ПИТАННЯ ТЕОРІЇ

УДК 347.77:004.8:355.488
DOI https://doi.org/10.32782/chc.v055.2024.1

Харитонова Олена Іванівна,
докторка юридичних наук, професорка,
завідувач кафедри інтелектуальної власності та патентної юстиції
Національного університету «Одеська юридична академія»,
член-кореспондент НАПрН України
ORCID ID: 0000-0002-9681-9605

Харитонов Євген Олегович,
доктор юридичних наук, професор,
завідувач кафедри цивільного права
Національного університету «Одеська юридична академія»,
член-кореспондент НАПрН України
ORCID ID: 0000-0001-5521-0839

ШТУЧНИЙ ІНТЕЛЕКТ У ГІБРИДНІЙ ВІЙНІ: ПРАВОВІ ПРОБЛЕМИ

«Віртуалізація» суспільства супроводжується зростанням значення кіберзброї та штучного інтелекту в гібридній війні.

Зокрема, це зумовлюється тим, що кіберзброя потенційно є не тільки руйнівною (та оборонною) потугою у традиційній («мілітарній») війні, а й потужним засобом політичного та психологічного тиску. Генерал Джеймс Картрайт, який у 2004 році очолив Стратегічне командування США в Омасі (котре відповідає за ядерний арсенал держави), пропонував використати її для «перезапуску дипломатії»: щоб змусити іншу країну усвідомити, що в неї немає іншого вибору, окрім як погодитися на переговори» [1, с. 44]. Найяскравішим прикладом є масштабна кібератака російських хакерів, здійснена 19 грудня 2024 року на державні реєстри України. Під атакою опинились ресурси Міністерства юстиції України. Внаслідок кібератаки були призупинена робота низки держреєстрів, а також деякі послуги у застосунку Дія. Встановлено, що напад був організований російськими хакерами з метою порушення функціонування ключових державних сервісів [2].

Характеризуючи кібервійну, Девід Е. Сенгер зазначав: «...хотілось би думати, наче кібервійна якось відрізняється від інших конфліктів, наче вона розгортається собі десь у хмарах окремо від того, що відбувається на землі. Коли держави створювали військово-повітряні сили, то міркували так само: повітряні бої – це одне, а перестрілка в окопах – інше. Аж під час Другої світової війни утвердилася концепція «єдиного бойового простору», що охоплює повітря, землю та море. У деяких країнах світу до цього вже додають і кіберпростір. Просто це важче помітити» [1, с. 227].

Наразі кібервійна стає «буденним» явищем, котре, до того ж, усе активніше охоплює/ включає й штучний інтелект. Разом із тим, це «буденне» явище є недостатньо осмисленим концептуально і регламентованим юридично.

Цим зумовлюється необхідність спеціального дослідження проблем, які тут виникають, та пошуку шляхів їх подолання.

Стан дослідження проблеми. Правові питання створення та використання штучного інтелекту останнє десятиліття досить активно розглядаються правознавцями [3, 4, 5, 6, 7, 8].

Однак проблемам використання його у якості кіберзброї та захисту від останньої уваги приділялося набагато менше. Ці питання досліджували Сенгер, Девід Е., [1] Костенко О., Джейнс Т., Журавльов Д., Дніпров О., Усенко Ю. [9], Дарина Бойко, Іван Городиський [10] та ін.

Окремі питання інформаційної гібридної війни ми також розглядали у 2016–2018 рр. [11, 12, 13, 14, 15, 16], але відтоді багато що змінилося, зокрема, у зв'язку з активним використанням штучного інтелекту.

Кібервійна та супутні терміно-поняття

«Інформаційна війна» є родовим поняття щодо усіх інших видів протиборства у інформаційній

сфері – як традиційних – таких, що мають тисячолітню історію, так і сучасних – які відбуваються у кіберпросторі тощо).

Констатуючи багатозначність поняття «інформаційна війна», обмежимось тут згадкою лише про розуміння її як форми протиборства між суб'єктами ... що передбачає інформаційний вплив на населення з використанням ЗМІ, комп'ютерних мереж тощо з метою формування відповідної суспільної думки, підриву морального духу як усього суспільства, так і окремих його інституцій [17, с. 140-141].

Враховуючи, що кібервійна є різновидом інформаційної війни у кіберпросторі [17, с. 189], а кіберзброя розуміється як різновид інформаційної зброї, головними елементами якої є інформація та інформаційні технології, способи і засоби інформаційного впливу й захисту від нього, призначені для ведення інформаційної боротьби у кіберпросторі [17, с. 190], надалі у процесі нашого дослідження будемо також використовувати такі поняття як «кіберпростір» та «кіберзахист».

При цьому «кіберпростір» має кілька значень: 1. Електроне інформаційне середовище, утворене організованою сукупністю взаємопоєднаних за єдиними принципами та правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем. 2. Середовище існування та розповсюдження інформації, створюване кіберінфраструктурою. 3. Середовище, створюване інформаційними системами, об'єднаними у локальні або глобальні комп'ютерні мережі або реалізованими на окремих комп'ютерах та інших пристроях. 4. Уявне середовище, в якому за допомогою комп'ютерних мереж циркулює цифрова інформація [17, с. 191].

«Кіберзахист» розуміється у двох значеннях: 1. Сукупність методів і заходів організаційного, нормативно-правового та технічного характеру, спрямованих на забезпечення кібербезпеки. 2. Реалізація у кіберпросторі комплексу організаційних, нормативно-правових, технічних та інших заходів для запобігання кібератакам та забезпечення кібербезпеки, котра розуміється як «стан захищеності кіберпростору від кібератак, за якого забезпечується його сталий розвиток, а також своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз функціонуванню його елементів» [17, с. 189-190].

Усі згадані поняття пов'язані з концептом «кіберпростір», котрий виступає і тлом, і кваліфікуючою ознакою кібервійни.

