ISSN 2308-0361

УДК 330.341.1
DOI: https://doi.org/10.33731/22021.236555

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

Постановка проблеми. Цифрові технології здійснюють істотний вплив на розвиток традиційних галузей економіки і є складовою частиною сучасних управлінських систем у підприємництві, державному управлінні, у сферах оборони країни, безпеки держави і забезпечення правопорядку, а також створюють нові бізнес-моделі. Технології штучного інтелекту, поширення яких засновано на масовому використанні цифрової інформації та стрімкому зростанні обчислювальної потужності комп'ютерів, виходять зі сфери чисто теоретичних досліджень і стають одним із сегментів світового ринку, що може зумовити по-справжньому революційні результати. Встановлюючи зв'язки між мільярдами зовні не пов'язаних один з одним елементів інформації, системи ШІ в змозі забезпечувати підвищення точності прогнозів погоди і зростання врожайності культур, покращувати діагностику захворювань, передбачати епідемії та підвищувати продуктивність праці у промисловості. У міру розширення можливостей ШІ зростають ризики

* Початок. Продовження в наступному номері.

його кримінального використання як у конкретній сфері обчислення (кібербезпека), так і в усіх сферах життєдіяльності. Деякі з цих загроз виникають як продовження існуючої злочинної діяльності, водночас інші можуть бути новими. Отож необхідно визначити, якими можуть бути ці загрози і як вони можуть вплинути на економіку та суспільство.

Метою статті є економіко-правовий аналіз стану і тенденцій розвитку ШІ, визначення його впливу на економіку, ролі інтелектуальної власності, оцінка ризиків, загроз і небезпеки застосування ШІ, вироблення механізмів протидії.

Аналіз досліджень і публікацій. Проблемам розвитку ШІ приділяють значну увагу ті, хто формує технологічну складову розвитку світу, — Ілон Маск, Стівен Хокінг, Марк Цукерберг, Джозеф Безос, а також фахівці, які нині в провідних лабораторіях та інститутах світу розробляють власне ШІ. Вагомий внесок у дослідження феномену ШІ здійснили іноземні науковці: А. Тюрінг (Alan Turing), Д. Баррат (James Barrat), Е. Хорвіц (Eric Horvitz), Н. Бостром (Niklas Boström), І. Маск (Elon Musk), Д. Дайсон (George Dyson), К. Келлі (Kevin Kelly), Р. Кало (Ryan Calo), П. Асаро (Peter M. Asaro), В. Віндже (Vernor Steffen Vinge), К. Шваб (K. Schwab), Е. А. Войниканис, П. М. Морхат, А. Г. Серго, О. А. Ястребов. Активно вивчають цю проблематику українські вчені: Г. О. Андрощук, О. А. Баранов, В. М. Брижко, І. Б. Жиляєв, О. С. Вишневський, О. М. Вінник, М. В. Карчевський, В. І. Ляшенко, В. А. Мисливий, В. Г. Пилипчук, О. Е. Радутний, Н. А. Савінова, М. О. Стефанчук, В. М. Фурашев, Є. О. Харитонов, О. І. Харитонова, А. І. Шевченко, І. Г. Яненкова та інші. Водночас, комплексний і міждисциплінарний характер цієї проблематики, динамічність змін у зазначеній сфері потребує подальших науково-технічних та економіко-правових досліджень, зокрема щодо економічного впливу ШІ, ролі інтелектуальної власності в його створенні, існуючих та потенційних ризиків, загроз і небезпек.

Виклад основного матеріалу. Економічний вплив ШІ. Слід зазначити, що розвиток технологій ШІ є невід'ємною частиною четвертої промислової революції «Індустрія 4.0». Індустрія 4.0 — це впровадження автоматизованих виробництв, у яких використовуються Інтернет речей (IoT), великі дані (BigData) та кіберфізичні системи, тобто такі, де людина майже не втручається у виробничий процес. З'являються розумні фабрики, на яких машини комунікують між собою. Аналітики міжнародного консалтингового агентства PwC вважають, що у найближче десятиріччя ШІ стане головною ринковою тенденцією та кращим бізнес-інструментом. Згідно з останнім звітом внесок інтелектуальних технологій у глобальний світовий ВВП оцінюється у 15,7 трлн доларів. За прогнозами експертів, саме завдяки ШІ до 2030 року цей показник виросте ще на 14 %. При цьому на збільшення продуктивності припаде до 7 трлн дол., а на зростання споживання — понад 9 трлн доларів. На думку PwC, у найближчі 5–10 років лідером з успішної експлуатації та адаптації технологій ШІ буде Китай. Передбачається, що до 2030 року його ВВП може виявитися ще на 26 % вище середнього світового показника. Істотний потенціал має і Північна Америка, яка, імовірно, покаже близько 14 % додатково до ВВП. Західна Європа поки що відстає [1]. Це визначає ШІ як найбільшу економічну можливість наступного десятиріччя, що становить більшу цінність, ніж нинішні страхування, нафта і газ, комерційна нерухомість і автомобільна промисловість разом узяті. Про це йдеться в доповіді, підготовленій експертами для Всесвітнього економічного форуму 2021 року в Давосі [2]. ШІ, окрім вказаного, може принести суспільству величезну користь. Так, дослідження, проведене Google у 2018 році, виявило 2602 випадки викори-

стання ШІ, що сприяють суспільному благу. Усе частіше люди застосовують ШІ для вирішення критичних соціальних проблем, наприклад, підвищення врожайності сільськогосподарських культур, перепідготовки робітників і боротьби з COVID-19. Водночас зі зростанням соціально-економічного потенціалу ШІ з'являються й ризики, пов'язані з небезпечними або неетичними системами ШІ. Суперечки щодо застосування технологій розпізнавання облич, автоматичного прийняття рішень і відстеження людей, пов'язаних з COVID-19, показали, що реалізація повного потенціалу ШІ потребує контролю з боку урядів, щоб ШІ застосовувався виключно в етичних рамках. Багато компаній і урядів погодилися з цим, і на сьогодні вже розроблено понад 175 наборів етичних принципів розробки та використання ШІ. Однак існує проблема в реалізації цих принципів — легше визначити етичні стандарти, яким повинна відповідати система, ніж утілювати їх на практиці. До того ж, часто ці принципи застосовуються розрізнено й неузгоджено, а механізмів для спільного застосування немає. Хоча ШІ обіцяє покращити життя мільярдів людей, на сьогодні доступ до нього більшості громадян світу є нерівномірним.

