DOI: 10.33270/01242702.45
УДК 340.11

Міжнародний досвід правового регулювання небезпеки штучного інтелекту в реаліях воєнного часу: етико-філософський аспект

СОВА Маргарита*
доктор педагогічних наук, професор,
професор кафедри психології, педагогіки та суспільних дисциплін Державного податкового університету
м. Ірпінь, Україна
ORCID: https://orcid.org/0000-0002-3190-7903;
ДЄНІЖНА Світлана
кандидат педагогічних наук, доцент,
доцент кафедри психології, педагогіки та суспільних дисциплін Державного податкового університету
м. Ірпінь, Україна
ORCID: https://orcid.org/0009-0009-4671-2162

Анотація. У статті аргументовано, що вивчення міжнародного досвіду правового врегулювання загроз штучного інтелекту в кіберпросторі за воєнного часу є актуальним напрямом наукових пошуків, який потребує поглибленого й системного дослідження. Мета статті – висвітлити етико-філософський аспект міжнародного досвіду правового врегулювання загроз штучного інтелекту воєнним діям і визначити стратегічні напрями державно-правової політики щодо його впровадження в реаліях воєнного часу. Для здійснення дослідження застосовано систему методів наукового пізнання: філософський, загальнонаукові (аналіз і синтез, індукція та дедукція, абстрагування та конкретизація, аналогія та контраст); приватні методи наукового пізнання, що використовують у багатьох галузевих науках (компаративний, кількісний і якісний аналіз); спеціально-юридичні (формально-юридичний, порівняльно-правовий, системно-структурний). Проаналізовано міжнародний досвід правового регулювання використання технологій штучного інтелекту в умовах глобальних загроз; пріоритетні орієнтири вітчизняної державно-правової політики щодо запобігання ризиків використання штучного інтелекту як інструментів військової небезпеки; окреслено перспективні напрями вдосконалення правового регулювання використання цифрових технологій за воєнного стану крізь призму інтеграційних процесів. З'ясовано, що впровадження міжнародного досвіду правового регулювання небезпеки використання штучного інтелекту під час війни має відбуватися в контексті євроінтеграційних процесів, ґрунтуватися на фундаментальних цінностях і принципах верховенства права, нормативно-правових актах, стандартах і правилах провідних країн, попри виклики й обмеження, пов'язані з воєнними обставинами. Обґрунтовано, що за воєнного часу в Україні гостро постало питання про підвищення ефективності розслідування кіберзлочинів завдяки використанню технологій штучного інтелекту. Новизна дослідження полягає у визначенні стратегічних напрямів правового регулювання небезпеки використання технологій штучного інтелекту за воєнного часу на підставі міжнародного досвіду та відповідно до європейських нормативно-правових актів, принципів міжнародного права, стандартів і рекомендацій провідних країн світу. У висновках зазначено, що правове врегулювання використання штучного інтелекту в Україні доцільно здійснювати за обраним державою євроінтеграційним курсом, згідно зі стандартами та правилами, висвітленими в міжнародних нормативно-правових документах. З цих позицій визначено ключові напрями правового регулювання загроз застосування сучасних цифрових технологій в умовах воєнного стану. Правове регулювання ризиків сучасного програмного забезпечення має сприяти стримуванню війни, зменшенню її смертоносності, врятуванню життя людей, захисту їх прав і свобод.

Ключові слова: правове регулювання; штучний інтелект; кіберпростір; кібербезпека; кіберзлочинність.

Історія статті:
Отримано: 02.02.2024
Переглянуто: 04.03.2024
Прийнято: 01.04.2024

Рекомендоване посилання:
Сова М., Дєніжна С. Міжнародний досвід правового регулювання небезпеки штучного інтелекту в реаліях воєнного часу: етико-філософський аспект. *Філософські та методологічні проблеми права.* 2024. № 1 (27). С. 45–57. doi: 10.33270/01242702.45.

*Відповідальний автор

Вступ

З початком російсько-української війни загострилася проблема правового врегулювання процесів використання штучного інтелекту під час захисту території та протистояння в кібернетикному просторі. В умовах сьогодення зазначена проблема набуває глобального масштабу, оскільки стосується міжнародної кібербезпеки, розвитку безпілотної авіації, застосування електронної боротьби для захисту населення та територій різних країн світу. Як відомо, значну загрозу в збройному конфлікті становлять кібератаки, спрямовані на руйнування оборонних підприємств і технологічних компаній, об'єктів критичної інфраструктури й енергосистеми країни.

Кіберзлочинність завдає збитків електро- та водопостачанню, електронним комунікаціям, транспортним підприємствам, пошкоджує сховища стратегічних видів сировини. Серйозні виклики зумовлені також переходом на 5G-мережі, функціонування яких залежить від роботи програмного забезпечення та непередбачених загроз новітніх технологій.

На жаль, у сучасному кіберпросторі відбувається зростання міждержавного протиборства із застосуванням технологій штучного інтелекту у сфері розвідувально-підривної діяльності, поширюються масштаби використання кіберпростору терористичними організаціями.

Певна річ, учинення кіберзлочинності впливає на стан обороноздатності держави, зумовлює дестабілізацію політичної, соціально-економічної ситуації, фінансову збитковість, фальсифікацію інформації. Тому для наукової галузі України, яка перебуває в стані війни, актуальною проблемою є удосконалення державної політики щодо кібербезпеки, зокрема правового регулювання загроз у сфері штучного інтелекту, мінімізації ризиків використання сучасних технологічних досягнень, що, відповідно, має сприяти соціально-економічному розвитку держави в цифровому світі.

Матеріали та методи

Складається враження, що у сучасному цифровому середовищі штучний інтелект панує над людьми, суспільством, державами поза часом і поза простором. Тому пошук шляхів розв'язання проблеми використання штучного інтелекту в кіберпросторі завдяки правовому регулюванню розширюється до транснаціональних масштабів. Стає очевидним, що цей процес має досягти позитивних результатів не лише з огляду на новітні технічні досягнення, а із залученням даних соціальних і гуманітарних наук.

Методологічна позиція полягає в тому, що правове регулювання штучного інтелекту, який швидко поширюється в кіберпросторі, – це не лише законодавчий акт і формальна нормативна регламентація, а інтегроване поняття, що містить як юридичні, цифрові й військові характеристики, так і закономірності етики, філософії, принципи моральної відповідальності, аналіз даних соціології та психології, постулати правової аксіології та заходи правової політики. Міждисциплінарний підхід до розв'язання досліджуваної проблеми втілено в сучасній політиці Європейського Союзу, що дає змогу розглянути її в різних вимірах, визначити стратегічні напрями, однакові для всіх держав Європи, виявити дієві механізми її комплексного вирішення та закріпити їх у нормативно-правових актах.

Необхідність у створенні системи управління ризиками та кіберзагрозами в умовах війни зумовлює доцільність застосування ризико-зорієнтованого підходу для правового регулювання порядку використання технологій штучного інтелекту. Цей підхід використовують у нормативно-правових документах ЄС, зокрема у сфері розвитку кібербезпеки та захисту персональних даних. Для визначення стратегічних напрямів правової бази значущості набуває методологічний підхід, заснований на оцінці ризику (Bart, 2021; Corbet, 2021).

У роботі застосовано систему методів наукового пізнання, зокрема загальнонаукові (аналіз і синтез, індукція та дедукція, абстрагування та конкретизації, аналогії та узагальнення), спеціальні (формально-юридичний, порівняльно-правовий, герменевтичний).