Кіберзброя. Штучний інтелект як кіберзброя

Значення кіберзброї у сучасному світі та сучасній війні яскраво охарактеризував Девід Е. Сенгер, згадавши побоювання Пентагону, що кібератаки становлять особливу загрозу, до протидії якій Штати зовсім не готувалися. І додає: «Іронія в тому, що США залишаються засекреченою і наймогутнішою кібердержавою світу... Однак розрив між державами скорочується. Створити кіберзброю настільки дешево, а приховати так легко, що спокуса стає непереборною» [1, с. 8].

(У зв'язку з цим варто згадати, що Мирослав Попович ще у 2010 році у передмові до книги Володимира Горбуліна «Без права на покаяння» наголошував на тому, що: «майбутні конфлікти потребують насамперед високоточної зброї й розвиненої системи інформаційних технологій» [18, с. 5]).

Спираючись на обґрунтоване твердження Девіда Сенгера, що «кіберконфлікти залишаються в сірій зоні між війною та миром» [1, с. 12], зауважимо, що це відповідає нашому баченню цього сегменту сучасної гібридної війни. При цьому, коли «десять років тому лише три-чотири країни володіли ефективною кіберзброєю, то зараз таких уже понад тридцять. Крива обсягу виробництва кіберзброї за останні десять років загалом нагадує траєкторію злету бойового літака. Нову зброю вже застосовували багато разів, навіть якщо результати були неоднозначні...

Як і напередодні Першої світової війни, держави, немов зазирнувши у майбутнє, почали швидко озброюватися. США були одними з перших – створили так звані «Сили кібероперацій» ... Сучасні збройні сили будь-якої країни не можуть функціонувати без кіберарсеналу так само, як після 1918 року годі було уявити військо без літаків. Сьогодні, як і тоді, неможливо передбачити, наскільки цей винахід змінить застосування державних сил» [1, с. 19].

Він зазначає: «Ми всі живемо в страху, що нашу залежність від цифрових технологій обернуть проти нас інші держави, які за останнє десятиліття знайшли нові способи продовжити давнє протистояння. Ми вже знаємо, що перед кіберзброєю, як і перед ядерною, усі рівні. І в нас є всі підстави непокоїтися, що через кілька років <u>ця зброя вкупі зі штучним інтелектом</u> (Підкреслено нами – Є. Х., О.Х.) діятиме настільки швидко, що люди не встигнуть ні усвідомити загрози, ні запобігти їй – тож атаки відбудуться і призведуть до ескалації конфлікту» [1, с. 21].

Отже зафіксуємо цю обставину, що зумовлює вищий ступінь загрози – такий, що може вийти з-під влади людини: <u>поєднання кіберзброї зі штучним інтелектом.</u> Цей випадок є головною

гібридною загрозою, а відтак потребує адекватної /гібридної відповіді, зокрема, за допомогою юридичних заходів.

При цьому зауважимо, що коли створення чи удосконалення кіберзброї вже за визначенням є справою непублічною, а регламентація відносин, пов'язаних з нею, є таємницею, то розробка штучного інтелекту сама по собі виглядає заняттям більш мирним, а досягнення часто стають матеріалом для обговорення у ЗМІ (хоча й переважно у публіцистично-популярній формі).

Разом із тим штучний інтелект може застосовуватися як кіберзброя (або – як елемент кіберзброї) не лише у інформаційній гібридній війні, але й у «мілітарній» гібридній війні (скажімо, для приховування інформації, важливої для розслідування воєнних злочинів або для викрадення інформації щодо планування воєнних дій, логістики тощо).

Зокрема, як з'ясувала ВВС, докази потенційних порушень прав людини можуть бути втрачені внаслідок їхнього видалення соцмережами, котрі за допомогою штучного інтелекту видаляють зі своїх платформ відео, що містять сцени насильства. Meta і YouTube кажуть, що у такий спосіб прагнуть захистити користувачів від шкідливого контенту.

Штучний інтелект запрограмований автоматично видаляти шкідливий і насильницький контент. Утім, коли справа доходить до модерації відео з країн, де триває війна, машина просто не може визначити, чи ці кадри – доказ порушення прав людини. «Штучний інтелект програмували так, щоби у момент, коли машина бачить щось, що здається важким або травматичним, одразу прибирати це», – пояснює Расбріджер ВВС. Раду Meta, до якої він входить, створив Марк Цукерберг. Це своєрідний незалежний «верховний суд» компанії, якій належать Facebook й Instagram.

Коли Ігор Захаренко, який від початку повномасштабної війни документує вбивства росіянами цивільних, хотів викласти відео в інтернет, щоби світ дізнався, що відбувається в Україні, фейсбук та інстаграм, їх швидко видалили. Використовуючи фіктивні акаунти, ВВС теж виклали кадри Ігоря в інстаграм і ютюб. Протягом хвилини інстаграм видалив три з чотирьох відео. YouTube спочатку застосував вікові обмеження до трьох відео, але за десять хвилин прибрав їх усі. Клопотання відновити відео на тій підставі, що вони містили докази воєнних злочинів, YouTube відхилив, попри запевнення компанії YouTube, що чутливий контент може залишатися в мережі, якщо він становить суспільний інтерес. Тобто експеримент ВВС з відео Ігоря свідчить про протилежне.

Журналісти ВВС з'ясували, що некомерційна організація Mnemonic, що базується в Берліні і займається документуванням порушень прав людини, розробила програму для автоматичного завантаження й збереження доказів потенційних воєнних злочинів. Спочатку вони це робили для Сирії, а тепер – для Ємену, Судану та України. Було збережено понад 700 тисяч відео із зон бойових дій, перш ніж їх видалили із соціальних мереж. Проте організаціям на кшталт Mnemonic бракує ресурсів. Тому архівування матеріалів з соцмереж часто лягає на плечі простих людей чи волонтерів, що ускладнює можливе притягнення до відповідальності за воєнні злочини у майбутньому [19].

Разом із тим, штучний інтелект може не лише видаляти інформацію, а й створювати її, викривлюючи сутність подій або створюючи події, яких не було [20], чим ще більше посилюється загроза його «некоректної» участі у «мілітарній» війні.

Штучний інтелект у «мілітарній війні»: колізія цілей оборони та та атаки/нападу

Використання штучного інтелекту у «воєнній війні» ускладнюється, крім усього іншого, існуванням колізії публічних та приватних інтересів, вирішення якої потребує і у цьому разі «гібридного» юридичного забезпечення.

