

ПРОБЛЕМНІ ПИТАННЯ ІНФОРМАЦІЙНОГО УБЕЗПЕЧЕННЯ КОСМІЧНОЇ ДІЯЛЬНОСТІ

(морально-правові засади використання штучного інтелекту)

У попередніх наших публікаціях наголошено, що інформаційна безпека як складова безпеки космічної діяльності складається з тріади:

«- діяльність із забезпечення – надання допомоги суб'єктам для досягнення поставлених цілей:

1) охорони прав інтелектуальної власності, державної, військової та комерційної таємниці;

2) забезпечення отримання повної, своєчасної, достовірної, цілісної доступної інформації;

3) дотримання законодавчого режиму обігу інформації з обмеженим доступом: конфіденційної; державної таємниці; службової інформації.

- засоби забезпечення – сукупність матеріальних, духовних, фінансових, правових, організаційних і технічних засобів здійснення діяльності щодо забезпечення;

- суб'єкти забезпечення – індивіди, організації, органи держави, які здійснюють діяльність щодо забезпечення космічної діяльності [1, с. 194]».

В той же час до засобів забезпечення інформаційної безпеки космічної діяльності на сучасному етапі розвитку науки й техніки, а в майбутньому до суб'єктів можливо віднести штучний інтелект. Означені перспективи визначають низку викликів, філософського, етично-морального та правового змісту. З одного боку враховуючі думки трансгуманістів, що вступ суспільства у інформаційну форму існування на тлі використання комп'ютерів та всесвітнього павутиння створило передумови управління людиною за допомогою алгоритмів, за якими працює штучний інтелект.

Ми згодні з думками науковців, що виникає низка безпекових морально-етичних та правових проблем використання андроїдів у різних сферах

діяльності у тому числі космічній, починаючи з наукових, дослідницьких, виробничих, обслуговуючих робіт закінчуючи забезпеченням різних рівнів інформаційної безпеки [2, с. 61-74; 3, с. 116-120].

Аналіз наукових публікацій останніх років свідчить, що окрім визначеного необхідно додати наступні умови побудови штучного інтелекту:

«як сконструювати цей інтелект таким чином, щоб жодна група людей не зуміла отримати з його допомогою переваги над іншими людьми, і щоб штучний інтелект не спрямував свою силу проти людства, а навпаки – використовувався на його благо» [4].

Дослідження складових космічної діяльності та законодавства у сфері її регулювання. Дозволяє констатувати, що на даному етапі розвитку людства постає питання як реалізувати потенціал штучного інтелекту у технологічному ланцюжку об'єкт-ЕОМ-ШІ-людина з забезпеченням обробки багатьох даних пов'язаних з космічною діяльністю:

- у виробництві об'єктів космічного та наземного базування устаткування з підтримкою ШІ використовується для оптимізації виробничого процесу та підтримки виконання завдань, які виконують люди;

- управління об'єктами космічного та наземного базування;
- підтримки зв'язку за допомогою супутників;
- вирішення комунікаційних, моніторингових задач пов'язаних з отримання та обробки значних обсягів інформації.

Окрім означеного ШІ повинен вирішити завдання стійкості на рівні конкретних суб'єктів-об'єктів космічної діяльності:

- спроможність надійно функціонувати у штатному режимі;
- адаптуватися до умов, що постійно змінюються;
- протистояти та швидко відновлюватися після реалізації загроз будь-якого виду: природного і техногенного характеру, загроз, що спричинені протиправними діями, та інших загроз [5, с. 17-18].

Реалізація означених задач визначається діяльністю суб'єктів забезпечення стійкості з використанням засобів та робототехніки зі штучним інтелектом в межах системи моніторингу ризиків та загроз безпеки, побудови організаційно-тактичної моделі запобігання, стримування, нейтралізації або пом'якшення наслідків терористичних дій спрямованих на знищення, виведення з ладу або зловмисне використання критичної інфраструктури в цілому та об'єктів космічної діяльності України, взагалі [6, с. 166-174.].

