Загуменна Юлія Олександрівна,
професор кафедри теорії та історії держави та права Харківського національного університету внутрішніх справ, доктор юридичних наук, доцент

ПРАВОВІ АСПЕКТИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ЯК ІНСТРУМЕНТУ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ У КОНТЕКСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Трансформація характеру сучасних збройних конфліктів дедалі чіткіше демонструє пріоритетну роль інформаційного середовища як стратегічного простору впливу. У цьому контексті штучний інтелект (далі − ШІ) виступає не лише як інструмент технологічного розвитку, а й як потенційно небезпечний механізм, що здатний радикально змінити як засоби, так і масштаби інформаційного протиборства. Особливого значення ця проблема набуває в умовах збройної агресії проти України, де ШІ активно використовується для створення та поширення дезінформаційних продуктів, маніпуляції суспільною думкою, психологічного тиску, порушення цілісності кіберпростору [4, с. 282; 3, с. 2].

Аналіз останніх наукових досліджень та практики застосування ШІ в рамках гібридних воєн свідчить про формування нового кластеру правових загроз, які виникають на перетині інформаційного, кібернетичного та технологічного правопорядку. Зокрема, дослідники наголошують на невизначеності статусу та відповідальності розробників і користувачів автономних систем, відсутності чіткого правового режиму ШІ у межах чинного українського законодавства, а також на ризиках порушення прав людини та основоположних свобод у процесі обробки даних і моделювання поведінки громадян за допомогою алгоритмів [1, с. 249; 2, с. 108; 8, с. 133].

Водночас варто відзначити і значний нормативний вакуум у національному правовому полі, який унеможливлює ефективне регулювання використання ШІ в умовах інформаційної війни. На сьогодні у правовій доктрині України відсутні законодавчо визначені ключові поняття, пов’язані з використанням ШІ в інформаційному просторі, що створює складнощі у кваліфікації відповідних суспільно небезпечних діянь та притягненні до юридичної відповідальності [5, с. 1; 7, с. 35]. На міжнародному рівні ці питання поки що врегульовані фрагментарно, а інституційні ініціативи, такі як AI Act Європейського Союзу, перебувають на стадії імплементації [6, с. 22].

У світлі викладеного особливої актуальності набуває потреба в системному переосмисленні концептуального підходу до правового регулювання штучного інтелекту з урахуванням його потенціалу у сфері військових конфліктів та інформаційної безпеки.

Використання штучного інтелекту у сфері інформаційної війни супроводжується рядом фундаментальних викликів для правового порядку, насамперед з огляду на транснаціональний, автономний та високодинамічний

характер таких технологій. Проблематика правового регулювання полягає не стільки у відсутності загального контролю над технологією, скільки у тому, що традиційні форми правового регулювання не встигають за темпами її розвитку, що призводить до виникнення правових лакун, колізій і невизначеності щодо режиму правової відповідальності.

По-перше, слід акцентувати на відсутності в українському законодавстві чіткого та системного визначення правового статусу систем штучного інтелекту. Зокрема, не визначено, чи є така система об'єктом або суб'єктом права, що викликає труднощі при застосуванні норм цивільного, кримінального та інформаційного права у випадку заподіяння шкоди [1, с. 250; 3, с. 3]. Подібна ситуація створює правову невизначеність як для розробників, так і для користувачів технологій, унеможливлюючи застосування принципів юридичної відповідальності в умовах, коли штучний інтелект функціонує автономно.

По-друге, в нормативному полі відсутня категорія «інформаційна зброя» або «інформаційна атака», здійснена за допомогою ШІ. Це не дозволяє кваліфікувати такі дії як акти агресії або як посягання на національну безпеку, хоча вони можуть мати наслідки, еквівалентні впливу класичних збройних дій [4, с. 284; 5, с. 3].

По-третє, значні труднощі викликає відсутність диференціації між комерційним, військовим та терористичним використанням ШІ. Така правова невизначеність унеможливлює побудову ефективної моделі превентивного контролю та реагування, включаючи відповідні процедури сертифікації, ліцензування та моніторингу застосування штучного інтелекту в чутливих сферах [7, с. 38].

У підсумку актуальною постає необхідність формування цілісної нормативної моделі, що враховувала б особливості автономного функціонування ШІ, його роль в умовах воєнного конфлікту та потенціал у сфері деструктивного інформаційного впливу.

У контексті зростання ролі технологій штучного інтелекту на політичному та правовому рівнях останніми роками окреслилися тенденції до формування національних і наднаціональних регуляторних підходів, спрямованих на забезпечення прозорості, етичності та безпеки використання ШІ. В Україні наразі відсутній спеціальний закон, який би цілеспрямовано регламентував обіг та функціонування систем штучного інтелекту. Окремі аспекти порушуються у документах стратегічного характеру, таких як Концепція розвитку штучного інтелекту в Україні, затверджена наказом МОН № 155 від 2 лютого 2021 року, а також у Концепції забезпечення кібербезпеки України, однак ці документи не мають належного імперативного статусу і здебільшого формулюють рекомендаційні підходи.

Разом із тим Європейський Союз значно випередив національне правове поле, запропонувавши концепцію так званого AI Act − регламенту ЄС про штучний інтелект, ухваленого в 2024 році. Цей акт уперше класифікує системи ШІ за рівнем ризику (від «мінімального» до «неприйнятного») і передбачає спеціальні вимоги до високоризикових додатків, серед яких − використання у сфері критичної інфраструктури, правосуддя, громадського нагляду тощо.