Хоча ми вже торкались загальних проблем такої колізії у більш ранніх наших працях, але маємо тут ще раз звернутися до цієї проблематики, аби визначити особливі вимоги до вирішення проблеми загроз «участі»/ використання штучного інтелекту у гібридній війні.

Спеціально аналізу проблем у цій сфері присвячений матеріал Дарини Бойко та Івана Городиського з Центру Дністрянського «Штучний інтелект у сфері оборони: виклики регулювання», підготовлений у січні 2024 року за підтримки Європейського Союзу та Міжнародного фонду «Відродження» у рамках спільної ініціативи «Європейське Відродження України» [10]. На їхню думку, головною проблемою у цій сфері є використання Україною технологій штучного інтелекту для розпізнавання осіб за допомогою зображень з соціальних мереж та інтернету [21], автоматизованого аналізу даних з використанням технології обробки природної мови тощо, розроблених відомими іноземними компаніями, які раніше зазнавали критики через «безпекові і праволюдинні моменти». Попри те, що застосування згаданих технологій штучного інтелекту дає очевидні пози-

тивні результати в ході збройного протистояння з Росією, вагомим викликом для їх використання в Україні, вважається проблема забезпечення захисту прав людини [10].

Назагал йдеться про те, що застосування технологій штучного інтелекту (навіть у суто воєнних цілях) викликало занепокоєння серед міжнародних організацій, на кшталт OpenDemocracy, котрі у березні 2022 року (тобто у то час, коли доля України висіла на волосині), хвилювалася, що українські військові отримали технологічні засоби, здатні допомогти їм стримати агресора [22]. На цю «схвильованість» відреагували представники громадянського суспільства в Україні, висловлюючи побоювання, що подальше використання технологій, заборонених на території деяких держав ЄС, може загальмувати або поставити під загрозу процес вступу України до ЄС [23]. Існування проблеми контролю над використанням штучного інтелекту констатували також зарубіжні та вітчизняні правознавці [9].

Враховуючи згадані ризики для подальшого використання в Україні технологій, схожих на системи Clearview AI, Palantir та ін., автори матеріалу «Штучний інтелект у сфері оборони: виклики регулювання» роблять акцент на тому, що захист прав людини при використанні технологій штучного інтелекту є головною проблемою для українських регуляторів у контексті війни, а вирішення її вбачають у розмежуванні двох сценаріїв розвитку штучного інтелекту – «мирного» та «воєнного» – і розробки для кожного з них відповідних правил [10].

Така пропозиція видається нам логічною, оскільки є ситуації звичайні, а є аномальні: правила, що стосуються звичайних відносин, не діють в аномальних ситуаціях.

Але тут слід зауважити, що проблема регулювання використання штучного інтелекту в Україні загострюється необхідністю враховувати не тільки особливості «мирного» та «воєнного» алгоритмів, а ще й євроінтеграційних процесів. У зв'язку з цим у жовтні 2023 року Міністерство цифрової трансформації оприлюднило Дорожню карту з регулювання штучного інтелекту в Україні [24], котра розглядається як підтвердження намірів уряду поступово імплементувати Закон ЄС про штучний інтелект (AI Act), який приділяє значну увагу захисту прав людини при впровадженні та застосуванні штучного інтелекту.

Закон ЄС про штучний інтелект (Artificial Intelligence Act, AIA), прийнятий у межах Європейського Союзу, є першим у світі деталізованим регуляторним актом, спрямованим на правове регулювання штучного інтелекту. Він визначає принципи та правила розробки, впровадження й використання штучного інтелекту з урахуванням ризиків, які такі технології можуть створювати для суспільства та економіки. Закон про штучний інтелект запроваджує єдину структуру для всіх країн ЄС, засновану на далекоглядному визначенні штучного інтелекту та підході, заснованому на оцінці ризиків:

– Мінімальний ризик: більшість систем штучного інтелекту, таких як спам-фільтри та відеоігри з підтримкою штучного інтелекту, не стикаються з зобов'язаннями відповідно до Закону про штучний інтелект, але компанії можуть добровільно прийняти додаткові кодекси поведінки.

– Специфічний ризик прозорості: такі системи, як чат-боти, повинні чітко інформувати користувачів про те, що вони взаємодіють з машиною, тоді як певний контент, створений штучним інтелектом, повинен бути позначений як такий.

– Високий ризик: системи штучного інтелекту з високим ризиком, такі як медичне програмне забезпечення на основі штучного інтелекту або системи штучного інтелекту, що використовуються для підбору персоналу, повинні відповідати суворим вимогам, включаючи системи зниження ризиків, високу якість наборів даних, чітку інформацію про користувачів, людський нагляд тощо.

– Неприйнятний ризик: наприклад, системи штучного інтелекту, які дозволяють урядам або компаніям «оцінювати соціальні показники», вважаються явною загрозою основним правам людей і тому заборонені. Такими особливо шкідливими застосуваннями штучного інтелекту є:

– Експлуатація вразливостей осіб, маніпулювання та використання підсвідомих прийомів;

– Соціальний скоринг для державних і приватних цілей (скоринг являє собою математичну або статистичну модель, за допомогою якої на основі кредитних історій інших клієнтів банк намагається визначити, наскільки велика ймовірність того, що конкретний потенційний позичальник поверне кредит в строк);

– Індивідуальна предиктивна поліція, що ґрунтується виключно на профілюванні людей;

– Нецілеспрямований скрейпінг Інтернету або камер відеоспостереження для отримання зображень обличчя для створення або розширення баз даних (скрейпінг – це форма копіювання, в якій конкретні дані збираються та копіюються з інтернету, як правило, в базу даних або електронну таблицю для подальшого пошуку чи аналізу);

– Розпізнавання емоцій на робочому місці та в навчальних закладах, за винятком медичних

причин або міркувань безпеки (наприклад, моніторинг рівня втоми пілота);

– Біометрична категоризація фізичних осіб для визначення або визначення їхньої раси, політичних поглядів, членства в профспілках, релігійних чи філософських переконань або сексуальної орієнтації. Маркування або фільтрація наборів даних та категоризація даних у сфері правоохоронних органів, як і раніше, будуть можливими;

– Дистанційна біометрична ідентифікація в режимі реального часу в загальнодоступних місцях правоохоронними органами, за рідкими винятками.

