УДК 342.951(004.896)+351.327.355
DOI https://doi.org/10.32782/2524-0374/2024-4/106

ВІЙСЬКОВІ СИСТЕМИ AI (MILAI): СУСПІЛЬНО-ПОЛІТИЧНІ ВИКЛИКИ

MILITARY AI SYSTEMS (MILAI): SOCIO-POLITICAL CHALLENGES

Прокопович-Ткаченко Д.І., к.т.н.,
доцент кафедри кібербезпеки та інформаційних технологій
Університет митної справи та фінансів

Саричев В.І., д.е.н.,
професор кафедри економіки та економічної безпеки
Університет митної справи та фінансів

Остальцев О.А., старший викладач кафедри військової підготовки
Університет митної справи та фінансів

Смишляєв С.М., доцент кафедри військової підготовки
Університет митної справи та фінансів

Шаволін А.О., доцент кафедри військової підготовки
Університет митної справи та фінансів

В роботі проводиться аналіз проблематики регулювання використання штучного інтелекту (AI) у військовій сфері з акцентом на відсутність глобальної консенсусної бази для створення ефективних і етичних рамок застосування військового AI. Дослідження розглядає нагальну потребу в адаптації та модифікації існуючих етичних принципів, зокрема тих, що були розроблені для цивільних додатків AI, до специфіки військового застосування, з урахуванням унікальних вимог та ризиків, що виникають у цьому контексті.

Визначається, що основні моральні та етичні виклики, пов'язані з розробкою, тестуванням, впровадженням і експлуатацією військових систем AI, такі як проблематика забезпечення відповідальності, прозорості програмних рішень та забезпечення справедливості у використанні військової сили. Особлива увага приділяється потенційним обмеженням використання AI, що вимагає ретельного розгляду, з метою запобігання порушенням законів війни та забезпечення загальної безпеки та стабільності.

В статті підтримується концепція створення міжнародного наглядово-керуючого органу, основною місією якого було б забезпечення нагляду та контролю над імплементацією та використанням морально прийнятного AI у військовій сфері, а також за розповсюдженням автономних систем AI. Цей наглядовий орган міг би відігравати ключову роль у розробці міжнародних стандартів безпеки та етичних норм для використання AI, встановлювати механізми моніторингу та відповідності, а також розробляти процедури сертифікації та ліцензування розробок з алгоритмами AI. Також актуалізується проблема делегування повноважень самостійно знищувати військові цілі від військового командира або начальника до програмних систем та комплексів, що застосовують AI.

Науковцям пропонується в найкоротші терміни сформувати єдиний категоріально-понятійний апарат у сфері AI, що сприятиме однозначному розумінню термінології у міжнародному масштабі та полегшить застосування законодавчих норм у різних країнах.

Наголошується на важливості міжнародної співпраці та уніфікованого підходу до регулювання використання AI у військовій сфері, з метою забезпечення безпеки, стабільності та етичної відповідальності на глобальному рівні.

Ключові слова: штучний інтелект, AI, військовий AI, MilAI, етика AI.

The paper analyzes the issues of regulating the use of artificial intelligence (AI) in the military sphere with a focus on the lack of a global consensus framework for creating an effective and ethical framework for the use of military AI. The study examines the urgent need to adapt and modify existing ethical principles, in particular those developed for civilian applications of AI, to the specifics of military use, taking into account the unique requirements and risks that arise in this context.

It is determined that the main moral and ethical challenges associated with the development, testing, implementation and operation of military AI systems, such as the problems of ensuring responsibility, transparency of software solutions and ensuring fairness in the use of military force. Particular attention is paid to potential limitations of the use of AI, which requires careful consideration in order to prevent violations of the laws of war and ensure overall security and stability.