Герменевтичний метод застосовувався під час тлумачення наукових понять теорії права і положень чинного законодавства. Метод дедукції надав можливість на підставі аналітичного огляду позицій науковців сформулювати загальний висновок щодо визначення стратегічних напрямів і змісту правового регулювання з питань штучного інтелекту в умовах війни. Метод індукції використано для освоєння міжнародного досвіду правового регулювання процесом використання штучного інтелекту та його застосування з урахуванням етичних принципів, правил і методів контролю над впровадженням новітніх цифрових технологій у кіберпросторі.

Формально-логічний метод сприяв розкриттю змісту положень закордонних і вітчизняних нормативно-правових актів, що стосуються запобігання проблем, пов'язаних з ризиками використання штучного інтелекту.

За допомогою порівняльно-правового методу проведено компаративний аналіз і виявлено особливості законодавчого регулювання штучного інтелекту в кіберпросторі провідних країн світу, розглянуто правові інструменти збереження кібербезпеки в умовах війни, які можуть бути інкрустовані до законодавства України.

До нормативної бази дослідження належать акти Європейського парламенту, рекомендації Європейської комісії, нормативно-правові акти країн світу та України, що регулюють правові відносини, які виникають у зв'язку із застосу-

ванням штучного інтелекту в кіберпросторі. Аналіз нормативно-правової бази свідчить про наявність у законодавстві ЄС необхідних правових засад і механізмів регулювання цифрової трансформації та розвитку технологій штучного інтелекту, зокрема в умовах збройного конфлікту.

Результати обговорення

Аналіз останніх досліджень і публікацій свідчить, що проблемні питання стосовно використання штучного інтелекту під час воєнних дій неабияк цікавлять сучасних дослідників. У наукових і політичних дискусіях навколо кібервійн і кіберзлочинності, кіберзагроз і кіберризиків, висловлюються побоювання щодо кібернетичної приреченості сучасної дійсності. Так, львівські дослідники В. Глотов, М. Фис, В. Колесніченко, А. Гуніна у своїй монографії (2022) порушили актуальне питання застосування БПЛА у воєнний час. Автори здійснили аналіз використання БПЛА у воєнних цілях, розглянули технологію їх використання для створення великомасштабних фото- і топографічних планів, а також дослідили застосування технології штучного інтелекту для створення масштабних фото- і топографічних планів.

Теоретико-методологічні засади використання штучного інтелекту для оптимізації слідчої та судової діяльності в умовах воєнного стану окреслили у своїй праці А. Ідлер і С. Куло (2021). Дослідники запропонували криміналістичні рекомендації щодо запровадження висвітлених теоретичних основ у практику правозастосування.

Особливої уваги вчених варті проблеми, принципи, механізми та правила правового регулювання штучного інтелекту, окреслені в положеннях Регламенту Європейського парламенту та Ради Європи (Pylypchuk, Baranov, & Hyliaka, 2022).

У вітчизняних дослідженнях здійснено спробу віднайти баланс у взаємодії між людиною та штучним інтелектом. З цих позицій пропонують моделі правового регулювання питань з використання новітніх технологій штучного інтелекту, розробляють державно-правові гарантії захисту прав, свобод і кібербезпеки людини (Baranov, 2019; Matuielene, Shevchuk, & Baltrunene, 2022; Tokarieva, & Savliva, 2021).

У контексті цієї роботи мають велику вагу філософські міркування Джеймса Джонсона з Університету Абердін у праці «Штучний інтелект і бомба» (2023), у якій автор окреслив ядерні стратегії в епоху цифрових технологій, висловив припущення щодо можливості розгортання сценарію ядерної війни в Східнокитайському морі 2025 року. Такі передбачення спричинені розвідувальними даними США та Китаю, керованими штучним інтелектом. Ідеться про помилки програми, схильність штучного інтелекту до гіпербол і небезпеку ситуації, за якої люди починають вірити, що машини «думають».

У книзі «Командир штучного інтелекту: командування кентаврів, командування та етичні дилеми» Дж. Джонсон (2024) називає ядерну війну з використанням штучного інтелекту небезпечною алгоритмізованою грою в «курку». У публікаціях Оксфордського університету також окреслено погляди Дж. Джонсона (2023) на ризики технологій штучного інтелекту за воєнного часу та висвітлено правові засади їх мінімізації.

Американський вчений Герберт Лін зазначає, що кібербезпека – це нескінченна боротьба. Міжнародний авторитет ученого у військовій сфері підсилюється тим, що Г. Лін брав участь у створенні новітніх технологій штучного інтелекту для навчання солдат, а також нових систем, які працюють у мережі 5G та забезпечують роботу приладів з тривимірними картами місцевості (від компанії Agile Acquisition Response) на цифрових тренувальних майданчиках. На допомогу тестуванню нових мінометів Г. Лін запропонував інноваційний софт, у якому поєднано реальну, віртуальну, доповнену та змішану реальності. Для прикладу: оскільки сучасна повітряна оборона в системах симуляції дозволяє моделювати вплив пожеж, задимлення та інших явищ, які супроводжують бойові дії, то замість звичайного ведення бойових дій за умов залпового вогню командири мають можливість оцінити успішність віртуальної атаки та досягти її мети.

Відтак проблема правового врегулювання штучного інтелекту стосується збереження кібербезпеки не лише в окремих країнах, а має загальносвітове значення, що свідчить про актуальність її дослідження.

Метою статті є розкриття етико-філософського аспекту міжнародного досвіду правового врегулювання загроз штучного інтелекту воєнним діям і визначення стратегічних перспектив державно-правової політики щодо його впровадження в реаліях воєнного часу.

Розвиток технологій штучного інтелекту в галузі кібербезпеки як сфери правового регулювання передбачає передусім визначення правосуб'єктності штучного інтелекту, сутності права на відтворення масиву інформації, баз даних і їх захисту. Так, у правовому аспекті занепокоєння викликало повідомлення щодо активного застосування технології розпізнання обличчя Clearview AI. Згідно з даними Міністерства цифрової трансформації, від початку повномасштабного вторгнення інструментом Clearview AI користується понад 900 осіб із семи державних органів. Крім того, для ідентифікації російських воєнних злочинців здійснено понад 100 тисяч пошукових запитів. Програму використовують також на блокпостах і пропускних пунктах, що зумовлює необхідність розв'язання питань щодо можливості порушення гарантій захисту персональних даних у разі здійснення такої діяльності.

На жаль, відповідальність за некоректну роботу штучного інтелекту станом на сьогодні в нашій державі нормативно не закріплена. Відтак, відсутність правового регулювання потребує здійснення певних дій, наприклад, виявити причинно-наслідкові зв'язки, які зумовили правопорушення в кіберпросторі, встановити момент його дії, проаналізувати обставини в кожному окремому випадку, визначити відповідальну особу, адже причинами кіберзлочинності можуть бути недоліки самої програми, що спричиняє відповідальність її розробника; некоректне використання програми, що зумовлює відповідальність користувача за такі дії; втручання третіх осіб, які пошкодили або зламали програму.

Варто зауважити, що у США, країнах ЄС, Японії поступово здійснюється врегулювання правових процесів щодо розвитку технологій штучного інтелекту та відповідного законодавства. Тому доцільно освоїти міжнародний досвід і на його підставі розробити стратегію та правила застосування новітніх цифрових технологій в умовах воєнного часу, зокрема у сфері кібербезпеки.