Класифікація ризиків ґрунтується на цільовому призначенні системи штучного інтелекту, відповідно до чинного законодавства ЄС про безпеку продукції. Це означає, що класифікація залежить від функції, яку виконує система штучного інтелекту, а також від конкретної мети та способів, для яких використовується система.

Як свідчить навіть побіжне ознайомлення з положеннями Закону, особливу увагу у ньому приділено забороні деяких застосунків штучного інтелекту, які загрожують правам громадян, таких як системи біометричної категоризації та розпізнавання емоцій. Це відображає тенденцію до захисту приватності та особистих даних, яка стає все більш актуальною в сучасному світі.

При цьому Закон припускає широке розуміння штучного інтелекту та залишає поза сферою застосування лише певні конкретні прояви цих систем. Зокрема, не підпадають під дію Закону: (1) системи, які розміщені на ринку, введені в експлуатацію або використовуються з модифікаціями або без них для військових цілей, оборони чи національної безпеки (це виключення поширюється на використання результати виробництва систем штучного інтелекту, які не розміщені на ринку чи введені в експлуатацію в ЄС); та (2) системи чи моделі штучного інтелекту, включно з їхніми вихідними результатами, спеціально розроблені та введені в експлуатацію виключно з метою наукових досліджень і розробок. Закон пояснює, що він не застосовуватиметься до будь-яких наукових досліджень і розробок систем або моделей штучного інтелекту до їх розміщення на ринку або введення в експлуатацію, хоча це виключення не включає тестування в реальних умовах.

Таким чином, норми Закону не застосовуються щодо систем, які розміщені на ринку, введені в експлуатацію або використовуються з модифікаціями або без них для військових цілей, оборони чи національної безпеки (це виключення поширюється на використання результатів виробництва систем штучного інтелекту, які не розміщені на ринку чи введені в експлуатацію в ЄС).

Саме тому, відповідно до Дорожньої карти з регулювання штучного інтелекту в Україні, на першому етапі регулювання, який триватиме до 2025/2026 року, уряд намагатиметься «не зарегулювати» галузь штучного інтелекту, водночас готуючи бізнес до юридично обов'язкової регуляції. При цьому під час повномасштабної війни регуляція штучного інтелекту у проєктах, що стосуються воєнних потреб, не передбачається.

«Нам потрібно використовувати принцип зонування: яким має бути регулювання штучного інтелекту під час війни та після перемоги. Під час війни ми плануємо розробити законодавчу базу, яка не заважатиме використанню інновацій та технологій штучного інтелекту задля перемоги. Але після війни регуляція штучного інтелекту має допомогти Україні й надалі посилювати демократичність», – повідомила Анна Булах, голова з етики штучного інтелекту та партнерства у Respeecher та член комітету штучного інтелекту при Мінцифри [25].

Нам таке рішення здається цілком виправданим.

Зазначимо також, що автори згадуваного раніше аналітичного матеріалу «Штучний інтелект у сфері оборони: виклики регулювання», попри констатацію тієї обставини, що штучний інтелект довів свою ефективність під час російсько-української війни, наполягають на врахуванні ризиків штучного інтелекту, вважаючи що ці ризики не можуть підлягати лише галузевому «саморегулюванню», зокрема коли це стосується застосування технологій штучного інтелекту за межами відсічі російській агресії.

На їхню думку, усунути ризики та забезпечити «справедливе й підзвітне» застосування технологій штучного інтелекту у «мирній» сфері, можуть, зокрема, такі заходи:

– Внесення змін до чинного законодавства, усунення прогалин регулювання застосовування технологій штучного інтелекту в оборонних цілях, з метою забезпечення гарантій захисту прав та свобод людини. Експерти Лабораторії цифрової безпеки пропонують, зокрема, з цією метою внести зміни до законів «Про захист персональних даних», «Про національну поліцію», а також до Кримінального та Кримінально-процесуального кодексів [26].

– Забезпечення пріоритетності впровадження регуляції (замість саморегулювання) у завдання розробки та використання технологій штучного інтелекту, що використовуються для оборонних

цілей. Ризик втручання в демократичні права та свободи є головним аргументом на користь проактивних дій.

– Контроль відповідальних осіб або суду за застосуванням цих технологій.

– Публічність процесу регламентації застосування цих технологій: постійні обговорення та дискусії для досягнення балансу інтересів між владою, громадянським суспільством та компаніями-розробниками штучного інтелекту.

Наостанок автори цього матеріалу ще раз наголошують, що головним завданням для українського регулювання сфери застосування технологій оборонного штучного інтелекту має стати забезпечення захисту прав людини (Підкреслено нами – Є. Х., О. Х.), які можуть постраждати від такого застосування, особливо якщо ці технології застосовуються не на полі бою. Саме це має стати стрижневою ідеєю при створенні правового регулювання технологій штучного інтелекту, поруч із забезпеченням економічного розвитку галузі [10].

У пошуках відповіді на це питання, пропонувалося розрізняти «оборонний штучний інтелект» та «наступальний штучний інтелект».

Перший з них – спрямований, передусім, на «кібернетичне забезпечення» військових/ воєнних потреб країни, а також на відвернення (переважно – пасивне) кіберзагроз. Другий – спрямований на ведення активних (наступальних) дій у кібервійні, котра може провадитись окремо або бути складовою частини мілітарної війни.