В той же час науковці дотримуються думки, що існує низка ризиків для людства пов'язаних з неконтрольним, або з порушення принципів моральності та етичності застосування технологій штучного інтелекту:

- втрата робочих місць людьми на ґрунті автоматизацію рутинних повторюваних операцій;
- порушення приватності, ледь не до повної її руйнації;
- Deepfakes («синтез слів «глибинне навчання» та «підробка» – методика синтезу зображення чи аудіо ряду мовлення людини, яка базується на штучному інтелекті; вона використовується для поєднання і накладення наявних зображень та відео на вихідні зображення або відеоролики»);
- автоматизована зброя, що поцілуватиме живі об'єкти без втручання людей-операторів;
- помилково-упереджені рішення систем через викривленість початкових навчальних даних (algorithmic bias) [7].

Останні два ризики найбільш небезпечні в умовах російської навали. Всі означені ризики безпосередньо пов'язані з поглядами представника трансгуманістів професора Ніка Бострома, голови Оксфордського інституту майбутнього людства щодо завантаження людського розуму до комп'ютера та створення та створення «швидкого надрозуму». Він зазначає, що швидкість надрозуму в десять тисяч разів перевищує швидкість біологічного мозку [8].

Як вбачається всі означені ризики можуть бути інтерпретовані як загрози національній безпеці та її підсистемі інформаційній безпеці космічної діяльності. Щоб уникнути цих проблемних питань слід погодитися з європейським законодавцем, яким було розроблено та опубліковано Рекомендації з етики для надійного штучного інтелекту (далі – Рекомендації) (European Commission, 2019).

Рекомендаціями визначена система принципів формування штучного ентелекту: поваги до автономії людини, запобігання шкоді, справедливості і пояснення. Фактично означені Рекомендації створюють умови реалізації системи методів контролю штучного інтелекту запропонованих Ніком Бостромом:

- ізоляційні методи - помістити ШІ в середовище, де він не зможе завдати шкоди людству;
- стимулюючі методи контролю полягають у створенні умов, за яких ШІ буде вигідно діяти на користь людей;
- методи затримки розвитку - свідомо обмежуємо інтелектуальні можливості системи або її доступ до інформації;
- методи розтяжок – це специфічне обладнання, яке дає можливість проводити діагностику ШІ, у тому числі без його відома [8].

Означені методи відповідно до Рекомендацій формують надійний штучний інтелект, який має три компоненти, що повинні бути протягом усього життєвого циклу системи:

- 1) Законність;
- 2) Етичність;
- 3) Надійність.

Ми згодні з думкою, що мета у вигляді надійного штучного інтелекту може бути досягнута лише тоді, коли людина візьме на себе відповідальність щодо формування такої надійності на різних етапах розробки, обігу та використання технологій ШІ. [9, 95-96].

Таким чином виникає низка викликів щодо використання ШІ взагалі та у космічній діяльності зокрема:

- загроза персональним даним;
- захисті прав і свобод осіб, які підлягають впливу штучного інтелекту;
- недостатній рівень регулювання використання та контролю за штучним інтелектом взагалі та забезпечення інформаційної безпеки космічної діяльності, зокрема.

Дслідження сучасних наукових публікацій свідчить, що підґрунтям таких ризиків є:

- відсутність досліджень щодо правового феномену штучного інтелекту та його статусу при реалізації завдань різного рівня;
- відсутній єдиний категорійний апарат;
- не сформовані загально-правові та наукові підходи до визначення поняття штучного інтелекту та його місця в сучасній системі суспільних відносин [10, с. 310-313].