The paper supports the concept of an international supervisory and governing body that would take on the task of overseeing and controlling the introduction and use of morally acceptable AI in the military sphere, as well as the proliferation of autonomous AI systems. Such a body could contribute to the development of international safety and ethical standards for AI, establish monitoring and compliance mechanisms, and develop certification and licensing procedures for developments with AI algorithms. The problem of delegating the authority to destroy military targets independently from a military commander or chief to software systems and complexes that use AI is also becoming more relevant.

The author suggests that scientists should form a unified categorical and conceptual apparatus in the field of AI as soon as possible, which will facilitate a clear understanding of terminology on an international scale and facilitate the application of legislative norms in different countries.

The author emphasizes the importance of international cooperation and a unified approach to regulating the use of AI in the military sphere, with a view to ensuring security, stability and ethical responsibility at the global level.

Key words: artificial intelligence, AI, military AI, MilAI, AI ethics.

Метою даного дослідження є вивчення та аналіз етичних, правових та безпекових аспектів застосування AI у військовій сфері. Дослідження має мету ідентифікувати потенційні ризики та виклики, пов'язані з впровадженням автономних військових систем, та розробити рекомендації щодо створення міжнародних стандартів та контрольних механізмів, які б допомогли забезпечити етичне та безпечне застосування AI.

Викладення основного матеріалу. Сучасна оборонна політика і стратегія стикаються з викликами, пов'язаними з інтеграцією AI у військові дії, що вимагає не лише технічної адаптації, але й розробки етичних рамок, здатних забезпечити правильне використання таких технологій [1]. В цілому в світі відзначається відсутність координованих зусиль з боку міжнародної спільноти щодо створення єдиних стандартів етичного використання військового AI,

за винятком окремих ініціатив, розроблених Сполученими Штатами Америки [2]. Це створює вакуум у глобальній безпековій політиці, де розвиток та впровадження автономних систем зброї здійснюється без чіткого розуміння етичних меж.

Важливо розуміти, що цивільні стандарти AI не можуть бути застосовані до військових систем без певних модифікацій або трансформацій, які б враховували унікальні вимоги та ризики, асоційовані з військовим AI. Однак модернізація має потенційні обмеження, включаючи труднощі у визначенні та імплементації «мінімально справедливого штучного інтелекту», який би гарантував, що автономна зброя не буде використана для неправомірних дій. Встановлення рамок є критично важливим для забезпечення того, щоб перехід до більш автономних форм ведення війни відбувався відповідально, з повагою до міжнародного гуманітарного права та етичних норм.

У контексті сучасних міжнародних дебатів, тема автономних систем зброї часто сприймається через призму етичних та моральних дилем, зокрема стосовно їх впливу на людську гідність та моральність використання смертоносної сили. Однак, існує і протилежне бачення проблеми, яким оскаржується загальноприйняте переконання про внутрішню аморальність автономних «роботів-вбивць» і розглядаються сценарії, де їх використання може бути морально обґрунтованим і стратегічно виправданим.

Насправді автономні системи зброї не є морально винятковими чи принципово зловмисними, і їхнє застосування не обов'язково порушує людську гідність. Зважаючи на це існує версія, що моральне та етичне використання летальної сили може бути забезпечено навіть без безпосереднього людського контролю, за умови, що використання такої сили відповідає встановленим міжнародним етичним нормам та законам війни.

Зокрема, важливим аспектом є розмежування між процесом прийняття рішення про використання сили та її фізичним застосуванням. Автономні системи, здатні визначати цілі та застосовувати смертоносну силу без безпосереднього людського втручання, можуть все ще діяти в рамках моральних та етичних принципів, якщо їх використання передбачає дотримання вимог до вибору цілей, пропорційності, та уникнення цивільних жертв. Відокремлення людини від безпосереднього процесу використання сили не є новим феноменом і не обов'язково має негативні моральні наслідки. Приклади історичного використання «зброї типу «вистрілив і забув» підкреслюють, що ключовим фактором є відповідність дій вимогам міжнародного гуманітарного права, а не безпосередній фізичний контакт між бійцем та ціллю.