При цьому «оборонний» штучний інтелект характеризується як потужний інструмент у боротьбі з кіберзагрозами, котрий, крім того, ефективно допомагає вирішувати логістичні проблеми, забезпечувати підвищення обізнаності, готовності та можливостей під час війни, зокрема шляхом моделювання сценаріїв бойової підготовки, моніторингу відеоспостереження, збору та аналізу даних з відкритих джерел, аналізу розпізнавання осіб, розвідки та оцінки збитків. Він також стимулює внутрішнє виробництво продукції подвійного призначення, такої як тепловізійні камери, датчики та безпілотники [27]. Натомість «наступальний» штучний інтелект, на думку його критиків, належить до систем, призначених для допомоги або виконання шкідливих дій. Майже 74% експертів з кібербезпеки, опитаних автором статті, де критикується «наступальний» штучний інтелект, назвали загрози від нього серйозною проблемою, оскільки відповідні технології здатні розробляти стратегії за межами людських можливостей, і здатні трансформувати поле бою в сфері кібербезпеки. Такий штучний інтелект може поширювати дезінформацію, порушувати політичні процеси та маніпулювати громадською думкою. Використання автономної зброї на основі штучного інтелекту може призвести до порушень прав людини. У підсумку робиться висновок, що встановлення керівних принципів їх відповідального використання є важливим для підтримки глобальної стабільності та гуманітарних цінностей [28].

Таким чином «оборонний» штучний інтелект розглядається, головним чином, як явище позитивне, а «наступальний» – переважно як носій загроз.

Проте слушним здається зауваження, що «на сучасному етапі розвитку інформаційних технологій, системи та/або моделі штучного інтелекту використовуються не лише для посилення систем кіберзахисту, а й для розробки нових типів (видів) інформаційно-руйнівних впливів у вигляді адаптивних кібератак, потенційно спроможних уникати виявлення існуючими захисними системами. Кібератаки, створені з використанням штучного інтелекту характеризуються прикладною новизною, складністю, швидкістю адаптації та масштабованістю Це робить існуючі методи виявлення кібератак майже не ефективними, що у свою чергу створює серйозну загрозу для інформаційних систем як державного, так і комерційного призначення. До того ж, останнім часом спостерігається значне зростання кількості випадків створення кібератак і шкідливого програмного забезпечення з використанням моделей штучного інтелекту, як наслідок загальнодоступності та фактичної відсутності обмежень на їх використання» [29].

Крім того, маємо також враховувати, шо «оборонний» інтелект забезпечує й можливість підтримувати підключення до мереж зв'язку супротивника та покращувати операції радіоелектронної боротьби (РЕБ). Він також може посилювати шифрування даних та мережі обміну, у той час як системи кібербезпеки на основі штучного інтелекту можуть автоматично визначати, аналізувати та класифікувати загрози, забезпечуючи швидші та ефективніші реакції, що практично нівелює різницю між оборонним та наступальним штучним інтелектом. Необхідним у сфері оборонного штучного інтелекту є прийняття законодавства для забезпечення прозорості, стандартизації та оптимізованих протоколів ліцензування та імпорту [27].

Висновки. У підсумку, констатувавши неможливість чіткого розмежування «оборонного» та «наступального» штучного інтелекту, повертаємось до питань: доцільно чи ні розмежувати

«воєнне» та «невоєнне» застосування «оборонного» штучного інтелекту? І що таке «оборонний штучний інтелект»: «призначений для оборони» чи такий, що колись «розроблявся для оборони», але втратив своє призначення і застосовується «не на полі бою». Тоді, чому він «оборонний»?

А найбільше сумнівів викликає теза щодо головного завдання для українського регулювання сфери застосування технологій оборонного штучного інтелекту. Усе ж таки: головне завдання – це забезпечення захисту прав людини чи забезпечення виживання країни у війні, що має екзістенційний характер, про що часто згадують експерти? Бо коли не враховувати друге, то й перша проблема просто відпаде, оскільки кривавий досвід свідчить, що наївно очікувати від російських окупантів забезпечення захисту прав людини.

У зв'язку з цим зауважимо раціональний підхід, відображений у «Білій книзі», розробленій Мінцифри [30]. Представляючи її, віце-прем'єр, міністр з цифрової трансформації Михайло Федоров зазначив, що Біла книга детально описує підхід України до регулювання штучного інтелекту та звернув увагу на те, що в ній враховані виклики нашої реальності, а тому сфера оборони залишається поза регулюванням: «Ми повинні не обмежувати такі ШІ-продукти, а навпаки – впроваджувати більше інновацій, які допомагають боротися з ворогом. Розуміємо і те, що для розвитку України необхідна максимальна дерегуляція та зменшення бюрократії, щоб позбутися перепон для впровадження технологій. Водночас небезпеку стрімкого розвитку штучного інтелекту та його потенційного впливу на права людини зараз визнає весь світ. Щоб зберегти баланс, ми розробили підхід, який адресує виклики без упровадження обов'язкового регулювання в найближчі 2–3 роки». Він також зазначив, що «Україна робить ставку на гнучкість і адаптивність. Ми даємо бізнесу час та інструменти для підготовки до майбутнього національного законодавства. Біла книга передбачає конкретні інструменти, частину з яких бізнес може використовувати вже зараз. Вони дадуть змогу підготуватися до виходу на ринок ЄС, де вже незабаром буде затверджено відповідне регулювання. Наступний етап – гармонізувати наше законодавство із законодавством ЄС. Це не тільки необхідно для євроінтеграції, а й дасть змогу активніше залучати інвестиції на український ринок. Зокрема, за рахунок ідентичних правових режимів» [31].

Порівнюючи законодавство ЄС щодо AI (ШІ) та позицію з цього питання України, Forbes зауважує, що згідно з опитуванням Kantar Ukraine, опублікованому у «Білій книзі», 45% українців вважають, що Україна має прийняти закон про регулювання штучного інтелекту. Прикладом для наслідування тут обраний Європейський Союз, котрий першим у світі взявся за регуляцію штучного інтелекту: як уже згадувалося, у березні 2024 року Європарламент ухвалив AI Act. Разом із тим, як йдеться у «Білій книзі», Україна на першому етапі цим шляхом поки не йде, але на другому ухвалить закон – аналог європейському AI Act [32].

Підбиваючи підсумки нашої розвідки, зауважимо, що дискусія у галузі, яка нас цікавить, очевидно триватиме, можливі різні варіанти рішень.

На нашу думку, наразі штучний інтелект (з погляду оцінки його значення в умовах гібридної війни) перебуває на порозі «зламу».

