, кібербезпеки, оборони та інших сферах для зростання довгострокової конкурентоспроможності України на міжнародному ринку; сформувати адекватне та дієве правове поле для застосування технологій ШІ з огляду на міжнародні стандарти в галузі та передовий іноземний досвід її державного регулювання. На жаль, питання захисту прав ІВ не знайшли відображення у вказаній концепції.

Висновки. Пандемія прискорила тенденції цифрової трансформації економіки, зокрема Інтернет речей (IoT), великі дані (BigData), штучний інтелект (Artificial Intelligence), хмарні технології. Криза COVID-19 показала, що цифрові технології мають важливе значення для економічного розвитку та повсякденного життя. Люди здійснили великий цифровий стрибок, перемістивши в Інтернет свою роботу, навчання та соціальне життя. Водночас, локдаун виявив значні прогалини в цифровій інфраструктурі, ризики, загрози і небезпеки в застосуванні ШІ. Важливим стає розуміння сутності ШІ з позиції сучасних глобальних ризиків, загроз і небезпек, зокрема з точки зору виявлення та усунення міждисциплінарних прогалин регулювання для забезпечення національної безпеки. Така оцінка може стати основою для розробки більш детальних моделей забезпечення безпеки і сприяти більш ефективному контролю ризиків [23].

Розширення використання ШІ в цивільному обороті, у комерційних відносинах і підприємницькій діяльності формує потребу та запит на створення організаційно-економічного механізму, спеціальних правових норм, що регулюють сферу використання технологій ШІ, включаючи норми, що визначають правосуб'єктність і режими правової охорони, використання і захисту технологій ШІ, створених ними об'єктів, форми і види відповідальності при використанні

технологій ШІ, розробку еталонної класифікації технологій ШІ. Тому об'єктивно необхідна не тільки законодавча база для практичного використання і застосування технологій ШІ, а й побудова комплексної моделі правового регулювання, що включає також формування універсальних стандартів і правил застосування ШІ в майновому обороті і цифровому (віртуальному) технологічному середовищі, регулювання способів і форм застосування технологій ШІ, використання майнових прав ІВ на технології ШІ, особливостей правових режимів регулювання залежно від виду технології ШІ.

На відкритті дискусії «Інтелектуальна власність і штучний інтелект» (WIPO Conversationon Intellectual Property (IP) and Artificial Intelligence (AI): Third Session) Генеральний директор ВОІВ Дарен Танг зазначив, що ШІ на сьогодні визначає майбутнє інновацій, у зв'язку з цим у рамках багатосторонньої та всеосяжної політики необхідно забезпечити позитивний вплив технологій ШІ на економіку всіх країн та їх використання для скорочення технологічного розриву. За словами пана Танга, проблеми, пов'язані з іноземними інвестиціями, потрапляють у саме серце діючої системи ІВ і провокують низку взаємопов'язаних питань, які потребують горизонтального підходу. На його думку, для вирішення питань, пов'язаних зі ШІ, необхідним є цілісний підхід, що стосується всієї системи ІВ, а не конкретні види прав ІВ [24].

Список використаних джерел / List of references

1. *Андрощук Г. Тенденції розвитку технологій штучного інтелекту: економіко-правовий аспект. Теорія і практика інтелектуальної власності. 2019. № 3. С. 84–101. № 4. С. 59–69.*
2. *This alliance aims to accelerate the adoption of inclusive, trusted and transparent AI worldwide. URL: https://www.weforum.org/agenda/2021/01/global-ai-action-alliance/ (дата звернення: 30.01.2021).*
3. *KOMISJAEUROPEJSKABruksela, dnia 19.2.2020 r. COM(2020) 65 finalBIAŁAKSIĘGAwsprawiesztucznejinteligencjiEuropejskiepodejściedodoskonałościizaufania. URL: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_pl.pdf (дата звернення: 13.02.2021).*
4. *Геннадій Андрощук. Єврокомісія опублікувала «Білу книгу з штучного інтелекту». URL: https://yur-gazeta.com/golovna/evrokomisiya-opublikuvala-biluknigu-z-shtuchnogo-intelektu.html (дата звернення: 30.01.2021).*
5. *World Intellectual Property Indicators 2020.*
URL: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_941_2020.pdf (дата звернення: 14.02.2021).
6. *Андрощук Г. О. Винаходи штучного інтелекту. Інтелектуальна власність в Україні. 2020. № 11. С. 67.*
7. *Глушков В. М. Кибернетика. Вопросы теории и практики. Москва : Наука, 1986. 488 с.*
8. *Морхат П. М. Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы : дисс. … д-ра юрид. наук. РГАИС. Москва, 2018. С. 243.*
9. *Про авторське право, дизайн і патенти : Закон Великої Британії від 1988 року. URL: https://www.legislation.gov.uk/ukpga/1988/48/contents (дата звернення: 30.01.2021).*