Концепція «значимого людського контролю» в контексті використання автономних систем зброї стала предметом гарячих дебатів у міжнародних дискусіях про етику та правові аспекти таких технологій. Це поняття виникло як спроба вирішити етичні та правові питання, пов'язані з розмежуванням участі людини в процесі прийняття рішень про застосування летальної сили, намагаючись забезпечити, що автономні системи зброї залишаються під контролем та відповідальністю людини.

Однак, критика цієї концепції часто вказує на відсутність чіткого, всесвітньо визнаного визначення, що робить її складною для практичного застосування та інтерпретації. Крім того, існують побоювання, що наголос на «значущому людському контролі» може призвести до концептуальних недоліків, в тому числі до потенційної ерозії відповідальності в умовах, коли визначення меж контролю стає неоднозначним.

Проте, аргумент проти цієї думки полягає в тому, що розвиток автономних функцій в системах зброї не обов'язково призводить до зменшення людського контролю, але може, навпаки, підвищити ефективність та точність військових операцій, зменшуючи ризики для цивільного населення та збільшуючи відповідність дій міжнародному гуманітарному праву. Автономні системи можуть бути програмовані на дотримання строгих правил ведення бойових дій, включаючи принципи розрізнення, пропорційності та обережності.

Для вирішення цих проблем і забезпечення, що автономні системи зброї використовуються відповідально та етично, необхідно розробити чіткі міжнародні стандарти та рекомендації, які б деталізували, що конкретно означає «значущий людський контроль». Це має включати в себе визначення обсягу відповідальності та контролю, який повинен зберігатися в руках людини, та розробку технічних і оперативних критеріїв, які забезпечують дотримання цих принципів на практиці.

Таким чином, хоча існують заперечення щодо концепції «значущого людського контролю», знайти збалансоване рішення, яке враховує як етичні, так і практичні аспекти використання автономних систем зброї, є ключем до забезпечення їхнього відповідального та законного застосування.

Виклики, пов'язані з використанням автономних систем зброї (AWS), наголошують на критичній необхідності впровадження строгого режиму прозорості та підзвітності. Це стає особливо актуальним у світлі можливості незаконного чи неетичного застосування смертоносної сили такими системами та існуючих прогалин у прозорості щодо їхнього розгортання.

Перш за все, існуюча прогалина в прозорості публічного контролю вже стає помітною в контексті дистанційно керованих БПЛА. Випадки, коли інформація про застосування смертоносної сили приховується або заперечується, підкреслюють нагальну потребу в більшій відкритості та підзвітності.

По-друге, незважаючи на попередні стратегії, розроблені Пентагоном для вирішення моральних, етичних і правових викликів, пов'язаних з AWS, залишається значний простір для покращення в контексті прозорості. Це підкреслює необхідність розробки та впровадження ефективних заходів, які б гарантували, що використання автономних систем зброї відбувається відповідно до міжнародного права та етичних норм [3].

По-третє, важливість прозорості контролю в контексті AWS не може бути недооцінена. Вона є ключовою для забезпечення підзвітності та дотримання установлених правил та стандартів. Це означає, що потрібно створити механізми, які б дозволяли відстежувати рішення про застосування смертоносної сили, забезпечувати їх відповідність законам і нормам, та відповідати за порушення.

Створення таких комплексних механізмів прозорості та підзвітності вимагає зусиль не лише від військових та оборонних агентств, але й від міжнародної спільноти, правових органів, громадянського суспільства та наукових кіл. Ці механізми повинні включати в себе чіткі процедури розгляду та звітності, доступність інформації про правила використання AWS, а також незалежний нагляд та перевірку. Тільки так можна забезпечити, що розгортання автономних систем зброї відбувається відповідально та етично, мінімізуючи ризики для цивільного населення та забезпечуючи дотримання міжнародних норм.