Одна з причин — відсутність інклюзивності: за даними Інституту AINow при Нью-Йоркському університеті, тільки 18 % авторів на провідних конференціях зі ШІ — жінки, приблизно 80 % розробників ШІ — чоловіки, а небілі інженери становлять менше 5 % співробітників більшості великих технологічних компаній. Якщо поточні тенденції збережуться, Північна Америка, Європа і Китай отримають 80 % економічних вигод від ШІ, а решті двом третинам населення світу залишиться лише 20 % [2]. Це призведе до загострення глобальної нерівності, не кажучи вже про величезні втрачені можливості покращити економічне становище мільярдів людей. Не дивно, що багато людей бояться майбутнього, яке може принести ШІ: згідно з дослідженнями Оксфордського університету і Європейської комісії 84 % американців і 88 % європейців вважають, що ШІ слід «обережно керувати» на основі його потенціалу, інакше він може призвести до згубних для суспільства наслідків.

Вплив ШІ на промисловість і суспільство з кожним днем посилюється, отже існує гостра необхідність спільно розробити норми етичного використання ШІ в інтересах світової громадськості. Саме тому Всесвітній економічний форум запустив The Global AI Action Alliance, нову платформу для спільної роботи за участю багатьох зацікавлених сторін та інкубатор проектів, призначений для прискорення впровадження інклюзивного, надійного та прозорого ШІ в усьому світі та в усіх галузях промисловості. Альянс об'єднує понад 100 провідних компаній, урядів, міжнародних організацій, некомерційних організацій і вчених. Члени альянсу спільно працюють над розробкою та впровадженням інструментів з метою забезпечення етичності ШІ для всіх груп суспільства. Альянс отримав грант від Фонду Патрика Дж. Макговерна, він контролюється також Керівним комітетом провідних світових лідерів з галузі ШІ під співголовуванням Арвінда Крішни, голови та генерального директора IBM. Жодна організація не може окремо вирішити весь спектр завдань щодо створення і безпечного функціонування ШІ, тому ефективною буде тільки масштабна співпраця всіх зацікавлених сторін.

Біла книга зі штучного інтелекту (AI): європейський підхід [3, 4]. *«Оскільки цифрові технології стають усе більш важливою частиною кожного аспекту життя, люди повинні мати можливість довіряти їм. Достовірність також є умовою його реалізації. Це можливість для Європи, враховуючи її тверду прихильність цінностям і верховенству закону, а також доведену здатність створювати безпечні, надійні і складні продукти і послуги від*

*авіації до енергетики, автомобільного і медич*ного обладнання», — йдеться в передмові до Європейської Білої книги зі штучного інтелекту (AI).

«Біла книга зі штучного інтелекту. Європейський підхід до досконалості і довіри» (ang. White Paperon Artificial Intelligence A European approach to excellence and trust), опублікована 19 лютого 2020 року, має на меті представити можливі зміни, «які сприятимуть надійному та безпечному розвитку штучного інтелекту в Європі при повній повазі цінностей і прав громадян ЄС». Комісія запропонувала створити правові засади для штучного інтелекту, засновані на «досконалості та довірі»:

- екосистема переваги, що розуміється як політична основа для дій на європейському, національному та регіональному рівнях, які повинні трансформуватися в партнерство між приватним і державним секторами. Мобілізація діяльності повинна полягати в усьому ланцюжку дій: від досліджень до створення стимулів для прийняття рішень, зокрема для малих і середніх підприємств (МСП);
- довірча екосистема, тобто забезпечення відповідності правилам ЄС, включаючи правила, що захищають основні права і права споживачів, зокрема, у разі систем ШІ, експлуатованих у ЄС, які становлять високий ризик.

ЄК гарантує, що вона хоче спонукати як державні установи, так і підприємців, включаючи малі та середні компанії, швидше впроваджувати штучний інтелект. Для розвитку ШІ ЄС також повинен інвестувати в дослідження і роботу вчених.

«Європейський підхід до ШІ спрямований на просування інноваційного потенціалу Європи у сфері ШІ, підтримуючи при цьому розвиток і використання етичного і такого, що заслуговує на довіру, ШІ в усій економіці ЄС. ШІ повинен працювати на людей і бути силою, яка працює на благо суспільства…», — ідеться в Білій книзі AI. На думку Євросоюзу, штучний інтелект у ЄС повинен бути орієнтований на людину. На практиці це означає, що системи ШІ повинні бути прозорими, користувач повинен знати про їх використання, і вони повинні контролюватися людиною. І саме людина, а не машина, повинна приймати остаточні рішення.

Комісія також хоче конкретно контролювати використання ШІ в системах високого ризику, тобто в системах, які можуть порушувати права громадян, наприклад, право на недоторканність приватного життя.

«Такі системи включають, наприклад, медичні дані, які містять детальну інформацію про стан здоров'я жителів, дані про набір персоналу, дані поліції і правоохоронних органів», — зазначила комісар ЄС з цифрових питань Маргрете Вестагер. Згідно з директивою ЄС ШІ, що використовується в системах цього типу, повинен бути протестований і сертифікований, перш ніж його буде дозволено використовувати. Комісія також посилається на використання системи розпізнавання облич. Чиновники ЄС вказали, що на сьогодні віддалений збір так званих біометричних даних регулюється правилами захисту даних ЄС, включаючи GDPR *(англ. General Data Protection Regulation, GDPR; Regulation (EU) 2016/679*), і, як правило, заборонений. Він може використовуватися тільки у виняткових, належним чином обґрунтованих і адекватних випадках на підставі законодавства ЄС або національного законодавства. Комісія хоче розпочати широку дискусію про те, які обставини можуть виправдати такі винятки і чи слід, і на яких умовах, дозволяти використання розпізнавання облич у громадських місцях. Документ також стосується правил використання ШІ у так званих системах з низьким рівнем ризику, таких як онлайн-ігри. У цій ситуації ЄК пропонує ввести добровільну систему маркуван-

ня для компаній, які застосовують більш високі стандарти. Документ комісії засвідчує, що ЄС має всі можливості стати світовим лідером у розробці безпечних систем ШІ.