10. Абрамова Е. Н., Старикова Е. В. Искусственный интеллект как субъект авторского права. Гипотеза / Hypothesis. Право. Экономические науки. 2020. № 1 (10) март. С. 32–38.
11. Андрощук Г. О. Машина винахідник: що вирішило ЄПВ. Інтелектуальна власність в Україні. 2020. № 2. С. 58–59.
12. Андрощук Г. О. Прецедент: твори, створені AI, мають право на захист авторських прав!? Інтелектуальна власність в Україні. 2020. № 1. С. 57–59.
13. Caldwell, M., Andrews, J.T.A., Tanay, T. et al. AI-enabled future crime. Crime Sci 9, 14 (2020). URL: https://doi.org/10.1186/s40163-020-00123-8 (дата звернення: 30.01.2021).
14. AI-enabled future crime. URL: https://crimesciencejournal.
biomedcentral.com/articles/10.1186/s40163-020-00123-8 (дата звернення: 30.01.2021).
15. Deepfakes' ranked as most serious AI crime threat. URL: https://www.ucl.ac.uk/news/2020/aug/deepfakes-ranked-most-serious-ai-crime-threat (дата звернення: 30.01.2021).
16. Баранов О. А. Інтернет речей і штучний інтелект: витоки проблеми правового регулювання (частина 1). IT Право: проблеми і перспективи розвитку в Україні (Друга міжнародна щорічна конференція).
URL: http://aphd.ua/publication-376/.
17. У 2020-му Нацполіція викрила понад 5 000 кіберзлочинів. URL: https://yurgazeta.com/golovna/u-2020mu-nacpoliciya-vikrila-ponad-5-000-kiberzlochiniv.html (дата звернення: 01.02.2021).
18. НКЦК: у 2021 році в Україні зафіксовано вже майже 14 мільйонів інцидентів у сфері кібербезпеки. URL : https://www.rnbo.gov.ua/ua/
Diialnist/4797.html (дата звернення: 01.02.2021).
19. Гайдай Юрій. Виклики близького майбутнього: як ЄС хоче регулювати штучний інтелект. URL: https://www.eurointegration.com.ua/articles/
2021/02/9/7119423/ (дата звернення: 13.02.2021).
20. Intellectual property rights for the development of artificial intelligence technologies. URL: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_EN.html (дата звернення: 13.02.2021).
21. Przeglądstrategiirozwojusztucznejinteligencjina świecie elix.pl/rynek/raporty-prezentacje/2018/07/przeglad-strategii-rozwoju-sztucznej-inteligencji-na-swiecie/ (дата звернення: 13.02.2021).
22. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р URL: http://search.ligazakon.ua/l_doc2.nsf/link1/KR201556.html (дата звернення: 03.02.2021).
23. Карцхия А. А. Искусственный интеллект как средство управления в условиях глобальных рисков. URL: https://www.kbtu.kz/images/
elibrary_42715049.pdf (дата звернення: 01.02.2021).
*24. WIPO Director General Opens WIPO Conversation on IP and AI: Third Session. URL: https://www.wipo.int/about-wipo/en/dg_tang/news/2020/news_*
0014.html (дата звернення: 04.02.2021).

1. Androshchuk H. Tendentsii rozvytku tekhnolohii shtuchnoho intelektu: ekonomiko-pravovyi aspekt. Teoriia i praktyka intelektualnoi vlasnosti. 2019. № 3. S. 84–101. № 4. S. 59–69.
2. This alliance aims to accelerate the adoption of inclusive, trusted and transparent AI worldwide. URL: https://www.weforum.org/agenda/2021/01/global-ai-action-alliance/ (data zvernennia: 30.01.2021).
3. KOMISJAEUROPEJSKABruksela, dnia 19.2.2020 r. COM(2020) 65 finalBIAŁAKSIĘGAwsprawiesztucznejinteligencjiEuropejskiepodejściedodoskonałości-

izaufania. URL: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_pl.pdf (data zvernennia: 13.02.2021).