Суспільне сприйняття та оцінка рішень, прийнятих AI, особливо у контексті життєво важливих рішень, таких як застосування летальної сили, піднімає важливі питання щодо моральної прийнятності та прозорості AI. Згідно з даними соціологічних опитувань, сьогодні значна частина населення схильна застосовувати до рішень, прийнятих AI, ті ж самі моральні та етичні стандарти, що й до рішень, прийнятих людьми. Однак, ця початкова схильність розходиться з реальністю, коли йдеться про безпосереднє особисте сприйняття та оцінку цих рішень. Це відхилення між теоретичними очікуваннями та фактичними оцінками можна пояснити відсутністю емпатії та емоцій-

ного розуміння в контексті, в якому діє AI. Людське схвалення рішень, прийнятих іншими людьми, часто ґрунтується на співпереживанні та взаєморозумінні, в той час як AI не викликає аналогічних емоційних реакцій.

Враховуючи цю розбіжність, стає очевидною необхідність для AI не лише «приймати» обґрунтовані та відповідальні рішення, але й прозоро комунікувати логіку та обґрунтовувати свої дії людям. Це вимагає розробки механізмів прозорості та інтерфейсів, зрозумілих для людей, які дозволяють зрозуміти процеси прийняття рішень AI. Прозорість AI не тільки підвищує довіру та прийнятність їхніх дій серед широкого населення, але й важлива для забезпечення відповідальності. Вона дозволяє оцінити, чи діяв AI відповідно до моральних та правових норм, та визначити, де лежить відповідальність у випадках неправомірних дій.

Щодо викликів, пов'язаних з регулюванням автономних систем зброї (AWS). Зв'язок між проблемами регулювання AWS і досвідом, отриманим від Конвенції про біологічну зброю (BWC), підкреслює важливість адаптації вже існуючих міжнародних засад і підходів до контексту штучного інтелекту та автономних технологій.

Стандарти безпеки AI, повинні відігравати ключову роль у розвитку та впровадженні AWS, забезпечуючи, що такі системи спроектовані з урахуванням етичних міркувань з «нуля». Заходи зміцнення довіри та забезпечення прозорості досліджень і розробок у сфері AI стануть фундаментом для побудови взаєморозуміння та довіри між державами, а також між державами та громадськістю.

Заборона наступальних розгортань AWS повинна розглядатися як частина масштабної стратегії забезпечення міжнародної безпеки та стабільності. Такий підхід допомагає обмежити ризики, пов'язані з неконтрольованим поширенням та використанням автономних технологій у військових цілях. Ефективне регулювання AWS вимагає міжнародної співпраці, розвитку технологічних стандартів, етики, моралі, цінностей та зобов'язання прозорості і підзвітності [4].

Оперативне середовище військових дій сьогодні оснащене великою кількістю пристроїв, що в реальному часі здатні збирати, обробляти та передавати дані, що, в свою чергу, забезпечує широкі можливості для оперативного управління та прийняття рішень. Проте слід відмітити, що вплив технологій на процес прийняття рішень у військовій сфері не обмежується виключно позитивними аспектами. Висока залежність від технічних систем і алгоритмічного аналізу може призвести до знеособлення процесу прийняття рішень, втрати гуманітарного контексту та ігнорування соціального значення, що є критично важливими для адекватного реагування на виклики сучасних військових конфліктів. Системний аналіз життєвих циклів систем AI, що використовуються у військових цілях, виявляє складну взаємодію між технічним прогресом і потребою в забезпеченні безпеки та етичності їх застосування. Виклики, з якими зіштовхуються розробники та оператори військових систем AI, особливо виділяються на кожному етапі життєвого циклу системи, від розробки до експлуатації.

Фаза Розробки. На етапі розробки критично важливим є створення стійких до атак баз даних та алгоритмів. Атака «отруєння» (Poisoning attacks) підкреслює необхідність ретельної верифікації та валідації даних, які використовуються для навчання AI, щоб запобігти спотворенню вивчених моделей і забезпечити, що система може надійно функціонувати у військових умовах.