«Щоб Європа повною мірою використовувала можливості, що надаються ШІ, вона повинна розвивати і зміцнювати необхідні виробничі та технологічні можливості...», — ідеться в Білій книзі AI.

«У нас є чудові дослідні центри, захищені цифрові системи і міцна позиція як у галузі робототехніки, так і у виробництві, а також у сфері послуг у широкому діапазоні — від транспорту, енергетики, систем охорони здоров'я до сільськогосподарської політики», — запевнила президент ЄС Урсула фон дер Лайєн. Упродовж наступного десятиріччя ЄС планує витрачати 20 млрд дол. на рік на розвиток ШІ. Тепер Біла книга зі штучного інтелекту буде проходити публічні консультації. На основі зібраних відгуків Комісія зробить подальші кроки щодо розвитку безпечного ШІ у Європейському Союзі.

ШІ та інтелектуальна власність. Генеральний директор ВОІВ Дарен Танг у ключовій доповіді ВОІВ «Світові показники діяльності в галузі інтелектуальної власності» (World Intellectual Property Indicators 2020) зазначив: *«Активне використання інструментів інтелектуальної власності свідчить про високий рівень інновацій і творчості в кінці 2019 р., якраз на початку пандемії COVID-19. Пандемія зміцнила тенденції, що давно зароджувалися, шляхом стимулювання використання нових технологій і прискорення цифровізації у повсякденному житті. Оскільки інтелектуальна власність настільки тісно пов'язана з технологіями, інноваціями і процесом цифровізації у світі, після закінчення пандемії вона стане ще важливішою для більшої кількості країн»* [5].

ШІ у правовому регулюванні розглядається як новий виклик для правової системи, нове явище, що має мультиплікаційний ефект, правовий феномен у структурі правовідносин, новий об'єкт для правового регулювання. Результатом сучасного науково-технологічного розвитку стало те, що ШІ здатний генерувати і створювати різні твори науки, літератури і мистецтва. Така здатність ШІ є невід'ємною сферою діяльності в сучасній цифровій економіці. Ці обставини актуалізують проблеми визнання авторства при створенні творів ШІ, можливості розпорядження авторами своїми правами і використання ними механізмів правової охорони об'єктів інтелектуальної власності. Результатом правового регулювання в Україні питань, пов'язаних з наявністю або відсутністю правосуб'єктності у ШІ, буде формування чіткого розуміння права у сфері використання результатів діяльності ШІ. Оскільки в національному законодавстві у сфері ІВ питання самостійної правосуб'єктності ШІ не вирішене, доцільно звернутися до аналізу зарубіжного законодавства та доктринальних позицій з цієї проблеми.

Згідно зі звітом Відомства інтелектуальної власності Великої Британії (IPO) «Штучний інтелект: всесвітній огляд патентів на AI і патентування в секторі AI Великої Британії» (Artificial Intelligence: A worldwide overview of AI patents and patenting by the UK AI sector), кількість опублікованих патентних заявок, що стосуються ШІ, за останнє десятиріччя збільшилася на 400 %. Кількість патентних заявок з використанням технології ШІ, поданих у США, збільшилася удвічі в період з 2002 до 2018 року. Всесвітня організація інтелектуальної власності розпочала серію консультацій про ШІ та інтелектуальну власність. Постійно обговорюється питання про те, чи слід захищати творіння ШІ авторськими правами, правами на дизайн, патентами або правами особливого роду-suigeneris. Існують добре відомі спірні приклади винаходів ШІ, такі як незвичайна, однак ефективна антена, розроблена у 2004 році для НАСА «еволюційним» програмним забезпеченням, і принаймні

один виданий патент був приписаний винахідливому ІШ. Виданий у 2005 році патент США № 6 847 851 стосується схеми, винахідником названий Джон Коза, хоча, як пізніше з'ясувалося, вона була розроблена за допомогою генетичного програмування [6].

Один із фундаторів кібернетики академік В. М. Глушков наголошував, що створення штучного інтелекту — це завдання великої складності, яке неможливо вирішити одразу в результаті геніального осяяння винахідника-одинака. І хоча в 1986 році вчений вважав, що до вершин творчості комп'ютерам досить далеко, проте вже тоді він вказав на факт видачі авторських свідоцтв на винаходи, зроблені комп'ютерами [7, 423, 429].

Упровадження ШІ у сферу ІВ формує нові правові та економічні проблеми. Звісно ж, замість того щоб наділяти ШІ правосуб'єктністю у сфері ІВ, можна передавати права на результати «творчої» діяльності ШІ фізичним особам, які брали участь у створенні ШІ і його функціонуванні. Іншою альтернативою є віднесення об'єктів ІВ, створених ШІ, до категорії суспільного надбання. Однак П. М. Морхат у своїй докторській дисертації, присвяченій теоретико-правовому науковому дослідженню поняття, особливостей, правової природи, сфер застосування і меж застосовності юнітів (систем, пристроїв) ШІ, акцентує увагу на тому, що якщо результати діяльності ШІ будуть вільно використовуватися, то внаслідок відсутності економічної вигоди може піти на спад зацікавленість компаній, що створюють ШІ, в інноваційному зростанні [8, 169].

На сьогодні в багатьох країнах авторські права надаються лише на твори інтелектуальної творчості людини. Бюро реєстрації авторських прав США заявляє, що «зареєструє оригінальний авторський твір за умови, що твір створений людиною».

У п. 3 статті 9 Закону Великої Британії «Про авторське право, дизайн і патенти» [9] зазначено, що «стосовно літературного, драматичного, музичного або художнього твору, згенерованого комп'ютерною системою, автором буде вважатися особа, за допомогою якої вживаються заходи, необхідні для створення твору». Так само Австралійське і Європейське патентні відомства в багатьох випадках визнавали і надавали патентні права тільки на об'єкти, створені людиною. Деякі країни, зокрема Індія, Велика Британія, Ірландія, Нова Зеландія і Гонконг, вважають за краще визнати зусилля, докладені для створення ШІ, який надає творчий контент. Отже, програміст ШІ отримує авторство творів [10].