Напрямами вирішення означених проблем є:

- прийняття закону про штучний інтелект з метою закріплення принципу збалансованого використання систем ШІ, захист прав громадян і підтримку інноваційного розвитку країни;
- здійснення досліджень на фундаментально-прикладному рівні щодо нейтралізації загроз збоку використання ШІ у оборонній сфері та космічній діяльності на ґрунті використання різних методів контролю штучного інтелекту;
- визначити теоретико-правові засади концепції, доктрини, стратегії та політики щодо використання штучного інтелекту з визначенням його правосуб'єктності та ймовірність відповідальності то що.

Список використаних джерел:

1. Шинкаренко І.О. Актуальні питання правового забезпечення інформаційної безпеки космічної діяльності. *Актуальні проблеми та перспективи розвитку юридичної науки, освіти та технологій у XXI столітті в дослідженнях молодих учених: збірник матеріалів доповідей учасників всеукраїнської науково-практичної конференції.* (Харків, 3

березня 2023 р.). Харків, 2023. с. 192-195. URL: <https://dspace.univd.edu.ua/server/api/core/bitstreams/5527496e-3372-40b5-b2dc-650e973e3df4/content>.

2. Бежевець А.М. Правовий статус роботів: проблеми та перспективи визначення. *Інформація і право*. № 1 (28). 2019. с. 61-67. URL: <https://ippi.org.ua/bezhevets-am-pravovii-status-robotiv-problemi-ta-perspektivi-viznachennya-st-61-67>. [https://doi.org/10.37750/2616-6798.2019.1\(28\).273347](https://doi.org/10.37750/2616-6798.2019.1(28).273347)

3. Позова Д. Д. Перспективи правового регулювання штучного інтелекту за законодавством ЄС. *Часопис цивілістики*. 2017. № 27. 116-120. URL: http://nbuv.gov.ua/UJRN/Час_2017_27_24

4. Онищук І. Правове регулювання технологій штучного інтелекту: теоретико-прикладні та етичні засади. *Наукові записки Інституту законодавства Верховної Ради України*. № 3. 2020. URL: https://risu.ua/tehnologiyi-shtuchnogo-intelektu-spivvidnoshennya-prava-i-morali_n116164

5. Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України : аналіт. доп. / [Бобро Д. Г., Іванюта С. П., Кондратов С. І., Суходоля О. М.] / за заг. ред. О. М. Суходолі. К. : НІСД, 2019. 224 с. ISBN 978-966-554-258-2. URL: https://niss.gov.ua/sites/default/files/2019-05/Dopov_Suchodolya_print.pdf

6. Шинкаренко О.І. Шинкаренко І.Р., Шинкаренко І.І. Теоретико - правові проблеми аналізу та оцінки загрози безпеці об'єктам аерокосмічного комплексу України. *Забезпечення стійкості у складних умовах: збірник матеріалів доповідей учасників міжнародної міждисциплінарної науково-практичної конференції*. (Харків – Брістоль, 8 червня 2023 р.). Харків- Брістоль, 2023. с. 166-174.

7. Вишня Г. Штучний інтелект і людина: загрози і можливості. 2 березня 2021, 17:50. URL: <https://www.radiosvoboda.org/a/shtuchnyi-intelekt-zagrozy-i-mozhlyvisti/31145992.html> (дата звернення 06.11/23, 13:38).

8. Superintelligence: Paths, Dangers, Strategies Джерело: <https://hub.kyivstar.ua/reviews/shtuchnyy-intelekt>.

9. Головка О., Боднар Є. Етико-правові проблеми використання роботів зі штучним інтелектом. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право. випуск 3(55)*. 2022. с. 95-96. DOI: [https://doi.org/10.20535/2308-5053.2022.3\(55\).269563](https://doi.org/10.20535/2308-5053.2022.3(55).269563)

10. Теличко О.А., Рекун В.А., Чабаненко Ю.С. проблеми визначення та нормативного закріплення поняття «штучний інтелект» у законодавстві зарубіжних країн та України. *Юридичний науковий електронний журнал*. № 2. 2021. С. 310-313. URL: sej.org.ua/2_2021/77.pdf