Зокрема, у статтях 5-7 AI Act чітко забороняється використання ШІ для соціального скорингу, маніпулювання поведінкою громадян без їхньої згоди, а також для масового біометричного спостереження в публічному просторі, що прямо стосується інструментів інформаційної війни [6, с. 24].

Для України, яка прагне до правового наближення до acquis communautaire, вивчення досвіду ЄС у регулюванні ШІ є критично необхідним, оскільки дозволяє інтегрувати в національне право стандарти, що передбачають не лише запобігання зловживанням, а й підвищення довіри до технологій у сфері безпеки. Водночас такий підхід має враховувати реалії воєнного стану, що вимагає інституціоналізації спеціального органу контролю за впровадженням і застосуванням ШІ в чутливих сферах − зокрема, через механізми, подібні до діяльності Кіберцентру при РНБО чи СБУ [2, с. 111; 8, с. 135].

Розгортання сучасної інформаційної війни на тлі широкого впровадження технологій штучного інтелекту детермінує нову парадигму правових загроз, які суттєво відрізняються від традиційних викликів у сфері національної безпеки. ШІ, функціонуючи в автономному та адаптивному режимі, здатний стати високоефективним інструментом деструктивного впливу на інформаційний простір держави, зокрема через маніпуляцію суспільною думкою, розповсюдження дезінформації, руйнування довіри до державних інституцій, а також через уразливість до зовнішнього програмного втручання.

Національна правова система України, як і більшість світових юрисдикцій, на сьогодні не має цілісного правового механізму регламентації використання ШІ у воєнних чи гібридних конфліктах. Відсутність законодавчо визначених понять «штучний інтелект», «інформаційна зброя», «автономна система впливу» створює суттєві труднощі в частині кваліфікації правопорушень, притягнення до юридичної відповідальності та унеможливлює ефективне застосування превентивних і захисних заходів.

Оцінка європейського досвіду, зокрема концептуальних положень AI Act, дозволяє сформулювати ключові орієнтири для подальшого оновлення національного законодавства, серед яких особливо важливими є: ризик-орієнтований підхід до регулювання, створення спеціального органу контролю за обігом ШІ-технологій, запровадження нормативного режиму для високоризикових систем, а також кодифікація етичних стандартів та процедур сертифікації.

Таким чином, правове регулювання штучного інтелекту в умовах інформаційної війни має ґрунтуватися на принципах національної безпеки, техноетики, відповідальності та прозорості, при цьому інтегруючи міжнародні стандарти, адаптовані до реалій воєнного часу. Розробка відповідного спеціального законодавчого акту є стратегічно важливим кроком для захисту інформаційного суверенітету України та запобігання масштабному зловживанню технологіями нового покоління у сфері безпеки та оборони.

Список використаних джерел

1. Буряченко О. Сучасні виклики глобальної інформаційної безпеки. *Вісник Львівського університету.* Серія: Міжнародні відносини. 2024. № 55. С. 247–254.

2. Гуржій С.В. Організаційно-технічні та кримінально-правові основи протидії російським ботам в умовах війни. *Науковий вісник Міжнародного гуманітарного університету.* Серія: Юриспруденція. 2023. № 64. С. 108–114.

3. Каранфілова О.В. Складові державно-правового механізму інформаційної безпеки України в умовах воєнного стану. *Наукові записки Південноукраїнського національного педагогічного університету імені К. Д. Ушинського.* 2024. Вип. 1. С. 1–7.

4. Авдєєва Г.К. Системи штучного інтелекту як засоби протидії інформаційній війні в Україні. Національна безпека України: правові та організаційні механізми забезпечення : матеріали наук. конф., Харків, 2023 р. Харків : Ін-т вивчення проблем законності НАН України, 2023. С. 282–287.

5. Павленко Т.А. Технології ШІ у забезпеченні інформаційної безпеки України. Національна безпека України: правові та організаційні механізми забезпечення : матеріали наук. конф., Харків, 2023 р. Харків : Ін-т вивчення проблем законності НАН України, 2023. С. 133–138.

6. Ярошевська Т. Переваги та недоліки використання технологій ШІ в умовах війни та у післявоєнний час. *Вісник Дніпропетровського державного університету внутрішніх справ.* 2024. № 1. С. 22–28.

7. Радзієвська О.Г. Проблеми забезпечення інформаційних прав та безпеки людини в сучасних умовах. Збірник наукових праць кафедри інформаційної та кібернетичної безпеки КПІ. 2023. С. 35–41.

8. Скіцько О., Складанний П., Ширшов Р. Загрози та ризики використання штучного інтелекту в інформаційній війні. Кібербезпека: освіта, наука, техніка. 2023. № 2. С. 1–8.

Колодій Олексій Анатолійович,
доцент кафедри теорії, історії та філософії права Національної академії внутрішніх справ, доктор юридичних наук

ПРИНЦИПИ КОНСТИТУЦІЙНО-ПРАВОВОГО СТАТУСУ УКРАЇНСЬКОГО НАРОДУ

Беззаперечно, що для того щоб об’єктивно дослідити принципи конституційно-правового статусу Українського народу доцільно, насамперед, з’ясувати загальне розуміння принципів.

А тому зазначимо, що у більшості випадків стверджують, що «Принципи права – це такі відправні ідеї існування права, які виражають найважливіші закономірності і підвалини даного типу держави і права, є однопорядковими із сутністю права і становлять його головні риси, відрізняються універсальністю, вищою імперативністю і загальнозначимістю, відповідають об’єктивній необхідності побудови і зміцнення певного суспільного ладу. Принципи права спрямовують і надають синхронності усьому механізму правового регулювання