4. Hennadii Androshchuk. Yevrokomisiia opublikuvala «Bilu knyhu z shtuchnoho intelektu». URL: https://yur-gazeta.com/golovna/evrokomisiya-opublikuvala-biluknigu-z-shtuchnogo-intelektu.html (data zvernennia: 30.01.2021).

5. World Intellectual Property Indicators 2020. URL: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_941_2020.pdf (data zvernennia: 14.02.2021).

6. Androshchuk H. O. Vynakhody shtuchnoho intelektu. Intelektualna vlasnist v Ukraini. 2020. № 11. S. 67.

7. Hlushkov V. M. Kybernetyka. Voprosы teoryy y praktyky. Moskva : Nauka, 1986. 488 s.

8. Morkhat P. M. Pravosubъektnost yskusstvennoho yntellekta v sfere prava yntellektualnoi sobstvennosty: hrazhdansko-pravovыe problemы : dyss. … d-ra yuryd. nauk. RHAYS. Moskva, 2018. S. 243.

9. Pro avtorske pravo, dyzain i patenty : Zakon Velykoi Brytanii vid 1988 roku. URL: https://www.legislation.gov.uk/ukpga/1988/48/contents (data zvernennia: 30.01.2021).

10. Abramova E. N., Starykova E. V. Yskusstvennыi yntellekt kak subъekt avtorskoho prava. Hypoteza / Hypothesis. Pravo. Эkonomycheskye nauky. 2020. № 1 (10) mart. S. 32–38.

11. Androshchuk H. O. Mashyna vynakhidnyk: shcho vyrishylo YePV. Intelektualna vlasnist v Ukraini. 2020. № 2. S. 58–59.

12. Androshchuk H. O. Pretsedent: tvory, stvoreni AI, maiut pravo na zakhyst avtorskykh prav!? Intelektualna vlasnist v Ukraini. 2020. № 1. S. 57–59.

13. Caldwell, M., Andrews, J.T.A., Tanay, T. et al. AI-enabled future crime. Crime Sci 9, 14 (2020). URL: https://doi.org/10.1186/s40163-020-00123-8 (datazvernennia: 30.01.2021).

14. AI-enabled future crime. URL: https://crimesciencejournal.
biomedcentral.com/articles/10.1186/s40163-020-00123-8 (data zvernennia: 30.01.2021).

15.'Deepfakes ranked as most serious AI crime threat. URL: https://www.ucl.ac.uk/news/2020/aug/deepfakes-ranked-most-serious-ai-crime-threat (data zvernennia: 30.01.2021).

16. Baranov O. A. Internet rechei i shtuchnyi intelekt: vytoky problemy pravovoho rehuliuvannia (chastyna 1). IT Pravo: problemy i perspektyvy rozvytku v Ukraini (Druha mizhnarodna shchorichna konferentsiia).
URL: http://aphd.ua/publication-376/.

17. U 2020-mu Natspolitsiia vykryla ponad 5 000 kiberzlochyniv. URL: https://yur-gazeta.com/golovna/u-2020mu-nacpoliciya-vikrila-ponad-5-000-kiberzlochiniv.html (data zvernennia: 01.02.2021).

18. NKTsK: u 2021 rotsi v Ukraini zafiksovano vzhe maizhe 14 milioniv intsydentiv u sferi kiberbezpeky. URL : https://www.rnbo.gov.ua/ua/
Diialnist/4797.html (data zvernennia: 01.02.2021).

19. Haidai Yurii. Vyklyky blyzkoho maibutnoho: yak YeS khoche rehuliuvaty shtuchnyi intelekt. URL: https://www.eurointegration.com.ua/articles/
2021/02/9/7119423/ (data zvernennia: 13.02.2021).

20. Intellectual property rights for the development of artificial intelligence technologies. URL: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_EN.html (data zvernennia: 13.02.2021).

21. Przeglądstrategiirozwojusztucznejinteligencjina świecie elix.pl/rynek/raporty-prezentacje/2018/07/przeglad-strategii-rozwoju-sztucznej-inteligencji-na-swiecie/ (data zvernennia: 13.02.2021).