Але, поки йдеться про використання його для виживання держави у екзістенційному протистоянні агресору, варто підтримати позицію Білої книги. Європейський Акт про штучний інтелект має враховуватися, Але зауважимо, що наразі штучний інтелект не віднесений до «неконвенційної» зброї, а його використання не розцінюється як «порушення правил війни».

ЛІТЕРАТУРА:

1. Сенгер, Девід Е. Досконала зброя. Війна, саботаж і страх у кіберепоху / пер. з англ. Вікторія Дєдик: фах.ред.укр.вид Олександр Дєдик і Олег Фешовець. Львів: Видавництво «Астролябія», 2022. 496 с.
2. Наймасштабніша кібератака росіян на державні реєстри: які дані українців були під загрозою. URL: https://acc.cv.ua/news/ukraine/naymasshtabnisha-kiberataka-rosiyan-na-derzhavni-reestri-yaki-dani-ukrayinciv-buli-pid-zagrozoyu-107163. Сайт https://acc.cv.ua/
3. Щербина Б.С., Ткаченко В.В. Штучний інтелект як суб'єкт цивільного права. Юридичний вісник. 2021. 1 (58). URL: https://er.nau. edu.ua/bitstream/NAU/53555/1/22197.pdf.
4. Стефанчук М.О., Музика-Стефанчук О.А., Стефанчук М.М. Перспективи правового регулювання відносин у сфері використання штучного інтелекту. Вісник Національної академії правових наук України. 2021. Т. 28. №1. С. 157–168. doi: 10.37635/jnalsu.28(1).2021.157-168.
5. Андрощук Г. О. Проблеми патентування винаходів, створених з використанням штучного інтелекту: доктрина і практика (Ч. 1). *Теорія і практика інтелектуальної власності.* 2022. № 2. С. 54–67. URL: https://doi.org/10.33731/22022.259744.
6. Якубівський І.Є. Цивільно-правовий режим об'єктів, згенерованих штучним інтелектом. Науковий вісник Ужгородського Національного Університету, 2024 Серія ПРАВО. Вип. 82. Ч. 1. С. 355–361.
7. Пилипчук В.Г., Баранов О.А., Гиляка О.С. Проблема правового регулювання у сфері штучного інтелекту в контексті розвитку законодавства Європейського Союзу. *Вісник Національної академії правових наук України.* Том 29, № 2. 2022. С. 35–62.

8. Харитонова О.І. Актуальні проблеми штучного інтелекту в праві інтелектуальної власності. *Юридичний вісник. 2024. № 5.*
9. Костенко О., Джейнс Т., Журавльов Д., Дніпров О., Усенко Ю. Проблеми використання автономного військового ші на фоні військової агресії росії проти України. *Балтійський журнал юридичних та соціальних наук*, 2023. 4, 131–145. https://doi.org/10.30525/2592-8813-2022-4-16
10. Дарина Бойко, Іван Городиський. Штучний інтелект у сфері оборони: виклики регулювання. 12 січня 2024. URL: https://dc.org.ua/news/shtuchnyy-intelekt-u-sferi-oborony-vyklyky-regulyuvannya
11. Information security and IT law in conditions of integration processes: [Collective monograph]. Edited by O. Kharytonova, E. Kharytonov. Riga: Izdevnieciba Baltija Publishing, 2017. 213 p.
12. Харитонов Є.О. Інформаційна безпека з погляду цивілістики / Цивільне право та інформаційна безпека в умовах інтеграційних процесів : мат. кругл. столу (3 червня 2017 р., м. Одеса). Збірник матеріалів Міжнародного Конгресу «Правові проблеми державно-правового партнерства в умовах євроінтеграції», присвяченого 20-річчю Національного університету «Одеська юридична академія», м. Одеса, 2-4 червня 2017 р. / відп.ред.: Є.О. Харитонов, О.І. Харитонова, Т.Є. Харитонова; Нац.ун-т «Одес.юрид.акад.». Одеса: Юрид. Літ., 2017. С. 64–68.
13 Харитонов Є.О., Харитонова О.І. Проблеми правового регулювання в ІТ-сфері в умовах інформаційної війни. Проблеми відновлення конституційного ладу в Україні: Матеріали міжнародної науково-практичної конференції. м. Київ. 19-20 травня 2017 р. Київ : Таврійський національний університет ім. В.І. Вернадського. 2017. С. 159–163.
14. Харитонов Є.О., Харитонова О.І. Проблеми відшкодування майнової шкоди у сфері використання інформаційних технологій. Спогади про Людину, Вченого, Цивіліста (до 90-річчя від Дня народження професора Діни Василівни Боброві); за заг. ред. Р.О. Стефанчука. К. : АртЕк, 2019 С. 275–287.
15. Харитонов Є.О. COVID-19 та проблеми інформаційної безпеки. Цивілістичні проблеми інформаційної безпеки в умовах COVID-19: матеріали Всеукр. круглого столу, Одеса, 21 червня 2021 р. / за заг. ред. д.ю.н., проф. Є.О. Харитонова, д.ю.н., проф. І.В. Давидової. Одеса : Фенікс, 2021. С. 5–9.
16. Kharytonov E., Kharytonova O., Tolmachevska Y., Fasii B., Tkalych M. Information Security and Means of Its Legal Support. Amazonia Investiga, 8(19). P. 255–265.
17. Попова Т.В., Ліпкан В.А. Стратегічні комунікації. Словник. Т.В. Попова, В.А. Ліпкан / за заг. ред. В.А. Ліпкана. К. : ФОП О.С. Ліпкан. 2016.
18. Горбулін В. П. Без права на покаяння. Харків : Фоліо, 2010. С. 5.
19. Як соцмережі видаляють докази воєнних злочинів Росії в Україні. Розслідування BBC. Джек Гудман і Марія Коренюк. Відділ BBC з боротьби з дезінформацією. 1 червня 2023. URL: https://www.bbc.com/ukrainian/features-65774526#:~:text=%D0%A0%D0%BE%D0%B7%D1%81%D0%BB%D1%96%D0%B4%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%92%D0%92%D0%A1,-%D0%94%D0%B6%D0%B5%D0%BA%20%D0%93%D1%83%D0%B4%D0%BC%D0%B0%D0%BD%20%D1%96&text=%D0%94%D0%BE%D0%BA%D0%B0%D0%B7%D0%B8%20%D0%BF%D0%BE%D1%82%D0%B5%D0%B
20. Як штучний інтелект перетворив українську блогерку на російську пропагандистку. Author,Фан Ван. Role, BBC News. 15 травня 2024. URL: https://www.bbc.com/ukrainian/articles/cw4d4weqn5lo
21. Україна – Clearview AI. URL: https://www.clearview.ai/success-stories
22. Чи наближає технологія розпізнавання обличь під час війни в Україні роботів-убивць? Clearview AI пропонує Україні свою суперечливу технологію для ідентифікації ворожих солдатів, тоді як автономні машини для вбивства набирають обертів. Даріан мічеммартін Гак. 30 березня 2022, URL: https://www.opendemocracy.net/en/technology-and-democracy/facial-recognition-ukraine-clearview-military-ai/
23. Дорожня_карта_з_регулювання_ШІ_в_Україні_compressed.pdf (thedigital.gov.ua) URL: https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs/%D0%94%D0%BE%D1%80%D0%BE%D0%B6%D0%BD%D1%8F_%D0%BA%D0%B0%D1%80%D1%82%D0%B0_%D0%B7_%D1%80%D0%B5%D0%B3%D1%83%D0%BB%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D0%A8%D0%86_%D0%B2_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%96_compressed.pdf
24. Наскільки «зрозуміла» законність Clearview AI в Україні? 9 жовтня 2023. Анна Людва, Тетяна Авдєєва. Аналітичний звіт підготовлено в рамках програми «Сприяння свободі Інтернету в Україні», що реалізується Американською асоціацією юристів в Україні / Ініціатива з верховенства права. URL: https://dslua.org/publications/how-clear-is-the-legality-of-clearview-ai-in-ukraine/
25. Коли в Україні запрацює регулювання ШІ. Розповідає Анна Булах з Respeecher (delo.ua). URL: https://delo.ua/telecom/yak-ta-koli-v-ukrayini-moze-zapracyuvati-regulyuvannya-stucnogo-intelektu-rozpovidaje-anna-bulax-golova-z-etiki-si-ta-partnerstva-u-respeecher-423903/
26. Наскільки «зрозуміла» законність Clearview AI в Україні? – Лабораторія цифрової безпеки (dslua.org). URL: https://dslua.org/publications/how-clear-is-the-legality-of-clearview-ai-in-ukraine/
27. Гончарук В. Як Україна використовує штучний інтелект для оборони від російської агресії – Foreign Ukraine. URL: https://foreignukraines.com/2024/10/10/how-ukraine-uses-artificial-intelligence-to-defend-against-russian-aggression/
28. Хазіка Саджид. Загроза наступального ШІ та як від неї захиститися. URL: https://www.unite.ai/uk/загроза-наступального-AI-і-як-від-нього-захиститися/
29. Фесьоха В. Особливості протистояння оборонного та наступального штучного інтелектів у кіберпросторі. International Science Journal of Engineering & Agriculture. 2024. № 3 (4). С. 105–114.
30. Регулювання штучного інтелекту в Україні: Мінцифри презентує Білу книгу. Міністерство цифрової трансформації України, опубліковано 26 червня 2024 року. URL: https://www.kmu.gov.ua/news/rehuliuvannia-shtuchnoho-intelektu-v-ukraini-mintsyfry-prezentuie-bilu-knyhu
31. Біла книга з регулювання ШІ в Україні: бачення Мінцифри. Версія для консультацій. URL: https://thedigital.gov.ua/storage/uploads/files/page/community/docs/%D0%A0%D0%B5%D0%B3%D1%83%D0%BB%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%A8%D0%86.pdf