Європейське патентне відомство (ЄПВ) опублікувало своє рішення від 27 січня 2020 року з викладенням причин відмови у двох європейських патентних заявках, у яких система ШІ була позначена як винахідник. Подані фізичною особою восени 2018 року заявки EP 18 275 163 і EP 18 275 174 були відхилені ЄПВ після усного розгляду із заявником у листопаді 2019 року на тій підставі, що вони не відповідають юридичним вимогам Європейської патентної конвенції (EPC): винахідник, вказаний у заявці, має бути людиною, а не машиною. В обох програмах у якості винахідника названа машина, що називається «DABUS», яка описується як «тип штучного інтелекту зв'язності». Заявник стверджував, що придбав право на європейський патент у винахідника, будучи його правонаступником, зазначаючи, що як власникові машини йому були передані будь-які права інтелектуальної власності, створені цією машиною. У своїх рішеннях ЄПВ вважало, що тлумачення правових рамок європейської патентної системи спонукає до висновку, що винахідник, зазначений у європейському патенті, повинен бути фізичною особою. Бюро також вказало, що розуміння терміна «винахідник», який стосується фізичної особи, є міжнародним стандартом і що різні національні суди ухвалили відповідні рішення. Окрім

цього, призначення винахідника є обов'язковим, оскільки воно має низку правових наслідків, зокрема, для забезпечення того, щоб призначений винахідник був законним і щоб він або вона могли користуватися правами, пов'язаними з цим статусом. Щоб скористатися цими правами, винахідник повинен володіти правосуб'єктністю, якою не володіють системи ШІ або машини. Нарешті присвоєння імені машині недостатньо для задоволення вимог вищевказаної EPC [11].

Варто згадати перший судовий прецедент. У січні 2020 року суд у Шеньчжені, провінція Гуандун (КНР), постановив, що твір, створений ШІ, може бути захищений авторським правом. Рішення було прийнято після того, як технічний гігант Tencent подав до суду на онлайн-платформу, яка надала інформацію про кредити за копіювання статті, написаної роботом Tencent Dreamwriter, без дозволу. Dreamwriter — це автоматизована програма для написання новин, заснована на даних і алгоритмах, розроблена Tencent у 2015 році. Dreamwriter 20 серпня 2018 року написала фінансовий звіт, що включає індекс Шанхая за цей день, обмін валюти і рух капіталу. У статті, опублікованій на веб-сайті Tencent Securities, зазначено, що *«стаття була автоматично написана Tencent Robot Dreamwriter»*. Пізніше компанія Shanghai Yingxun Technology скопіювала її на свій сайт. Народний суд району Наньшань заявив, що відповідач — Shanghai Yingxun Technology Company — порушила авторські права Tencent і повинна нести цивільну відповідальність. Суд заявив, що форма вираження статті відповідає вимогам письмового твору, а зміст показав вибір, аналіз та оцінку відповідної інформації і даних про фондовий ринок. Це свідчить, що структура статті була розумною, логіка — зрозумілою, і в ній була відповідна оригінальність. З огляду на те що відповідач вилучив роботу, що порушує авторські права, шанхайській компанії Yingxun Technology було наказано виплатити Tencent 1500 юанів (216 дол. США) за економічні втрати і захист прав. Суд не повідомив, чи подаватиме шанхайська компанія апеляцію.

«Згідно з нашим законом про авторське право, а також деякими міжнародними конвенціями, визначення твору в першу чергу підкреслює, що творіння є оригінальним, відтвореним і здійсненим на основі інтелектуальної діяльності людини. Таким чином, людський інтелект є ядром і передумовою», — зазначив Ван Гохуа, юрист пекінської юридичної фірми Zhongwen. За його словами, якщо контент створювався машинами після того, як люди вводили якісь ключові слова, то машини повинні бути автором, а не людським інтелектом, а контент не повинен захищатися в сенсі закону про авторське право. *«Оскільки машини можуть використовуватися будь-якою людиною і генерувати один і той же контент під одними і тими ж ключовими словами, нам потрібно подумати про те, що саме захищає закон про авторське право, — інтелектуальну діяльність за вибором ключових слів або твір, дійсно створений людським інтелектом»*, — додав він [12].

На підставі аналізу розглянутих судами справ, пов'язаних з проблемою правосуб'єктності ШІ, і вивчення законотворчої діяльності з цього питання, дослідниками вказується, що для вирішення проблеми визначення прав ІВ на створений ним твір, можливі такі варіанти: 1. Не наділяти ШІ правами автора і не визнавати створений твір об'єктом ІВ. 2. Визнати за ШІ права автора. 3. Розподілити авторські права між ШІ і фізичною особою, яка брала участь у діяльності ШІ. 4. Наділити авторськими (патентними) правами фізичну особу, яка створювала ШІ або набувала його для створення творів (винаходів). 5. Створити неіснуючого автора і наділити його правами на створений твір [8, 182]. При цьому ми дотримуємося точки зору

щодо передачі таких прав власникові або творцеві ШІ.

Кримінальне застосування ШІ. У дослідженні, опублікованому нещодавно в журналі Crime Science і фінансованому Dawes Centerfor Future Crimeat UCL, визначено 20 способів використання ШІ для сприяння злочинності протягом наступних 15 років [13, 14]. Вони були проранжовані в порядку їх небезпеки — залежно від шкоди, яку можуть заподіяти, потенційної вигоди або вигоди злочинним шляхом, того, наскільки легко їх буде виконати і наскільки складно їх буде зупинити.

Автори дослідження заявили, що фальшивий контент буде складно виявити і зупинити і що він може переслідувати найрізноманітніші цілі: від дискредитації громадського діяча до вилучення грошових коштів особи шляхом видачі себе за сина або дочку подружжя під час відеодзвінка. На їхню думку, такий контент може викликати повсюдну недовіру до аудіо- і візуальних свідчень, що завдасть шкоди суспільству.

Окрім фальшивого контенту, п'ять інших злочинів з використанням ШІ були визнані такими, що викликають серйозне занепокоєння. Вони використовують безпілотні автомобілі в якості зброї, допомагають створювати більш спеціалізовані фішингові повідомлення (цільовий фішинг), порушують роботу систем, керованих ШІ, збирають онлайн-інформацію для цілей великомасштабного шантажу і створюють підготовлені ШІ фальшиві новини.