Деякі фахівці пропонують брати за основу концепції правової охорони результатів, створених штучним інтелектом, і правове регулювання баз даних. Науковці беруть до уваги ідеї ядерного стримування та примусу часів холодної війни. Як результат, створено теорію кіберстримування кібератак і контратак, які відбуваються поза колом людського зору з блискавичною швидкістю.

Проте реальність кібернетичних операцій не завжди відповідала цим очікуванням. У цьому аспекті варто згадати події «ідеального шторму», що проводила американська кібернетична кампанія Stuxnet, діяльність якої стала на перешкоді іранській програмі збагачення ядерного палива, операції «Освітлена симфонія», проведеної кіберкомандуванням США, та заподіяння шкоди діяльності «фабрики тролей» Internet Research Agency, пов'язаної з РФ.

У Міністерстві оборони США розроблено нову «Кіберстратегія–2023», яка відрізняється від попередніх стратегій орієнтацією на кіберреалізм і повсякденну дійсність кібероперацій. Нова кіберполітика США заперечує сторінку «кібер Перл-Харбору», що ґрунтувалася на значному збільшенні сил американських кібервійськ. Якщо підґрунтя минулих стратегій складали концепції стримування в кіберпросторі (2015) та «випереджального захисту» (2018), проведення атакуючих кібероперацій, демонстрація військового потенціалу та нарощування сил кібервійськ, то нова кіберстратегія США спрямована переважно на концепцію проведення кампаній.

Стратегічна конструкція кампаній передбачає проведення послідовних військових дій для досягнення цілей протягом певного часу, наприклад, небойові заходи – навчання, операції щодо забезпечення свободи навігації. Заплановано здійснювати такі види діяльності, як здобуття цифрової інформації щодо кіберзагроз, руйнування та знищення шкідливих кіберсуб'єктів за допомогою передового захисту, досягнення цілей об'єднаних сил завдяки демонстрації своїх кіберможливостей. Відтак жоден з цих видів діяльності не є актом війни, а є складовою загального фону міждержавного протистояння.

І хоча в Стратегії зауважено, що США будуть зміцнювати норми відповідальної поведінки в кіберпросторі, однак самі норми, на жаль, залишаються невизначеними. Тому Збройні Сили США планують оприлюднити нову доктрину, яка міститиме використання штучного інтелекту та квантових обчислень. Передбачено, що третина армії, яка буде роботизована в штучний інтелект, має змінити перебіг війни.

Американський генерал М. Міллі переконаний у необхідності роботизації сучасних збройних сил світу як пріоритетної тенденції здобуття перемоги над ворогом. Також він вважає, що робототехніці належатиме провідна роль у безпілотних літальних апаратах, безпілотних морських суднах і безпілотних наземних транспортних засобах. На його думку, найближчим часом навіть безпілотні військово-повітряні сили та військово-морський флот буде «без матросів, а танк – без екіпажу».

Існує певна небезпека від використання штучного інтелекту під час воєнних дій, а саме: по-перше, небезпека полягає в тому, що особи, які ухвалюють рішення, можуть надмірно покладатися на штучний інтелект як частину командування та контролю над озброєнням, оскільки він працює зі швидкістю, яка значно перевищує швидкість людей; по-друге, занепокоєння викликає те, що штучний інтелект може спричинити набуття інформації для терористів і шахраїв щодо розсекречення місць розташування зброї та боєприпасів, створення брудних бомб й інших смертоносних пристроїв. Причому значну їх кількість зберігають приватні компанії, які можуть бути вразливими для шпигунства, керованого штучним інтелектом.

Проте основне завдання використання штучного інтелекту полягає в тому, щоб зробити війну менш смертоносною, посилити її стримування, підвищити ефективність техніки для врятування життя людей. З цих позицій відоме американське видання Foreign Policy інформує, що Міністерство оборони США експериментує з ботами зі штучного інтелекту, які можуть керувати модифікованими винищувачами F-16. Очевидно також, що найближчим часом підвищиться ефективність озброєних безпілотників.

Певна річ, значущим є формування нормативно-інституційного каркаса для впровадження державно-правової політики США на федеральному рівні. Правове регулювання щодо використання технологій штучного інтелекту на федеральному рівні містить низку федеральних

законів, у яких регламентовано утворення спеціалізованих інституцій.

Правове регулювання штучного інтелекту стало нагальною проблемою, яку доводиться розв'язувати регулятивним органам у країнах Європи (Німеччині, Франції, Італії, Естонії, Італії). Повноваження з напрацювання політики у цій сфері наразі здійснює Європейська комісія. За її ініціативи створено Європейський альянс зі штучного інтелекту, який охоплює понад шість тисяч стейкхолдерів і слугує платформою для публічних дискусій (Pistrakevych, 2021). У напрямі створення правової основи для ефективного використання штучного інтелекту значний вплив здійснив Європейський парламент, створивши самостійний орган Європейської ради з питань штучного інтелекту (European Artificial Intelligence Board). Перший у світі Закон про штучний інтелект (Artificial Intelligence Act) було схвалено Радою ЄС 21 травня 2024 року. У цьому документі передбачено розвиток надійного штучного інтелекту, визначення етичних стандартів, принципів, норм і правил його застосування у фізичному та віртуальному середовищі, а також рекомендації щодо використання систем автоматизованого прийняття рішень. Закон про штучний інтелект (EU AI Act) передбачає системне регулювання штучного інтелекту, запобігання ризикам його використання та є моделлю глобального врегулювання цього процесу[1].

Активну участь в імплементації Artificial Intelligence Act бере український уряд, який ухвалив рішення про запуск регуляторної «пісочниці» – sandbox – для розробників штучного інтелекту. Він складає контрольоване середовище, у межах якого компанії-розробники зможуть протягом усього періоду створення продукту враховувати вимоги майбутнього Акта Європейського Союзу. Варті уваги Рекомендації Комітету Міністрів Ради Європи державам – членам CM/Rec (2010) 4 «Про права людини стосовно військовослужбовців» (прийняті на 1077-му засіданні 24.02.2010), а також Конвенція прав людини, у якій окреслено пріоритетні підходи до функціонування військових судів, розкрито постулати забезпечення права на справедливий суд у контексті можливих порушень ст. 6 цієї Конвенції військовими судами. Упровадження в практику перспективних напрацювань нормативно-правових документів Європейського Союзу дає змогу інтегрувати основні підходи щодо функціонування правових установ і військових судів[2].

Обговоренню актуальних питань зовнішньої політики, політики оборони та безпеки, зокрема реальній загрозі з боку Росії та підвищенню здатності до оборони та стримуванню військової агресії, була присвячена 60-та Мюнхенська конференція з безпеки (Munich Security Conference), що відбулася 16–24 лютого 2024 року. Глава Єврокомісії Урсула фон дер Ляєн заявила, що українці використовують застарілу зброю та покращують її, зокрема з використанням штучного інтелекту, під час кібератак для досягнення більшої точності й ефективності. Главу Єврокомісії вразило спостереження за виробництвом безпілотників, саме тому ЄС має наміри інтегрувати Україну в Стратегію воєнної промисловості для стабілізації миру та сумісного подолання військових конфліктів.