22. Pro skhvalennia Kontseptsii rozvytku shtuchnoho intelektu v Ukraini : Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 2 hrudnia 2020 r. № 1556-r URL:

http://search.ligazakon.ua/l_doc2.nsf/link1/KR201556.html (data zvernennia: 03.02.2021).

23. Kartskhyia A. A. Yskusstvennыi yntellekt kak sredstvo upravlenyia v uslovyiakh hlobalnыkh ryskov. URL: https://www.kbtu.kz/images/elibrary_42715049.pdf (data zvernennia: 01.02.2021).

24. WIPO Director General Opens WIPO Conversation on IP and AI: Third Session. URL: https://www.wipo.int/about-wipo/en/dg_tang/news/2020/news_0014.html (data zvernennia: 04.02.2021).

Надійшла до редакції 24.03.2021 року

Андрощук Г. Искусственный интеллект: экономика, Интеллектуальная собственность, угрозы. В работе представлены экономико-правовой анализ состояния и тенденций развития искусственного интеллекта (ИИ), определено его влияние на экономику, роль интеллектуальной собственности (ИС), дана оценка рисков, угроз и опасностей уголовного применения ИИ, выработаны механизмы соответствующей противодействия. Рассмотрено развитие технологий ИИ как неотъемлемой части «Индустрия 4.0», исследованы основные положения «Белой книги по искусственному интеллекту» ЕС. В правовом регулировании ИИ рассматривается как новый вызов для экономики и правовой системы, новое явление, имеющее мультипликационный эффект, правовой феномен в структуре правоотношений, новый объект для правового регулирования. Внедрение ИИ в сферу ИС формирует новые правовые и экономические проблемы. Проведен анализ рассмотренных судами дел, связанных с проблемой правосубъектности ИИ, изучено законотворческую деятельность по этому вопросу. Указано на возможности и опасности уголовного применения ИИ, которые проранжированы в порядке уровня их опасности. Определены перспективы развития ИИ в Украине, проанализированы Концепцию развития искусственного интеллекта в Украине. Сделан вывод о том, что ИИ должен стать одним из ключевых драйверов цифровой трансформации и общего роста экономики Украины.

Ключевые слова: искусственный интеллект, экономическое влияние, интеллектуальная собственность, регулирование, кибербезопасность, риски, угрозы, национальная безопасность

Androshchuk G. Artificial intelligence: economy, intellectual property, threats. Artificial intelligence (AI) technologies, the spread of which is based on the widespread use of digital information and the rapid growth of computing power, are leaving the realm of purely theoretical research and becoming one of the segments of the world market that can have truly revolutionary consequences. The paper provides economic and legal analysis of the state and trends of AI, identifies its impact on the economy, the importance of the role of intellectual property (IP), assesses the risks, threats and dangers of criminal use of AI, developed mechanisms to counter them. The development of AI technologies as an integral part of «Industry 4.0» is considered, the main provisions of the «White Paper on Artificial Intelligence» of the EU are studied.

Over the next decade, the EU plans to spend $20 billion a year on AI development. At the same time, the protection of IP rights in the context of AI development and related technologies has been unconsidered by the Commission, despite the key importance of these rights. In legal regulation, AI is seen as a new challenge for the economy and the legal system, a new phenomenon that has a multiplier effect, a legal phenomenon in the structure of legal relations, a new object for legal regulation.

The introduction of AI in the field of IP creates new legal and economic problems. The creation of AI works is an integral area of activity in the modern digital economy. These circumstances bring to the fore the problem of recognition of authorship in the creation of AI works, the possibility of authors to dispose of their rights and their use of mechanisms for legal protection of IP. The analysis of the cases considered by courts connected with a problem of legal personality of AI is carried out, legislative activity on this question is studied. Possibilities and dangers of criminal use of AI are shown. They are ranked in order of their level of danger — depending on the harm they may cause, the potential benefit or the benefit of crime. Prospects for the development of AI in Ukraine are shown, the Concept of development of artificial intelligence in Ukraine is analysed. It is concluded that AI should become one of the key drivers of digital transformation and overall growth of Ukraine's economy.

Keywords: artificial intelligence, economic impact, intellectual property, regulation, cybersecurity, risks, threats, national security