Фаза Тестування. Під час тестування, увага зосереджується на виявленні та мінімізації ризиків, пов'язаних з атаками «ухилення» (Evasion attacks), де зловмисники можуть намагатися маніпулювати вхідними даними для індукції помилкових рішень системою. Тестування в різних умовах і з різними типами вхідних даних допомагає виявити потенційні вразливості в алгоритмах AI.

Фаза Експлуатації. Під час експлуатації, системи AI повинні бути захищені не тільки від атак «отруєння» та «ухилення», але й від зусиль «зворотного проектування» (Reverse Engineering attacks), що можуть дозволити противникам розкрити внутрішню логіку та алгоритми системи. Захист від таких атак вимагає застосування складних методів шифрування та обмеження доступу до системи.

Фаза Обслуговування. На етапі обслуговування, постійний моніторинг та оновлення систем AI є ключовими для забезпечення їх безпеки та ефективності. Це включає в себе оновлення захисних механізмів для протидії новим методам атак та вдосконалення алгоритмів для кращої адаптації до змінних умов використання.

Забезпечення безпеки та ефективності військових систем AI вимагає цілісного підходу до розробки, тестування, експлуатації та обслуговування. Розуміння та мінімізація вразливостей на кожному з цих етапів є критично важливими для забезпечення, що автономні системи зброї можуть виконувати свої функції ефективно.

У контексті оборони від атак зворотного інжинірингу (Reverse engineering attack), дослідження розглядає комплексні підходи до зміцнення військових систем AI. Пропонуються стратегії, які включають посилення безпеки на рівні даних та алгоритмів, обмеження доступу до вихідних даних системи для неавторизованих користувачів, а також розробку політик і технік, які ускладнюють процес витягу корисної інформації шляхом аналізу поведінки системи. Окрім технічних заходів, акцентується на значенні розробки правових рамок, які регулюють використання військових систем AI, встановлюючи межі для виконання автоматизованих запитів та доступу до інформації, яка може бути використана для зворотного інжинірингу [5].

Сценарій виникнення автономного агресивного штучного інтелекту (AI) у країнах з диктаторськими режимами вимагає ретельного аналізу ризиків та викликів, як загрозу глобальній безпеці та стабільності. Агресія, як свідчить війна, розв'язана рф проти України, може виходити за межі традиційного розуміння воєнного конфлікту, підкреслюючи потенціал для зловмисного використання технологій AI у військових цілях. В цьому контексті, ризик розвитку та використання автономних агресивних військових систем AI стає особливо актуальним.

Моральні та етичні виміри. Моральні та етичні вимоги до застосування AI у військовій сфері вимагають визначення чітких правил, які б забезпечували відповідність дій міжнародним нормам і принципам гуманітарного права. Проблематика стає ще більш складною у випадку диктаторських режимів, де міжнародні зобов'язання можуть ігноруватися на користь власних інтересів.

Виклики для міжнародної спільноти. Міжнародна спільнота стикається з величезним викликом щодо регулювання та контролю за розповсюдженням та використанням військового AI. Потрібен всеохоплюючий підхід, який включає розробку міжнародних норм та стандартів, спрямованих на запобігання розвитку та застосування автономних агресивних систем AI.

Роль технологічних інновацій. Інновації у сфері штучного інтелекту та машинного навчання відіграють ключову роль у розробці оборонних механізмів проти потенційно агресивних автономних систем, що можуть ідентифікувати, відстежувати та нейтралізувати загрози від автономного AI.

В контексті цифрового розвитку та зростання важливості Metaverse [6], забезпечення безпеки та етичності застосування AI стає ще більш складним. Майбутнє суспільного устрою вимагає від міжнародної спільноти адаптації до нових викликів, пов'язаних з технологічним прогресом, та розробки стратегій, які забезпечать мирне співіснування та стримування ризиків, пов'язаних з автономними агресивними системами AI [7].