Сполучене Королівство Великої Британії та Північної Ірландії є одним з лідерів у встановленні міжнародних стандартів у галузі штучного інтелекту, визначенні як внутрішніх, так і глобальних засад розвитку технологій майбутнього. Стратегічні напрями правового регулювання процесами, пов'язаними з впровадженням технологій штучного інтелекту, окреслено в Національній Стратегії штучного інтелекту, який підготував уряд Великої Британії (від 22 вересня 2021 року). Ця стратегія спрямована на максимальне використання досвіду та наявних ресурсів, що дозволить швидко адаптуватися до нових технологічних змін. Адаптивний підхід ґрунтується на реалізації фундаментальних принципів (безпека, прозорість, справедливість, підзвітність) як основи для розвитку штучного інтелекту та водночас підтримки безпеки й етики використання штучного інтелекту, забезпечення захисту прав людини[3].

Англійська система штучного інтелекту нараховує понад 200 стартапів і підприємств. Наразі відомий центр «Цифрова катапульта» (Digital Catapult), зосереджений на новітніх технологіях, зокрема: data-driven (конфіденційність даних, кібербезпека, технологія blockchain); immersive (технології віртуальної та доповненої реальності, тактильні технології); connected (інтернет речей, технологія зв'язку 5G, бездротові зв'язки енергетичного споживання).

Згідно з положеннями Звіту англійського уряду, впровадження штучного інтелекту містить чотири рівні: потужне управління, розширення комунікацій, розповсюдження культури штучного інтелекту в державному секторі, просування англійської екосистеми на міжнародній арені. Рекомендовано створити Раду зі штучного інтелекту, яка має бути відповідальною за координацію ініціатив у зазначеній галузі.

[1] EU AI Act: first regulation on artificial intelligence. Abgerufen am 24. Mai 2024. URL: https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/.

[2] Конвенція про захист прав людини і основоположних свобод (Європейська конвенція з прав людини) : міжнар. док. від 4 листоп. 1950 р. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text.

[3] National AI Strategy. URL: https://www.gov.uk/government/publications/national-ai-strategy/national-ai-strategy-html-version.

Варте особливої уваги міжнародної спільноти підписання 12 січня 2024 року Угоди про співробітництво у сфері безпеки між Україною та Сполученим Королівством Великої Британії та Північної Ірландії (Agreement on Security Co-operation between the United Kingdom of Great Britain & Northern Ireland and Ukraine). Міжнародна угода передбачає співпрацю в таких напрямах, як обмін розвідувальними даними, військова та медична підготовка, кібербезпека, оборонно-промислове співробітництво[1].

Для реалізації положень цієї міжнародної угоди Сполучне Королівство буде надавати «комплексну допомогу Україні із захисту та відновлення територіальної цілісності в межах міжнародно визнаних кордонів», здійснювати «активне стримування проти військової ескалації та/чи нової агресії Російської Федерації». У документі зауважено, що Велика Британія має наміри надавати «сучасне військове озброєння в доменах землі, повітря, моря, космосу та кіберпростору». Адже саме в цих вимірах тривають війни в сучасному світі.

Міжнародна співпраця у сфері кібербезпеки передбачає проведення кіберконсультацій щодо розвідки намірів російської конвенційної агресії та шпигунства шляхом підвищення кіберстійкості; галузеву підтримку для захисту ІТ-інфраструктури від кібератак; обмін розвідувальними даними щодо кібернетичної та інформаційної безпеки.

Учасники – сторони Угоди визнали необхідність виявлення, припинення та запобігання зловмисним кібероперaціям і, зокрема, зловмисному використанню кіберпотужностей Російською Федерацією та іншими ворожими державними й недержавними суб'єктами. Передбачено надання міжнародної технічної допомоги Україні для доступності сучасних технологічних рішень у сфері захисту критичної інфраструктури для суб'єктів кібербезпеки.

Планується спільна робота над упровадженням спільного протоколу стримування та реагування на кібератаки з боку Російської Федерації, її сателітів і проросійських хакерських угруповань, зокрема, переслідуючи спільні цілі стримування та створюючи механізм для оперативного надання експертних послуг у сфері кібербезпеки.

У Канаді набуває поширення державницький підхід до розвитку та використання штучного інтелекту, подібний до базових стандартів Великої Британії. Про високий рівень державницької політики щодо правового регулювання використання штучного інтелекту свідчить схвалення урядом Канади Національної стратегії ШІ (Панканадська стратегія ШІ), у якій представлено план щодо фінансування досліджень і пошуку талантів для цієї галузі. Для практичної реалізації положень Панканадської стратегії ШІ створено Консультативну раду уряду Канади з питань штучного інтелекту.

Водночас уряд Канади запропонував на розгляд парламенту комплексний федеральний законопроєкт С-27 «Про імплементацію Цифрової хартії 2022» та законопроєкт «Про штучний інтелект і дані» (AIDA).

Про вагомий міжнародний статус Канади в галузі штучного інтелекту свідчить те, що держава є співзасновником Глобального партнерства зі штучного інтелекту, яке вивчає питання досягнення миру та протидії війні у світовій спільноті.

Аналізуючи міжнародний досвід, зазначимо, що Північноатлантичний альянс (НАТО) приділяє значну увагу правовому регулюванню використання штучного інтелекту в галузі військових дій з урахуванням національних пріоритетів, а також проблемам, пов'язаним з відповідальністю за поширення цифрових технологій як загрози щодо порушення прав людини на життя та свободу. Фундаментальні цифрові технології покликані сприяти трансформації та вдосконаленню всіх сфер суспільного життя.

На підставі вивчення кращих досягнень закордонних практик, Україна, перебуваючи в умовах воєнного стану, рухається в напрямі Європейської стратегії законодавчого врегулювання штучного інтелекту, реалізації міжнародних стандартів, правил і рекомендацій. Розвиток нормативно-правової бази здійснюється на підставі прав людини та фундаментальних цінностей з орієнтацією на безпеку громадян, підприємництва та бізнесу[2].

Особливість правового регулювання процесу використання штучного інтелекту в Україні за умов воєнного часу полягає в урахуванні норм військово-адміністративного права як галузі Особливого адміністративного права з визначенням повноважень, обов'язків і відповідальності суб'єктів забезпечення кібербезпеки, зокрема тих фахівців, які працюють у сфері штучного інтелекту воєнного спрямування в системі національної безпеки.

До розв'язання проблеми правового регулювання штучного інтелекту під час війни

[1] Угода про співробітництво у сфері безпеки між Україною та Сполученим Королівством Великої Британії і Північної Ірландії від 12 січ. 2024 р. URL: https://www.president.gov.ua/news/ugoda-pro-spivrobitnictvo-u-sferi-bezpeki-mizh-ukrayinoyu-ta-88277.

[2] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions – Coordinated Plan on Artificial Intelligence (COM(2018) 795 final) / European Commission. URL: https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence.

залучено як державні органи, так і неурядові організації, дослідників та лідерів в зазначеній галузі, представників громадськості та ініціативні робочі групи. Інтегровані зусилля усіх зацікавлених сторін мають сприяти належній підготовці законодавчого забезпечення та захисту прав людей під час використання штучного інтелекту в умовах війни.

Для координації зусиль державного та приватного секторів щодо запобігання кіберінцидентам у 2015 році створено Кіберполіцію України, успішно функціонують Державна служба спеціального зв'язку та захисту інформації України, Національний координаційний центр кібербезпеки як орган РНБО, а також сформовано центри (підрозділи) забезпечення кіберзахисту в СБУ України, Міністерстві оборони України та Збройних Силах України, Національному банку України, Міністерстві інфраструктури України. Активну діяльність здійснюють Національний центр резервування державних інформаційних ресурсів і урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA.