32. Мінцифри пропонує прийняти аналог європейського AI Act і створити регуляторний орган. Що ще передбачає «Біла книга» регулювання ШІ? Анастасія Несенюк. URL: https://forbes.ua/innovations/mintsifri-proponue-priynyati-zakon-analog-evropeyskomu-ai-act-ta-stvoriti-regulyatorniy-organ-shcho-shche-peredbachae-bila-kniga-regulyuvannya-shi-27062024-22020

Харитонова Олена Іванівна, Харитонов Євген Олегович

Штучний інтелект у гібридній війні: правові проблеми

Стаття присвячена правовим проблемам штучного інтелекту у гібридній війні. Зазначається, що віртуалізація суспільства супроводжується зростанням значення кіберзброї та штучного інтелекту в гібридній війні. Наразі кібервійна стає «буденним» явищем, котре, до того ж, усе активніше включає й штучний інтелект. Разом із тим, це «буденне» явище є недостатньо осмисленим концептуально і регламентованим юридично. Встановлено, що кібервійна є різновидом інформаційної війни у кіберпросторі, а кіберзброя розуміється як різновид інформаційної зброї, головними елементами якої є інформація та інформаційні технології, способи і засоби інформаційного впливу й захисту від нього, призначені для ведення інформаційної боротьби у кіберпросторі. Зроблено висновок, що вищим ступенем загрози є такий, що може вийти з-під влади людини: поєднання кіберзброї зі штучним інтелектом. Це є головною гібридною загрозою, а відтак потребує адекватної (гібридної) відповіді, зокрема, за допомогою юридичних заходів. Крім цього, зазначається, що штучний інтелект може застосовуватися як кіберзброя (або – як елемент кіберзброї) не лише у інформаційній гібридній війні, але й у «мілітарній» гібридній війні.

Зроблено висновок, що використання штучного інтелекту у «воєнній війні» ускладнюється, крім усього іншого, існуванням колізії публічних та приватних інтересів, вирішення якої потребує і у цьому разі «гібридного» юридичного забезпечення. Зокрема, встановлено, що застосування технологій штучного інтелекту (навіть у суто воєнних цілях) викликало занепокоєння серед міжнародних організацій, на кшталт OpenDemocracy, котрі у березні 2022 року (тобто у то час, коли доля України висіла на волосині), хвилювалася, що українські військові отримали технологічні засоби, здатні допомогти їм стримати агресора. Отже, захист прав людини при використанні технологій штучного інтелекту є головною проблемою для українських регуляторів у контексті війни, а вирішення її вбачають у розмежуванні двох сценаріїв розвитку штучного інтелекту – «мирного» та «воєнного» – і розробки для кожного з них відповідних правил.