Звертаємо увагу на атаки «висновку» (watering hole attack) для Metaverse, які представляють собою розширену загрозу в контексті безпеки військових систем AI, доповнюючи виклики, пов'язані зі зворотним інжинірингом. Цей клас атак зосереджений на екстракції даних, які були використані в процесі навчання системи AI, безпосередньо атакуючи конфіденційність даних. Відмітною особливістю атак «висновку» є їх здатність ідентифікувати, чи входила конкретна точка даних до набору даних, використаного для тренування системи, що може розкрити чутливу інформацію про військові засоби або стратегії.

Атаки «висновку» на військові системи AI ставлять під загрозу безпеку секретних знань про оборонні технології. Такі атаки можуть призвести до втрати критичної інформації, що у свою чергу відкриває потенційні стратегічні вразливості перед противниками. Ось чому стратегії протидії цим загрозам вимагають ретельної уваги та розробки.

Зміцнення політик обробки даних. Одним із ключових напрямів протидії атакам «висновку» є розробка і впровадження вдосконалених політик обробки даних. Це означає встановлення чітких процедур для вибору та використання даних у навчанні систем AI, з особливим акцентом на захист конфіденційної інформації.

Контроль доступу. Контроль доступу до даних, що використовуються для тренування військових систем AI, є критично важливим. Це включає обмеження доступу до ключової інформації та впровадження багаторівневих систем безпеки для захисту цих даних від несанкціонованого доступу.

Розробка та впровадження загальновійськових політик. Необхідність в балансі між захистом секретної інформації та забезпеченням ефективності систем AI вимагає розробки загальновійськових політик щодо навчання та використання алгоритмів AI [8].

Управління ризиками, пов'язаними з атаками «висновку», вимагає комплексного підходу, що об'єднує технічні, організаційні та політичні стратегії. Чіткі політики обробки даних, контроль доступу, застосування технологій збереження приватності та розробка загальновійськових політик є ключовими елементами для забезпечення безпеки та ефективності військових систем AI. Це не тільки захищає режимні дані, але й сприяє зміцненню стратегічної стабільності на національному та міжнародному рівні [9].

Створення міжнародного наглядово-керуючого органу для контролю за застосуванням морального AI і розповсюдженням автономних систем AI військового або подвійного призначення є важливим кроком у забезпеченні безпеки на глобальному рівні. Враховуючи потенціал AI та його здатність до автономного прийняття рішень, існує реальна необхідність у міжнародній координації та стандартизації підходів до регулювання та контролю над такими технологіями.

Єдина міжнародна система сертифікації. Запровадження Єдиної міжнародної системи сертифікації та ліцензування для розробок з алгоритмами AI може забезпечити уніфікований підхід до оцінки безпеки, надійності та етичності таких технологій. Це дозволить створити прозорі та зрозумілі критерії для визначення допустимості використання систем AI у різних сферах, перш за все у військовій.

Система фіксації та реагування на інциденти. Створення Міжнародної системи для фіксації та реагування на інциденти, пов'язані з використанням систем на основі AI, є ключовим для вчасного виявлення та мінімізації наслідків потенційно небезпечних подій. Така система могла б зібрати дані про інциденти з усього світу, аналізувати їх та надавати рекомендації щодо запобігання аналогічним ситуаціям у майбутньому.

Міжнародна типова модель загроз. Формування Міжнародної типової моделі загроз, що включає технічні, біологічні, фінансові, економічні, політичні та військові аспекти застосування AI, дозволить краще розуміти потенційні ризики та розробляти ефективні стратегії їх нейтралізації.

Типовий Закон «Про штучний інтелект». Розробка та прийняття Типового закону «Про штучний інтелект» на міжнародному рівні стане фундаментом для формування відповідних національних законодавчих актів. Такий закон повинен охоплювати всі аспекти використання AI, включаючи етичні норми, права та обов'язки розробників та користувачів, а також механізми контролю та відповідальності. Слід зазначити, що прийнятий 13 березня 2024 року Європейським парламентом Закон «Про штучний інтелект» [10], безперечно є своєчасним та корисним нормативно-правовим актом. Однак, детальне його вивчення ставить під сумнів раціональності та сучасності його окремих положень.