Важливим кроком для створення умов безпечного функціонування держави стала розробка та впровадження Стратегії кібербезпеки України, яка визначає пріоритети національних інтересів у згаданій сфері, наявні та можливі кіберзагрози. У Стратегії кібербезпеки України визначено комплекс цілей, а саме: цілі формування потенціалу стримування – дієва кібероборона, ефективна протидія розвідувально-підривній діяльності в кіберпросторі та кібертероризму, ефективна протидія кіберзлочинності, розвиток асиметричних інструментів стримування; цілі набуття кіберстійкості, спрямовані на розвиток Національної кіберготовності та надійного кіберзахисту, професійне вдосконалення й кіберобізнаність суспільства, науково-технічне забезпечення кібербезпеки та безпечні цифрові послуги; цілі вдосконалення взаємодії, які зорієнтовані на зміцнення системи координації, формування нової моделі відносин у сфері кібербезпеки, прагматичне міжнародне співробітництво[1].

Реалізація цілей, поставлених у цій Стратегії для розв'язання проблеми кіберзлочинності, через свою специфіку не може бути лише внутрішньодержавною, і тому активізується розвиток міжнародного співробітництва у сфері кібербезпеки, зокрема з такими країнами, як США, Сполучене Королівство Великої Британії і Північної Ірландії, Німеччина, Королівство Нідерландів, Канада, Норвегія, Румунія, Японія. Розвиток співпраці з іноземними партнерами поглиблюється завдяки спільній діяльності з ЄС та НАТО, проведенню кібердіалогів і кібернавчання за участю міжнародних організацій.

При Раді Європи здійснюється робота Спеціального комітету зі штучного інтелекту, членом якого є Україна. На засіданнях Комітету обговорюють питання відповідальності, пов'язаної з використанням штучного інтелекту у військовому кіберпросторі.

Отже, стратегічними напрямами зовнішньої діяльності в цьому контексті є: поглиблення євроінтеграційних процесів шляхом уніфікації підходів, методів і засобів забезпечення кібербезпеки з усталеними практиками ЄС і НАТО, організація заходів, спрямованих на посилення кіберстійкості України, розвиток спроможностей національної системи кібербезпеки та захист національних інтересів у кіберпросторі[2]. З цих позицій в Україні започатковано проведення щорічного заходу – місяця кібербезпеки.

Відомства зовнішніх справ співпрацюють з іншими уповноваженими органами над удосконаленням нормативно-правової бази у сфері кібербезпеки «шляхом впровадження норм міжнародних стандартів, а також стандартів ЄС та НАТО у сфері кібербезпеки». У п. 14 Плану дій до Стратегії подано перелік заходів зі зміцнення міжнародного співробітництва, у якому йдеться про «утворення спільних двосторонніх або багатосторонніх груп для здійснення розслідувань кіберзлочинів, а також проведення спільних операцій, обміну інформацією та досвідом».

Виконання окреслених стратегічних напрямів здійснюють суб'єкти Національної системи кібербезпеки, Міністерство закордонних справ України, Міністерство цифрової трансформації України, Міністерство освіти і науки України та інші суб'єкти забезпечення кібербезпеки в межах їхньої компетенції. Координатором практичної реалізації визначених стратегічних напрямів є робочий орган Ради національної безпеки і оборони України – Національний координаційний центр кібербезпеки.

Проте залишаються невирішеними питання розробки концептуальних підходів щодо реалізації державної політики у сфері забезпечення прав громадян у кіберпросторі, оперативного обміну інформацією про кіберзагрози, правового регулювання щодо застосування штучного інтелекту зі стримування деструктивної діяльності в кіберпросторі та запобігання зловживанню новими цифровими технологіями.

Водночас зазначимо, що в Україні вже було зроблено певні кроки для створення правового регулювання в галузі штучного інтелекту. Так, у Розпорядженні Кабінету Міністрів України від 02.12.2020 № 1556-р було схвалено Концепцію

[1] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серп. 2021 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013.

[2] Там само.

розвитку штучного інтелекту в Україні, у якій на законодавчому рівні визначено мету, завдання та принципи її розвитку.

Позитивним кроком в окресленому напрямі є підписання в липні 2023 року в межах саміту НАТО у Вільнюсі Спільної декларації країн – членів Group of 7, основу якої складає проєкт Київського договору з безпеки (Kyiv Security Compact), розроблений міжнародною експертною групою. Ця декларація є документом, що свідчить про надання країнами G-7 довгострокових гарантій безпеки та економічної підтримки України, спрямованими на забезпечення стійких сил, здатних захищати Україну, зокрема підтримку ініціативи з кіберзахисту для протидії гібридним загрозам. До зазначеної декларації приєдналися вже 30 держав. Подібні домовленості є взірцем, який додає впевненості під час захисту країни та фіксує сильні безпекові позиції на весь період до вступу України в НАТО.

У відповідь на агресивну війну Росії Міністерство закордонних справ України спільно з міжнародними партнерами з Канади, Данії, Естонії, Франції, Німеччини, Нідерландів, Польщі, Швеції, Великої Британії та Сполучених Штатів Америки в травні 2023 року започаткували новий інструмент співпраці в кіберпросторі. Десять країн – союзників України об'єдналися з метою створення Талліннського механізму, який має допомогти державі із самообороною в кіберпросторі на тлі протидії російській агресії. Механізм включає естонський фронт-офіс у Києві та польський бек-офіс у Варшаві. У межах Талліннського механізму здійснюватиметься координація допомоги Україні для підтримки та зміцнення її кібербезпеки, кіберстійкості, кіберзахисту критичної інфраструктури країни та попередження російських кібероперацій. Діяльність механізму відбувається з дотриманням норм міжнародного права[1].

Особливої уваги варте створення в Національній асоціації адвокатів України робочої групи з правового регулювання штучного інтелекту, яка займається аналізом важливих юридичних питань розвитку штучного інтелекту, визначення меж його використання в різних галузях, а також захистом персональних даних, зібраних системами штучного інтелекту, формулювання правил щодо їх збереження та застосування.

За воєнного часу розвиток українського виробництва дронів є одним з ключових пріоритетів нашої держави. У цьому аспекті Україна має реальну можливість розробити рішення світового рівня. У зв'язку з цим Кабінет Міністрів України виділив значну фінансову допомогу для інвестування у виробництво БПЛА та розробку програмного забезпечення штучного інтелекту, які працюють без наведення GPS. З цих позицій авторитетні військові висловлюють думку, що майбутнє війни будуть диктувати безпілотники, які матимуть вирішальну роль у розмінуванні простору та формуванні зграй БПЛА-камікадзе (Mosov, & Khoroschylova, 2018).

Проте експерти у сфері кібербезпеки зазначають, що після розробки відповідного програмного забезпечення для безпілотників зі штучним інтелектом, його розповсюдження може стати фактично безплатним. Тим самим недержавні організації, зокрема терористичні, зможуть отримати й змінити їх призначення. Такої думки дотримується американський експерт Пол Шарр. Тому існує розбіжність: з одного боку розповсюдження технологій штучного інтелекту є необхідністю в боротьбі за виживання українців, з іншого, є зворотна сторона – загроза для майбутнього.