Старший автор, професор Льюїс Гріффін (Lewis Griffin) (UCL Computer Science) зазначив: *«У міру розширення можливостей технологій на основі ШІ зростає і їх потенціал для злочинної експлуатації. Щоб належним чином підготуватися до можливих загроз штучного інтелекту, нам необхідно визначити, якими можуть бути ці загрози і як вони можуть вплинути на наше життя».*

Дослідники відібрали 20 злочинів з використанням ШІ з наукових статей, новин і поточних подій, а також з художньої літератури та популярної культури. Потім вони вибрали 31 фахівця, що мають досвід у галузі ШІ, для дводенних обговорень, щоб оцінити серйозність потенційних злочинів. Експертами виступили представники академічних кіл, приватного сектору, поліції, уряду та органів державної безпеки.

Злочини середнього ступеня тяжкості включали продаж товарів і послуг обманним шляхом, помічених як «ШІ», таких як перевірка безпеки і таргетована реклама. Цього було б легко досягти з потенційно великим прибутком.

До злочинів, що не викликають особливого занепокоєння, віднесли ботів-грабіжників — маленьких роботів, які використовуються для проникнення у власність через точки доступу, такі як поштові скриньки або відкидні дверцята для кішок, нескладні для проникнення, з наступним переслідуванням за допомогою ШІ, яке хоча й надзвичайно небезпечне для людей, однак не може працювати у великих масштабах.

Доктор Метью Колдуелл (Matthew Caldwell) (UCL Computer Science) зазначив: *«Люди тепер проводять більшу частину свого життя в мережі, і їх діяльність в мережі може створювати і руйнувати репутацію. Таке онлайн-середовище, в якому дані є власністю і владою інформації, є ідеальним для використання у злочинній діяльності на основі ШІ». «На відміну від багатьох традиційних злочинів, злочини в цифровій сфері можна легко поширювати, повторювати і навіть продавати, що дозволяє продавати злочинні методи і надавати злочини в якості послуги. Це означає, що злочинці можуть віддати на аутсорсинг більш складні аспекти своєї злочинної діяльності з використанням ШІ».*

Професор Шейн Джонсон (Shane Johnson), директор Центру майбутніх злочинів Дауеса при UCL, який фінансував дослідження, підкреслив: *«Ми жи-*

вемо в постійно мінливому світі, який створює нові можливості — хороші і погані. Таким чином, вкрай важливо, щоб ми передбачали майбутні загрози злочинності, щоб політики та інші зацікавлені сторони, які мають компетенцією діяти, могли зробити це до того, як відбудеться новий «урожай злочинності». Цей звіт є першим із серії, у якій будуть визначені майбутні загрози злочинності, пов'язані з новими технологіями, і те, що ми можемо з ними зробити.

Розглянемо загрози злочинності із застосуванням ШІ більш докладно.

Високий рівень небезпеки. *Аудіо- та відеоуособлення.* Люди мають стійку тенденцію вірити своїм очам і вухам, тому аудіо та відео зі свідченнями традиційно приділяється велика увага (часто і юридична сила), незважаючи на довгу історію фотографічних прийомів. Однак нещодавні розробки у сфері глибокого навчання, зокрема з використанням GAN, значно розширили можливості для створення підробленого контенту. Уже можна сфабрикувати переконливе уособлення цілей за фіксованим сценарієм і очікується, що за цим виникнуть інтерактивні уособлення. Експерти передбачили широкий спектр кримінальних додатків для такої технології *deepfake*, щоб використовувати приховану довіру людей до цих засобів масової інформації, включаючи видачу себе за дітей старих батьків за допомогою відеодзвінків для отримання доступу до засобів; використання по телефону для запиту доступу до захищених систем; фальшиві відео публічних діячів, які говорять або здійснюють негідні дії з метою маніпулювання підтримкою. Можливості, пропоновані *deepfake*, безмежні. Автори дослідження вказали, що можна було б створювати відеоролики і зображення провідних політиків, які погано поводяться, щоб знизити їх суспільну підтримку або поліпшити аферу з «внучкою», у якій шахраї можуть створити силует коханої людини і переконати літню людину переказати їм гроші. Усе ще, на думку дослідників, у найближчі роки стане невід'ємною частиною світу електронної злочинності. ЗМІ вже писали про можливості технології deepfake в контексті китайського додатка ZAO. Користувач Twitter Аллан Ся опублікував цікаву демонстрацію можливостей цього додатка. У 30-секундному кліпі обличчя Леонардо Дікапріо в знаменіті моменти з декількох його фільмів було замінено зображенням Ся. Інтернет-користувач повідомляє, що кліпи були створені менш ніж за вісім секунд з однієї фотографії. Однак додаток може попросити користувача зробити серію фотографій, наприклад, із закритими і відкритими очима або ротом, щоб отримати більш реалістичні результати. За словами Аллана Ся, додаток пропонує лише обмежену кількість кліпів, у які ви можете вставити своє обличчя. Творець програми «навчився» своїм алгоритмам роботи з кожним з цих кліпів, і змінити зображення в будь-якому фільмі неможливо [15].

Відтворення аудіо/відео за іншу особу було визнано найбільш небезпечним видом злочинів з усіх розглянутих. Наслідки вважалися серйозними: дослідники продемонстрували певні успіхи в алгоритмічному виявленні видачі себе за іншу особу, однак це може виявитися неможливим у довгостроковій перспективі. Існує дуже багато неконтрольованих маршрутів, за якими може поширюватися підроблений матеріал, тому зміни в поведінці громадян можуть бути єдиним ефективним захистом. Ці поведінкові зрушення, зокрема недовіра до візуальних свідчень, можна розглядати як непряму цивільну шкоду, заподіяну злочином, на додаток до прямої шкоди, такої як шахрайство або шкода репутації. Якщо виявиться, що навіть невелика частина візуальних доказів є переконливою підробкою, то вдасться набагато легше дискредитувати справжні докази, що підривають кримінальне розслідуван-

ня та довіру до політичних і соціальних інститутів, які покладаються на достовірні повідомлення. Подібні тенденції вже проявляються в дискурсі навколо «фейкових новин». Прибуток було оцінено як найменш високий параметр для цього злочину не тому, що необхідні інвестиції є зависокими, а тому, що злочини, пов'язані з видачею себе за іншу особу, з метою придбання, імовірно, буде найпростіше здійснити проти окремих осіб, а не організацій.