Єдиний категоріально-понятійний апарат. Формування єдиного категоріально-понятійного апарату в галузі AI та його максимальне поширення забезпечить однозначне розуміння термінології та полегшить міжнародну співпрацю та обмін знаннями в цій області.

Ці заходи можуть стати основою для створення безпечного та відповідального майбутнього, де технології штучного інтелекту використовуються для покращення якості життя та забезпечення глобальної безпеки, з одночасним мінімізуванням ризиків та негативних наслідків їх застосування.

Висновки. У дослідженні проведено аналіз сучасних викликів та проблем, пов'язаних із розвитком та впровадженням AI у військовій сфері. Основна увага приділялася необхідності розробки єдиних міжнародних стандартів та рамок для регулювання цієї сфери. Важливим висновком є те, що без створення чітких міжнародних директив та контрольних механізмів ризик зловмисного використання автономних систем AI, здатних наносити шкоду людям та цивільній інфраструктурі, залишається критичним.

Підкреслюється важливість міжнародної співпраці у формуванні загальноприйнятих норм та стандартів, які б обмежували застосування AI безпосередньо у військовій сфері, тим самим сприяючи збереженню миру та безпеки на глобальному рівні, розвитку подальшого міжнародного діалогу та співпраці в області регулювання та контролю за використанням військових систем AI, з метою забезпечення їх етичного та безпечного застосування.

ЛІТЕРАТУРА

1. Danielle C. Tarraf, Shelton, W., Parker, E., Alkire, B., Gehlhaus, D., Grana, J., Levedahl, A., Léveillé, J., Mondschein, J., Ryseff, J. (2019). The Department of Defense Posture for Artificial Intelligence. Assessment and Recommendations. URL: https://www.rand.org/content/dam/rand/pubs/research_reports/RR4200/RR4229/RAND_RR4229.pdf.

2. Artificial Intelligence and National Security. (2020). *Congressional Research Service.* URL: https://sgp.fas.org/crs/natsec/R45178.pdf.

3. Zoe Stanley-Lockman, Edward Hunter Christie. (2021). NATO's Artificial Intelligence Strategy. URL: https://www.nato.int/docu/review/ru/articles/2021/10/25/strategiya-nato-v-oblasti-iskusstvennogo-intellekta/index.html

4. Jai Galliott (ed.), Duncan MacIntosh (ed.), Jens David Ohlin (ed.). Lethal Autonomous Weapons: Re-Examining the Law and Ethics of Robotic Warfare. Collection: Oxford Scholarship Online. (2021). URL: https://oxford.universitypressscholarship.com/view/10.1093/oso/9780197546048.001.0001/oso-9780197546048

5. Department of Defense USA, Directive 3000.09, Autonomy in Weapon Systems. (2023). URL: https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf.

6. Kostenko, O., Furashev, V., Zhuravlov, D. & Dniprov, O. (2022). Genesis of Legal Regulation Web and the Model of the Electronic Jurisdiction of the Metaverse. *Bratislava Law Review*, vol. 6(2), pp. 21–36. DOI: https://doi.org/10.46282/blr.2022.6.2.316

7. Kostenko, O., Jaynes, T., Zhuravlov, D., Dniprov, O., & Usenko, Y. (2022). Problems of using autonomous military AI against the background of Russia's military aggression against Ukraine. *Baltic Journal of Legal and Social Sciences*, vol. 4, pp. 131–145. DOI: https://doi.org/10.30525/2592-8813-2022-4-16

8. D. F. Reding, J. Eaton. Science & Technology Trends 2020-2040, Exploring the S&T Edge, NATO Science & Technology Organization, 2020. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

9. Rigaki, M., Garcia S. (2023). A Survey of Privacy Attacks in Machine Learning. *ACM Computing Surveys*, vol. 56(4), article 101, pp. 1–34. DOI: https://doi.org/10.1145/3624010

10. European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))