Крім того, на часі постала проблема збирання доказів і розслідування воєнних кіберзлочинів. У цьому контексті науковий інтерес становлять праці О. Дуфенюк (2022), Ю. П. Тимошенко (2022).

Дослідники акцентують на значенні технологій штучного інтелекту, які використовують у таких аспектах, як: використання безпілотників для проведення військових операцій і протидії незаконному обігу вогнепальної зброї; збирання доказової інформації в умовах війни та ведення бойових дій з метою фіксування воєнних злочинів; аналіз супутникових знімків для виявлення змін ландшафту; аналіз відеоматеріалів, зроблених на місцях воєнних злочинів; запобігання правопорушенням з використанням інтелектуальних систем безпеки; опрацювання аудіо- та відеоматеріалів для ідентифікації голосів і місця знаходження абонентів; розпізнавання обличчя для виявлення підозрюваних, причетних до воєнних правопорушень; аналіз текстової інформації для встановлення винних і притягнення їх до відповідальності, а також аналіз даних медичних закладів для визначення причин смерті й ідентифікації жертв воєнних злочинів (Zhuravel, Konovalova, & Avdeyeva, 2021).

Використання штучного інтелекту має певні виклики й обмеження, серед яких: складність добути достовірну інформацію через екстремальність ситуації; ризик у разі переслідування політичних опонентів або некоректного відображення даних; законодавчі обмеження щодо застосування штучного інтелекту під час розслідування злочинів. Європейський вектор розвитку нормативно-правових засад у галузі криміналістики та судової експертизи в Україні, який передбачає застосування міжнародних стандартів доказування під час розкриття воєнних кіберзлочинів, свідчить про становлення в країні цифрової криміналістики

[1] As endorsed by Canada, Denmark, Estonia, France, Germany, The Netherlands, Poland, Sweden, United Kingdom, United States on 30 May, 2023. URL: https://mfa.gov.ua/storage/app/sites/1/tm-mission-statement.pdf.

(Karmaza & Fedorenko, 2021; Matuielene, Shevchuk, & Baltrunene, 2022; Tymoshenko et al., 2022).

Освоєння міжнародного досвіду використання технологій штучного інтелекту в реаліях воєнного часу має прискорити процес розслідування воєнних злочинів і кіберзлочинів, що сприятиме перемозі справедливості, притягненню винних до відповідальності. Завдяки застосуванню цифрових слідів як джерела кримінально значущої інформації та основи доказової бази, стає очевидною ефективність створення «слідової картини», зокрема в разі аналізу фактів і під час розслідування кримінальних правопорушень. Адже саме в цифрових слідах, які залишаються у віртуальному просторі, незмінним є цифрове кодування інформації.

Слід зазначити, що штучний інтелект може спричинити нові етичні та юридичні проблеми, пов'язані з відповідальністю за кіберзлочини або потенційно упередженим прийняттям рішень. Тому використання міжнародного досвіду, зокрема напрацювань, висвітлених у нормативно-правових актах Європейської етичної Хартії із застосування штучного інтелекту в судових системах (2018) та Резолюції Європейського парламенту з рекомендаціями Комісії щодо норм цивільного права з робототехніки (2017), має забезпечити впровадження цифрових технологій у межах відповідної правової бази, яка сприятиме введенню інновацій згідно з фундаментальними цінностями, правами громадян й етичними принципами.

Однак у зв'язку з можливістю ризикованих випадків використання технологій штучного інтелекту, завдяки яким створюється небезпека, слід висувати вимоги щодо подолання реальних загроз, підвищення безпеки, протидії кіберзлочинності й тероризму. Тим самим має відбуватися допомога органам правопорядку відстежувати застосовані кіберзлочинцями технології та способи транскордонної злочинної діяльності. Як показав час, необхідним є збирання доказів воєнних кіберзлочинів, що зумовило необхідність поширення застосування технологій штучного інтелекту з метою виявлення, документування та розслідування кіберзлочинів проти людства й геноциду, притягнення винних до відповідальності за вчинене.

З огляду на викладене вище, зазначимо, що для запобігання нелегальному використанню штучного інтелекту, варто створити глобальну міжнародну законодавчу базу з розробки та впровадження новітніх цифрових технологій за воєнного часу.

Висновки

Розвиток правового регулювання штучного інтелекту в Україні зорієнтований на виклики сучасних воєнних реалій. У цьому напрямі в різних країнах світу державні правові установи спільно з бізнес-структурами працюють над створенням адаптованих і ефективних правових норм, що враховують особливості розробки та функціонування штучного інтелекту. Це дозволить забезпечити кібербезпеку та захист прав і свобод людей, створити сприятливий кіберпростір для розвитку інновацій і цифрової економіки, відновлення країни.

З огляду на міжнародний досвід варто визначити такі стратегічні перспективи правового регулювання загроз штучного інтелекту та протистоянню війні, як: проведення кампаній, кібероперацій і небойових заходів щодо забезпечення свободи навігації, руйнування та знищення шкідливих кіберсуб'єктів; використання міждисциплінарного, адаптивного та ризико-зорієнтованого підходів до нових технологічних змін на підставі фундаментальних принципів безпеки, прозорості, справедливості, підзвітності; визначення етичних стандартів, норм і правил застосування штучного інтелекту у фізичному та віртуальному середовищі; роботизація армії та зміцнення кадрового потенціалу високотехнологічного спрямування; поєднання наукового, університетського та промислового секторів для оптимізації розвитку технологій штучного інтелекту, створення інноваційних центрів із залученням приватного бізнесу; міжнародний обмін розвідувальними даними, досвідом військового вишколу в галузі кібербезпеки, проведення кіберконсультацій щодо розвідки намірів конвенційної агресії та шпигунства шляхом підвищення кіберстійкості; надання міжнародної технічної допомоги й експертних послуг Україні для доступності сучасних технологічних рішень у сфері захисту критичної інфраструктури для суб'єктів кібербезпеки; забезпечення необхідної правової визначеності та відповідальності за поширення цифрових технологій як загрози щодо порушення прав людини на життя та свободу, зміцнення норм відповідальної поведінки в кіберпросторі; створення контрольованого середовища та проведення експертної оцінки безпеки всіх провайдерів ШІ-сервісів з отриманням адміністративного дозволу для запобігання можливих зловживань.

З огляду на те, що Україна стала країною-кандидатом до членства в Європейському Союзі, передбачено, що в майбутньому наше законодавство у сфері правового регулювання штучного інтелекту буде відповідати стандартам, стратегічним напрямам і нормативно-правовим актам європейського законодавства.

Правове регулювання штучного інтелекту в Україні має забезпечити збалансований підхід до використання технологій штучного інтелекту під час війни, захист прав громадян і підтримку для цивілізаційного відновлення країни.

Використання штучного інтелекту в умовах воєнного часу має виступати як високотехнологічна допомога встановленню світового порядку в кіберпросторі.

Зважаючи на міжнародний досвід і сучасну воєнну практику для запобігання нецивільному застосуванню штучного інтелекту, доцільно сформувати глобальну (міжнародну) законодавчу базу з розробки та впровадження цифрових технологій з урахуванням їх недосконалості, загроз для порушення прав людини, небезпеки кіберзлочинів.

Поєднання зусиль міжнародної спільноти, зокрема дослідників і розробників у галузі штучного інтелекту та регламентування їх діяльності, ініціатива організацій громадянського суспільства, робочих груп сприятиме гармонізації політики в царині цифрових технологій, підготовці належного законодавчого забезпечення та захисту прав і свобод людей від воєнної агресії.