Безпілотні автомобілі як зброя. Автомобілі давно використовуються і як засіб доправлення вибухових речовин, і як власне кінетична зброя терору, причому остання стає все більш поширеною. Транспортні засоби в більшості країн набагато доступніші, ніж вогнепальна зброя і вибухові речовини, і автомобільні атаки можуть бути здійснені з відносно невеликими організаційними витратами фрагментарними, квазіавтономними терористами, терористами-одинаками або такими, що заявляють про свою приналежність до ІДІЛ. Ця тактика стала особливо популярною після серії атак у західних містах, включаючи Ніццу (2016), Берлін (2016), Лондон (2017), Барселону (2017) і Нью-Йорк (2017). Хоча повністю автономні безпілотні автомобілі з керуванням від ШІ ще не доступні, численні виробники автомобілів і технологічні компанії прагнуть їх створювати, а деякі дозволені для випробувань на дорогах загального користування. Уже задіяні більш обмежені можливості автономного водіння, зокрема допоміжна парковка та управління смугою руху. Автономні транспортні засоби потенційно дали б змогу розширити тероризм на транспортних засобах, зменшивши потребу в наймі водіїв, дозволивши окремим зловмисникам здійснювати кілька атак, навіть координуючи одночасно велику кількість транспортних засобів. Безпілотні автомобілі обов'язково міститимуть великі системи безпеки, які необхідно буде ігнорувати, тому атаки без водія матимуть вищий бар'єр для проникнення, аніж нині, що потребує технологічних навичок і організації.

Індивідуальний фішинг. Фішинг — це атака «соціальної інженерії», метою якої є збір захищеної інформації або встановлення зловмисного програмного забезпечення за допомогою цифрового повідомлення, яке нібито відправлено довіреною особою, наприклад банком користувача. Зловмисник використовує існуючу довіру, щоб переконати користувача виконати дії, яких він в іншому випадку міг би боятися, наприклад, розкриття паролів або перехід за сумнівними посиланнями. Хоча деякі атаки можуть бути націлені на конкретних людей, що називається «цільовим фішингом», це не є дуже масштабованим. Нині більшість фішингових атак мають відносно невибірковий характер, з використанням загальних повідомлень, стилізованих під основні бренди або тематичні події, що, як очікується, можуть зацікавити деяку частину користувачів чисто випадково. Зловмисник покладається на простоту відправлення величезної кількості цифрових повідомлень, щоб перетворити низьку швидкість відповіді на прибуток. Штучний інтелект може підвищити ймовірність успіху фішингових атак, створюючи повідомлення, які здаються більш справжніми, наприклад шляхом включення інформації, отриманої з соціальних мереж або шляхом імітації стилю довіреної сторони. Замість того щоб надсилати однакові повідомлення по всіх цілях, які здебільшого можуть не спрацювати, повідомлення можна було б адаптувати для використання конкретних вразливостей, передбачуваних для кожної людини, ефективно автоматизуючи підхід цільового фішингу. Окрім того, методи ШІ можуть використовувати активне навчання, щоб виявити, «що працює», змінюючи деталі повідомлень для збору даних про те, як максимізувати відповіді. Оскільки злочинна мета фішингових атак найчастіше має фінан-

совий характер, злочин було оцінено як такий, що лише незначно перевищує середній потенціал шкоди, проте було оцінено високо з точки зору прибутку, досяжності та вразливості, тобто його буде важко зупинити.

Порушення систем, керованих ШІ. У міру того як використання ШІ в уряді, бізнесі та вдома збільшується, а ролі, виконувані системами ШІ, стають усе більш важливими, можливості для атак будуть зростати. Системи, засновані на навчанні, часто розгортаються для підвищення ефективності та зручності, а не для забезпечення надійності, і їх не можна апріорі визнати критично важливою інфраструктурою. Експерти могли передбачити безліч кримінальних і терористичних сценаріїв, що виникають унаслідок цілеспрямованого порушення роботи таких систем, викликаючи масові перебої в електропостачанні, тупиковий рух і порушення логістики продовольства. Системи, що відповідають за будь-які аспекти громадської безпеки, імовірно, стануть ключовими цілями, як і ті, що контролюють фінансові операції. Відповідно, були високі рейтинги прибутку і збитків, як і ураженість. У цілому, чим складнішою є система управління, тим важче повністю захиститися. Явище ворожих збурень підкреслює цю проблему, припускаючи, що досить просунуті ШІ можуть бути вразливі для ретельно продуманих атак. Однак досяжність була оцінена нижче на тій підставі, що такі атаки зазвичай потребують докладних знань про задіяні системи або навіть доступу до них, що може бути складно отримати.

Масштабний шантаж. Традиційний шантаж має на меті вимагання під загрозою розкриття доказів вчинення злочину, або правопорушення, або сумнівної особистої інформації. Обмежуючим фактором традиційного шантажу є отримання таких доказів: злочин має сенс тільки в тому разі, якщо жертва заплатить за приховування доказів більше, ніж коштує їх придбання. ШІ може бути використаний для цього в набагато ширшому масштабі, збираючи інформацію (яка сама по собі не повинна бути переконливим доказом) із соціальних мереж або великих особистих наборів даних, таких як журнали електронної пошти, історія браузера, вміст жорсткого диска або телефону, а потім виявляти конкретні вразливості для великої кількості потенційних цілей і адаптація повідомлень про загрози для кожної. ШІ також може бути використаний для створення фальшивих доказів, наприклад, коли виявлена інформація передбачає вразливість без надання доказів primafacie. Великомасштабний шантаж був високо оцінений з точки зору прибутку: як і в разі з фішингом, ефект масштабу означає, що для отримання прибутку атака може зажадати лише невеликої кількості влучань. Перемога вважалася важкою в основному з тієї ж причини, через яку вона є проблематичною в традиційних випадках: небажання жертви вийти вперед і зіткнутися з уразливістю. Однак збиток був оцінений як середній, оскільки злочин за своєю природою в першу чергу спрямовано проти окремих осіб, а досяжність також відносно низька через високі вимоги до даних та комбінації декількох різних методів ШІ, які необхідно координувати. Варто зазначити, що серед сучасних методів фішингу поширений дуже грубий аналог шантажу, не пов'язаний з використанням ШІ. Термін «сексторція» включає неправдиву заяву про компрометуючий відеозапис зі зламаного комп'ютера або телефону користувача. Як і у випадку з усіма подібними шахрайствами, неможливо дізнатися відсоток влучань, однак експерти вважають, що він досить низький.