Проаналізовано доцільність виокремлення оборонного і наступального штучного інтелекту. Зазначається, що на сучасному етапі розвитку інформаційних технологій, системи та/або моделі штучного інтелекту використовуються не лише для посилення систем кіберзахисту, а й для розробки нових типів (видів) інформаційно-руйнівних впливів у вигляді адаптивних кібератак, потенційно спроможних уникати виявлення існуючими захисними системами. Тому зроблено висновок про неможливість чіткого розмежування «оборонного» та «наступального» штучного інтелекту. Констатується, що проблема регулювання використання штучного інтелекту в Україні загострюється необхідністю враховувати не тільки особливості «мирного» та «воєнного» алгоритмів, а ще й євроінтеграційних процесів. У зв'язку з цим у жовтні 2023 року Міністерство цифрової трансформації оприлюднило Дорожню карту з регулювання штучного інтелекту в Україні, котра розглядається як підтвердження намірів уряду поступово імплементувати Закон ЄС про штучний інтелект (AI Act), який приділяє значну увагу захисту прав людини при впровадженні та застосуванні штучного інтелекту. Таким чином, головним завданням для українського регулювання сфери застосування технологій оборонного штучного інтелекту має стати забезпечення захисту прав людини, які можуть постраждати від такого застосування, особливо якщо ці технології застосовуються не на полі бою. Саме це має стати стрижневою ідеєю при створенні правового регулювання технологій штучного інтелекту, поруч із забезпеченням економічного розвитку галузі. У підсумку зазначається, що дискусія о триватиме, можливі різні варіанти рішень. На думку авторів, наразі штучний інтелект (з погляду оцінки його значення в умовах гібридної війни) перебуває на порозі «зламу». Але, поки йдеться про використання його для виживання держави у екзистенційному протистоянні агресору, варто підтримати позицію Білої книги. Європейський Акт про штучний інтелект має враховуватися, Але наразі штучний інтелект не віднесений до «неконвенційної» зброї, а його використання не розцінюється як «порушення правил війни».

Ключові слова: штучний інтелект, гібридна війна, мілітарна війна, кіберзброя, кіберзахист, кіберпростір, права людини, оборона, інформаційні технології, закон про штучний інтелект.

Kharytonova Olena, Kharytonov Evhen

Artificial intelligence in hybrid warfare: legal issues

The article is devoted to the legal issues of artificial intelligence in hybrid warfare. It is noted that the virtualization of society is accompanied by an increase in the importance of cyber weapons and artificial intelligence in hybrid warfare. Currently, cyberwarfare is becoming a "commonplace" phenomenon, which, moreover, increasingly includes artificial intelligence. At the same time, this "everyday" phenomenon is not sufficiently conceptualized and legally regulated. It is established that cyberwar is a type of information warfare in cyberspace, and cyberweapons are understood as a type of information weapon, the main elements of which are information and information technology, methods and means of information influence and protection intended for information warfare in cyberspace. It is concluded that the highest degree of threat is the one that can get out of human control: the combination of cyber weapons

with artificial intelligence. This is the main hybrid threat, and therefore requires an adequate (hybrid) response, in particular, through legal measures. In addition, it is noted that artificial intelligence can be used as a cyber weapon (or as an element of cyber weapons) not only in information hybrid warfare, but also in "military" hybrid warfare.

It is concluded that the use of artificial intelligence in a "war of war" is complicated, among other things, by the existence of a conflict of public and private interests, the resolution of which requires "hybrid" legal support in this case. In particular, it is established that the use of artificial intelligence technologies (even for purely military purposes) has caused concern among international organizations such as OpenDemocracy, which in March 2022 (i.e., when the fate of Ukraine hung in the balance) was worried that the Ukrainian military had received technological means that could help them deter the aggressor. Thus, the protection of human rights in the use of artificial intelligence technologies is the main problem for Ukrainian regulators in the context of war, and the solution is seen in the distinction between two scenarios of artificial intelligence development – "peaceful" and "military" – and the development of appropriate rules for each of them.

The expediency of distinguishing between defensive and offensive artificial intelligence is analyzed. It is noted that at the current stage of development of information technologies, artificial intelligence systems and/or models are used not only to strengthen cyber defense systems, but also to develop new types (types) of information-destructive impacts in the form of adaptive cyber attacks which are potentially able to avoid detection by existing defense systems. Therefore, the author concludes that it is impossible to clearly distinguish between "defensive" and "offensive" artificial intelligence. It is stated that the problem of regulating the use of artificial intelligence in Ukraine is exacerbated by the need to take into account not only the peculiarities of "peaceful" and "military" algorithms, but also European integration processes. In this regard, in October 2023, the Ministry of Digital Transformation published a Roadmap for the Regulation of Artificial Intelligence in Ukraine, which is seen as a confirmation of the government's intention to gradually implement the EU Artificial Intelligence Act (AI Act), which pays significant attention to the protection of human rights in the introduction and use of artificial intelligence. Thus, the main task for Ukrainian regulation of the use of defense artificial intelligence technologies should be to ensure the protection of human rights that may be affected by such use, especially if these technologies are not used on the battlefield. This should be the core idea when creating legal regulation of artificial intelligence technologies, along with ensuring the economic development of the industry. In conclusion, it is noted that the discussion will continue, and various solutions are possible. According to the authors, artificial intelligence (in terms of assessing its importance in hybrid warfare) is currently on the verge of a "breakthrough". However, as long as it is used for the survival of the state in the existential confrontation with the aggressor, the position of the White Paper should be supported. The European Artificial Intelligence Act should be taken into account, but currently artificial intelligence is not classified as a "non-conventional" weapon, and its use is not considered a "violation of the rules of war."

Key words: artificial intelligence, hybrid warfare, military warfare, cyberweapons, cyber defense, cyberspace, human rights, defense, information technology, law on artificial intelligence.