Перспективи подальших досліджень в окресленому напрямі полягають у встановленні гарантій щодо дотримання прав людини у воєнний і мирний час. Наукові дослідження також доцільно спрямувати на розв'язання проблеми використання технологій штучного інтелекту в правоохоронній діяльності та правосудді з огляду на міжнародний досвід і реалії воєнного часу.

References

[1] Baranov, O.A. (2019). Legal aspects of national strategies for the development of artificial intelligence. *Legal Ukraine*, 7, 25-29.

[2] Bart, V.B. (2021). Europese Unie neemt de leiding in regulering van AI. *SIRIUS.LEGAL*. Retrieved from https://siriuslegaladvocaten.be/europese-unie-neemt-de-leiding-in-regulering-van-ai.

[3] Corbet, R. (2021). The EUs new Regulation on Artificial Intelligence. *ARTHUR COX.* Retrieved from https://www.arthurcox.com/knowledge/the-eus-new-regulation-on-artificial-intelligence/.

[4] Dufeniuk, O. (2022). Investigation of war crimes in Ukraine: challenges, standards, innovations. *Baltic Journal of Legal and Social Sciences*, 1, 46-56. doi: 10.30525/2592-8813-2022-1-6.

[5] European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment (2018). Adopted at the 31st plenary meeting of the CEPEJ. *Council of Europe.* Retrieved from https://rm.coe.int/ethical-charter-en-for-publication-4-december- 2018/16808f699c.

[6] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2018). *Official Journal of the European Union,* 239-257. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX-:52017IP0051&rid=9.

[7] Hlotov, V.M., Fys, M.M., Kolesnichenko, V.B., & Hunina, A.V. (2022). *Use of UAVs in military affairs and aerial photography.* Lviv: Lviv. politekhnika. Retrieved from https://vlp.com.ua/node/20709.

[8] Idder, A., & Coulaux, S. (2021). Artificial intelligence in criminal justice: invasion or revolution? *International Bar Association.* Retrieved from https://www.ibanet.org/dec-21-aicriminal- justice.

[9] Johnson, J. (2023). *Nuclear Strategy and Risk in the Digital Age.* Oxford University Press. Retrieved from https://warontherocks.com/2023/09/nuclear-brinkmanship-in-ai-enabled-warfare-a-dangerous-algorithmic-game-of-chicken.

[10] Johnson, J. (2023). *AI and the Bomb.* Oxford Scholarschip Online. Retrieved from https://global.oup.com.

[11] Johnson, J. (2024). *The AI Commander: Centaur Teaming, Command, and Ethical Dilemmas.* Oxford University Press. Retrieved from https://nuclear-brinkmanship-in-ai-enabled-warfare-a-dangerous-algorithmic-game-of-chicken 10.

[12] Karmaza, O.O., & Fedorenko, T.V. (2021). Principles of artificial intelligence in the justice system of Ukraine. *Law and society*, 2, 18-24. doi: 10.32842/2078-3736/2021.2.3.

[13] Kryvytskyi, Yu.V. (2021). Artificial intelligence as a tool of legal reform: potential, trends and perspectives. *Scientific Bulletin of the National Academy of Internal Affairs,* 2(119), 90-101. doi: 10.33270/01211192.90.

[14] Matuielene, S., Shevchuk, V., & Baltrunene, Yu. (2022). Artificial intelligence in law enforcement and justice: domestic and European experience. *Theory and practice of forensic examination and criminology*, 4(29), 12-46. doi: 10.32353/khrife.4.2022.02.

[15] Milli, M. (2023). A third of the army will be robotic, and artificial intelligence will change the course of wars. Retrieved from https://www.radiosvoboda.org/a/viyna-roboty-shtuchnyy-intelekt/32486834.html.

[16] Mosov, S.P., & Khoroshylova, S.Y. (2018). Peculiarities of the use of strategic unmanned reconnaissance aircraft in military conflicts of the XXI century. *Collection of scientific works of the Center for Military and Strategic Studies of the National Defense University of Ukraine named after Ivan Chernyakhovsky*, 2(63), 104-109. Retrieved from http://nbuv.gov.ua/UJRN/Znpcvsd_2018_2_19.

[17] Pistrakevych, O.V. (2021). Strategies for the development of artificial intelligence in the European Union (on the example of the countries of the Visegrad Group). *International relations, public communications and regional studies,* 1(9), 160-173. Retrieved from https://elibrary.kubg.edu.ua/id/eprint/39141/1/O_Pistrakevych.

[18] Pylypchuk, V.H., Baranov, O.A., & Hyliaka, O.S. (2022). Problems of legal regulation in the field of AI in the context of the development of EU legislation. *Bulletin of the National Academy of Legal Sciences of Ukraine*, 2, 35-62. doi: 10.37635/jnalsu.29 (2).2022.35-62.

[19] Tokarieva, K.S., & Savliva, N.O. (2021). Peculiarities of legal regulation of artificial intelligence in Ukraine. *Scientific Works of National Aviation University,* 3(60), 148-153. doi: 10.18372/2307-9061.60.15967.
[20] Tymoshenko, Y.P., Kozachenko, O.I., Kyslenko, D.P., Horodetska, M.S., Chubata, M.V., & Barhan, S.S. (2022). Latest technologies in criminal investigation (testing of foreign practices in Ukraine). *Amazonia Investiga,* 11(51), 149-160. doi: 10.34069/ AI/2022.51.03.14.
[21] Zhuravel, V.A., Konovalova, V.E., & Avdeyeva, G.K. (2021). Reliability Evaluation of a Forensic Expert's Opinion: World Practices and Ukrainian Realities. *Journal of the National Academy of Legal Sciences of Ukraine,* 28(2), 252-261. doi: 10.37635/ jnalsu.28(2).2021.252-261.