Фейкові новини, створені ШІ. Фальшиві новини — це пропаганда, метою якої є завоювання довіри, оскільки вони виходять або здаються такими, що виходять, з надійного джерела. Окрім надання неправдивої інформації, фейкові новини в достатній мірі

можуть відвернути увагу від достовірної інформації. Експерти розглянули можливість створення фальшивого новинного контенту за допомогою технології ШІ для досягнення більшої ефективності, присутності або специфічності. ШІ можна використовувати для створення безлічі версій певного контенту, очевидно, з багатьох джерел, щоб підвищити його видимість і довіру; і вибирати контент або його подання на індивідуальній основі, щоб посилити вплив. Злочин отримав оцінку вище середнього за збитком, досяжністю і вразливістю та нижче середнього за прибутком. Шкода вважалася високою через значний потенціал впливати на певні політичні події, наприклад, на голосування (незалежно від того, було це вже зроблено чи ні); і через дифузні соціальні наслідки, якщо передача реальних новин підривається або витісняється фальшивими ЗМІ. На сьогодні найбільш успішні спроби боротьби з фейковими новинами відбуваються за допомогою освіти, особливо у Фінляндії. Більш низький показник прибутку відображає складність його отримання від фальшивих новин, хоча є можливості для використання фейкових новин у маніпулюванні ринком.

Середній рівень небезпеки

Військові роботи. Як і в багатьох галузях технологічного розвитку, військові серйозніше зацікавлені в дослідженнях робототехніки з потенційно дуже різними цілями, ніж цивільні користувачі, незважаючи на велику кількість методологічних збігів. Можна очікувати, що будь-яка доступність військової техніки, наприклад, вогнепальної зброї або вибухових речовин, для злочинних чи терористичних організацій буде становити серйозну загрозу, і це, безумовно, стосується й автономних роботів, призначених для бойових дій або оборонного розгортання. Експерти оцінили такий доступ як дуже шкідливий та вигідний. Однак було також визнано, що рейтинги обов'язково були спекулятивними. Військові можливості зазвичай зберігаються в секреті, і у дослідників дуже обмежені відомості про поточний стан справ і темпи їх просування.

Зміїна олія (Snakeoil). Продаж шахрайських послуг під виглядом ШІ або використання димової завіси з жаргону машинного навчання. Таке шахрайство надзвичайно досяжне і практично не має технічних барєрів, оскільки технологія за визначенням не працює. Потенційний прибуток високий: є безліч сумнозвісних історичних прикладів того, як шахраї продають дорогі технологічні підробки великим організаціям, включаючи національні уряди і збройні сили. Можливо, це невикористання ШІ для вчинення злочинів, однак злочин залежить від того, чи вірить ціль у заявлені можливості ШІ, що, у свою чергу, залежить від того, чи буде ШІ сприйматися громадськістю як успішний. Це повинно бути потенційно легко подолано за допомогою навчання і належної обачності, хоча нині можливість є відкритою, поки ці заходи не будуть вжиті.

Отруєння даних. Маніпуляції з даними навчання машинного навчання з метою навмисного введення певних упереджень, або як самоціль (з метою завдати шкоди комерційним конкурентам, спотворити політичний дискурс або викликати недовіру в суспільстві), або з наміром подальшої експлуатації. Наприклад, зробити автоматичний рентгенівський детектор загроз нечутливим до зброї, яку потрібно пронести контрабандою на борт літака, або спонукати консультанта з інвестицій дати несподівані рекомендації, які змінять ринкову вартість таким чином, щоб у вас були попередні знання, які ви можете використовувати. Чим ширше використовується джерело даних і чим більше йому довіряють, тим небезпечнішим воно може бути. Хоча це потенційно шкідливо і прибутково, рівень небезпеки вказаного злочину було оцінено як низький за ступенем досяжності, оскільки надійні дже-

рела даних, як правило, важко змінити і, як наслідок їх широкого використання, піддаються частим перевіркам.

Кібератаки на основі навчання. Існуючі кібератаки, як правило, або витончені й адаптовані до конкретної мети, або грубі, однак значною мірою автоматизовані, засновані на величезній кількості цифр, наприклад, розподілені атаки відмови в обслуговуванні, сканування портів. Штучний інтелект підвищує ймовірність атак, що є як конкретними, так і масовими, використовуючи, наприклад, підходи від навчання з підкріпленням для паралельного дослідження слабких місць багатьох систем перед одночасним запуском декількох атак. Такі атаки вважалися шкідливими і прибутковими, хоча експерти були менш упевнені в їх досяжності.

Автономні атакуючі дрони. Неавтономні радіокеровані дрони вже використовуються для здійснення злочинів, зокрема контрабанда наркотиків у тюрми, а також відповідальні за серйозні порушення транспорту. Автономні дрони під управлінням ШІ на борту потенційно забезпечують більшу координацію і складність атак, звільняючи зловмисника від необхідності перебувати в межах досяжності передавача безпілотника, що ускладнює нейтралізацію та затримання. На сьогодні дрони зазвичай не використовуються для вчинення насильницьких злочинів, однак їхня маса і кінетична енергія потенційно небезпечні при правильному націлюванні (наприклад, у двигуни літаків), і вони також можуть бути оснащені озброєнням. Дрони можуть бути особливо небезпечними, якщо діють масово в самоорганізованих роях. Вони отримали високу оцінку потенційної шкоди, проте низьку ураженість, оскільки в багатьох контекстах захист може бути забезпечено за допомогою фізичних бар'єрів.

Розробки ШІ в перегонах озброєнь досягли такого рівня ефективності, що відома міжнародна неурядова організація Amnesty International уже почала вимагати від урядів усіх країн заборони розробки роботів-убивць, які базуються на нових технологіях. За даними Bureauof Investigative Journalism («Бюро журналістських розслідувань»), унаслідок використання безпілотників у період між 2004 та 2013 роками було вбито від 2500 до 3500 осіб, у тому числі мирних жителів і дітей, і більш ніж тисячі завдано поранення. Інтенсивне застосування безпілотників (війна дронів) призвело до людських жертв у 2020 році в зоні конфлікту в Нагірному Карабасі.

Онлайн-виселення. Приймати онлайн-активності в сучасному житті, у сфері фінансів, зайнятості, соціальної активності та громадянства, являє собою нову мету для атак на людину: відмова в доступі до того, що стало найважливішими послугами, є потенційно виснажливою. Це може бути використано як загроза вимагання, щоб завдати шкоди або позбавити права груп користувачів, викликати хаос. Деякі фішингові та кібератаки здійснюють щось подібне за допомогою «програм-вимагачів», а квазіорганізовані групи людей іноді беруть участь у таких діях як масове неправдиве повідомлення про зловживання в соціальних мережах. Водночас ШІ може допускати й більш тонкі, обережні атаки: адаптація підробленої діяльності до порушення умов обслуговування, визначення конкретних вразливостей для кожної — і більш масштабовані.

Обман розпізнавання облич. Системи ШІ, які виконують розпізнавання облич, усе частіше використовуються для підтвердження особи на таких пристроях, як смартфони, а також проходять тестування поліцією і службами безпеки для завдань відстеження підозрюваних у громадських місцях і прискорення перевірки пасажирів на міжнародних кордонах. Ці системи можуть стати привабливою мішенню для злочинців. Були продемонстровані деякі успішні атаки, у тому числі «морфінг» (morphing) атаки, які дають змогу одно-

му фотографічному посвідченню особи, наприклад паспорту, передаватися (і використовуватися) кількома людьми. Прибуток і шкода вважалися нижчими середньої, оскільки атаки, швидше за все, дають можливість здійснити відносно дрібні злочини.

Вибух ринку. Маніпулювання фінансовими або фондовими ринками за допомогою цільових, імовірно, часто повторюваних моделей угод з метою завдати шкоди конкурентам, валютами або економічній системі в цілому (а не безпосередньо для отримання прибутку від торгівлі, хоча це також може бути побічним ефектом), обговорювалося. Ідея є посиленою ШІ версією вигаданої змови Холстомера про холодну війну, яка передбачала спробу Росії спровокувати фінансовий крах, раптово продавши величезні запаси американської валюти через підставні компанії. Навчання з підкріпленням було запропоновано як метод виявлення ефективних торгових стратегій, можливо, у поєднанні з аналізом медіа на основі НЛП і створенням підробленого контенту. Досяжність була оцінена як низька через крайню складність точного моделювання поведінки ринку і дуже високу вартість входу для участі у великомасштабній торгівлі, однак потенційна шкода і прибуток були відповідно високими.

Низький рівень небезпеки

Використання зміщення, тобто виявлення і використання засвоєних (існуючих) упереджень у широко використовуваних або впливових алгоритмах. Наприклад, ігрові рекомендації YouTube для направлення глядачів до пропаганди або рейтинги Google для підвищення впізнаваності продуктів або дискредитації конкурентів. Така поведінка вже широко поширена, часто не є незаконною, хоча вона може суперечити умовам обслуговування провайдера, і навіть у формі пошукової оптимізації або SEO розглядається як законна, хоча й сумнівна, бізнес-модель в Інтернеті. Швидше за все, за допомогою ШІ цю модель буде легше використовувати та протидіяти їй.

Боти-зломщики. Невеликі автономні роботи, які можуть бути доставлені в приміщення через непримітні точки доступу, зокрема поштові скриньки, відкидні дверцята для кішок, для вилучення ключів або відкриття дверей, що дають змогу проникнути грабіжникам-людям. Технічні вимоги дуже обмежені, що має зробити їх більш доступними, ніж більш амбітні класи автономних роботів. Однак шкода і прибуток невеликі, оскільки вони дають можливість здійснювати дуже локальні дрібні злочини.

Ухилення від виявлення ШІ. Очікується, що поліцейська служба і безпека будуть усе більше покладатися на сортування й автоматизацію на основі ШІ для обробки постійно зростаючих обсягів даних, що збираються в ході розслідувань. Атаки, які підривають такі процеси, щоб видалити докази або іншим чином перешкодити викриттю, стають усе більш привабливими для злочинців. Змагальність обурення (наприклад, використовувані для приховування порнографічних матеріалів від автоматичного виявлення) пропонує один можливий шлях до цього, хоча вимоги до знань системи можуть бути непомірно високими. Шкода і прибуток були оцінені як низькі частково тому, що природа і контекст «злочину» недостатньо визначені, а експерти були переконані, що вони досяжні. Однак якби це було досягнуто, ураженість була б оцінена як важка, оскільки злочин за визначенням зводиться до того, щоб зійти з рук.

Підроблені огляди, створені ШІ. Ідеться про автоматичне створення контенту для таких сайтів, як Amazon чи Trip Advisor, щоб створити помилкове враження про продукт або послугу і спонукати клієнтів перейти або до них, або від них. Такі підробки вже здійснюються людськими агентами. ШІ може підвищити ефективність, однак прибу-

ток і збитки від подібних окремих кампаній, імовірно, залишаться невеликими і локальними.

Переслідування за допомогою ШІ. Основа злочину — використання навчальних систем для відстежування місцеперебування (геолокації) й активності людини через соціальні мережі або дані особистих пристроїв. Вважається також, що він охоплює інші злочини, пов'язані з примусом, домашнім насиллям, газлайтингом тощо, і належить до поточних новин, що стосуються співучасті західних технологічних компаній в наданні додатків для забезпечення дотримання соціальних норм у репресивних суспільствах. Шкоду було оцінено як низьку не тому, що ці злочини не є надзвичайно руйнівними, а тому, що вони спочатку націлені на окремих осіб і не мають значних можливостей для масштабних дій.

Підробка. Створення підробленого контенту, наприклад творів мистецтва або музики, який може продаватися під хибним приводом щодо його авторства було оцінено як найменш небезпечна загроза з усіх розглянутих, як з точки зору шкоди, так і ймовірності успіху. Можливості ШІ тут залишаються строго обмеженими: хоча був досягнутий певний успіх у створенні цифрових зображень, які в цілому імітують візуальний стиль великих митців, це дуже відрізняється від створення реальних фізичних об'єктів, які пройшли б перевірку в галереї або аукціонному домі. Світ мистецтва століттями стикався з підробками і має великі, якщо не завжди достатні, методи захисту. ШІ навіть не намагається усунути більшість із цих перешкод.

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 (датазвернення: 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