Список використаних джерел

[1] Баранов О. А. Правові аспекти національних стратегій розвитку штучного інтелекту. *Юридична Україна.* 2019. № 7. С. 25—29.
[2] Bart V. B. Europese Unie neemt de leiding in regulering van AI. *SIRIUS.LEGAL*. May 5, 2021. URL: https://siriuslegaladvocaten.be/europese-unie-neemt-de-leiding-in-regulering-van-ai.
[3] Corbet R. The EU's new Regulation on Artificial Intelligence. *ARTHUR COX.* May 06, 2021. URL: https://www.arthurcox.com/knowledge/the-eus-new-regulation-on-artificial-intelligence/.
[4] Дуфенюк О. Розслідування воєнних злочинів в Україні: виклики, стандарти, інновації. *Baltic Journal of Legal and Social Sciences.* 2022. № 1. С. 46–56. doi: 10.30525/2592-8813-2022-1-6.
[5] European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment. Adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3–4 December 2018) / Council of Europe. URL: https://rm.coe.int/ethical-charter-en-for-publication-4-december- 2018/16808f699c.
[6] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). *Official Journal of the European Union.* 2018. P. 239–257. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX-:52017IP0051&rid=9.
[7] Глотов В. М., Фис М. М., Колесніченко В. Б., Гуніна А. В. Застосування БПЛА у військовій справі та аерозніманні : монографія. Львів : Львів. політехніка, 2022. 196 с. URL: https://vlp.com.ua/node/20709.
[8] Idder A., Coulaux S. Artificial intelligence in criminal justice: invasion or revolution? *International Bar Association.* 2021. URL: https://www.ibanet.org/dec-21-aicriminal- justice.
[9] Johnson J. AI and the Bomb. Oxford Scholarschip Online, 2023. 288 p. URL: https://global.oup.com.
[10] Johnson J. Nuclear Strategy and Risk in the Digital Age. Oxford University Press, 2023. URL: https://warontherocks.com/2023/09/nuclear-brinkmanship-in-ai-enabled-warfare-a-dangerous-algorithmic-game-of-chicken.
[11] Johnson J. The AI Commander: Centaur Teaming, Command, and Ethical Dilemmas. Oxford University Press, 2024. URL: https://nuclear-brinkmanship-in-ai-enabled-warfare-a-dangerous-algorithmic-game-of-chicken.
[12] Кармаза О. О., Федоренко Т. В. Принципи штучного інтелекту в правосудді України. *Право і суспільство.* 2021. № 2. С. 18–24. doi: 10.32842/2078-3736/2021.2.3.
[13] Кривицький Ю. В. Штучний інтелект як інструмент правової реформи: потенціал, тенденції та перспективи. *Науковий вісник Національної академії внутрішніх справ.* 2021. № 2 (119). С. 90–101. doi: 10.33270/01211192.90.
[14] Матуєлене С., Шевчук В., Балтрунене Ю. Штучний інтелект в діяльності органів правопорядку та юстиції: вітчизняний та європейський досвід. *Теорія та практика судової експертизи і криміналістики.* 2022. Вип. 4 (29). С. 12–46. doi: 10.32353/khrife.4.2022.02.
[15] Міллі М. Третина армії буде роботизована, а штучний інтелект змінить хід воєн. URL: https://www.radiosvoboda.org/a/viyna-roboty-shtuchnyy-intelekt/32486834.html.
[16] Мосов С. П., Хорошилова С. Й. Особливості застосування стратегічної безпілотної розвідувальної авіації у воєнних конфліктах XXI століття. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. 2018. № 2 (63). С. 104–109. URL: http://nbuv.gov.ua/UJRN/Znpcvsd_2018_2_19.
[17] Пістракевич О. В. Стратегії розвитку штучного інтелекту в європейському союзі (на прикладі країн Вишеградської групи). *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2021. № 1 (9). С. 160–173. URL: https://elibrary.kubg.edu.ua/id/eprint/39141/1/O_Pistrakevych_IRPCRS_1%289%29_2021.pdf.
[18] Пилипчук В. Г., Баранов О. А., Гиляка О. С. Проблеми правового регулювання у сфері ШІ в контексті розвитку законодавства ЄС. *Вісник Національної академії правових наук України.* 2022. № 2. С. 35–62. doi: 10.37635/jnalsu.29(2).2022.35-62.

[19] Токарєва К. С., Савліва Н. О. Особливості правового регулювання штучного інтелекту в Україні. *Наукові праці Національного авіаційного університету.* 2021. Вип. 3 (60). С. 148–153. doi: 10.18372/2307-9061.60.15967.
[20] Tymoshenko Y. P., Kozachenko O. I., Kyslenko D. P., Horodetska M. S., Chubata M. V., Barhan S. S. Latest technologies in criminal investigation (testing of foreign practices in Ukraine). *Amazonia Investiga.* 2022. Vol. 11. No. 51. P. 149–160. doi: 10.34069/AI/2022.51.03.14.
[21] Zhuravel V. A., Konovalova V. E., Avdeyeva G. K. Reliability Evaluation of a Forensic Expert's Opinion: World Practices and Ukrainian Realities. *Journal of the National Academy of Legal Sciences of Ukraine*. 2021. Vol. 28. No. 2. P. 252–261. doi: 10.37635/ jnalsu.28(2).2021.252-261.

International Experience of Legal Regulation of the Danger of Artificial Intelligence in the Realities of Wartime: the Ethical and Philosophical Aspect

SOVA Marharyta
Doctor of Pedagogic, Professor,
Professor of the Department of Psychology, Pedagogy and Social Disciplines
of the State Tax University
Irpin, Ukraine
ORCID: https://orcid.org/0000-0002-3190-7903;
DIENIZHNA Svitlana
PhD in Pedagogic, Associate Professor,
Associate Professor of the Department of Psychology, Pedagogy and Sociology
of the State Tax University
Irpin, Ukraine
ORCID: https://orcid.org/0009-0009-4671-2162

Abstract. It is argued that the study of the international experience of legal regulation of threats of artificial intelligence in cyberspace during wartime is an actual direction of scientific research that deserves an in-depth and systematic study. The purpose of the article is to reveal the ethical and philosophical aspect of the international experience of the legal regulation of artificial intelligence threats to military actions and to determine the strategic directions of state and legal policy regarding its implementation in the realities of wartime. To carry out the research, a system of methods of scientific knowledge was applied, namely: philosophical, general scientific (analysis and synthesis, induction and deduction, abstraction and concretization, analogy and contrast); private methods of scientific knowledge used in many branches of science (comparative, quantitative and qualitative analysis); special-legal (formal-legal, comparative-legal, systemic-structural). The content of the article analyzes the international experience of legal regulation of the use of artificial intelligence technologies in conditions of global threats; the priority orientations of the domestic state and legal policy regarding the prevention of the risks of using artificial intelligence as tools of military danger are highlighted; perspective directions for improving the legal regulation of the use of digital technologies under martial law through the prism of integration processes are outlined. It was found that the implementation of the international experience of legal regulation of the danger of using artificial intelligence during war should take place in the context of European integration processes and be based on fundamental values and principles of the rule of law (equality of all before the law, respect for human rights, impartiality and justice), normative legal acts, standards and rules of the leading countries of the world, regardless of the challenges and restrictions associated with military circumstances. Attention is drawn to the fact that artificial intelligence is not capable of completely replacing military specialists, but its use will contribute to reducing the risks of danger to people's lives and health, optimizing the activities of military personnel for the sake of establishing peace and justice on the planet. It is substantiated that during the wartime in Ukraine, the question of increasing the effectiveness of the investigation of cybercrimes due to the use of artificial intelligence technologies arose acutely. The novelty of the research consists in determining the strategic directions of legal regulation of the danger of using artificial intelligence technologies during wartime on the basis of international experience and in accordance with European regulations, principles of international law, standards and recommendations of the leading countries of the world. The conclusions state that the legal regulation of the use of artificial intelligence in Ukraine should be

carried out according to the European integration course chosen by the state in accordance with the standards and rules outlined in international legal documents. From these positions, the key areas of legal regulation of the threats of the use of modern digital technologies in conditions of martial law are defined. It is substantiated that among the priority directions for improving the legal regulation of the danger of artificial intelligence in the state and legal policy of Ukraine, the signing of relevant international agreements, the organization of joint events, joint campaigns, military exercises, cyber operations and cyber consultations with representatives of NATO member countries in the conditions of military conflicts are chosen. The practical significance lies in the fact that the application of international experience in the legal regulation of the danger of artificial intelligence is a factor in preventing threats and reducing risks when using modern digital technologies during war. Legal regulation of the risks of modern software should contribute to deterring war, reducing its lethality, saving people's lives, and protecting their rights and freedoms. Proposals for promising areas of scientific research on the problems of legal regulation of the use of artificial intelligence technologies in cyberspace as instruments of military threat to people's lives and peace are outlined.

Keywords: legal regulation; artificial intelligence; cyberspace; cybersecurity; cybercrime.