DOI https://doi.org/10.30525/978-9934-26-608-9-19

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ВІЙСЬКОВІЙ ГАЛУЗІ: РИЗИКИ ТА ЗАГРОЗИ ДЛЯ ОСОБОВОГО СКЛАДУ

Краснов Р. В., Шумлянський С. В., Свєтлічний І. В.

ВСТУП

В умовах повномасштабної збройної агресії проти України наука, як одна із суспільних сфер, перебуває у перманентному розвитку. Одним із інноваційних технологічних досягнень у сфері науки (техніки) сучасності є спроби створення технологій штучного інтелекту (далі – ШІ), який би мав такі ж когнітивні можливості що й інтелект людини. Створення ШІ з такими когнітивними можливостями є одним із найбільш перспективних напрямків науки. Тому наукові розробки на основі ШІ в теперішніх умовах повномасштабної російської агресії необхідно якмога швидше впроваджувати у військову галузь, зокрема у новітні зразки озброєння та військової техніки.

В Україні впровадження інформаційних технологій, частиною яких є технології штучного інтелекту, є невід'ємною складовою розвитку соціально-економічної, науково-технічної, оборонної, правової та іншої діяльності у сферах загальнодержавного значення. Зокрема, у Концепції розвитку штучного інтелекту в Україні, яка схвалена розпорядженням Кабінету Міністрів України 2 грудня 2020 року визначений розвиток технологій штучного інтелекту в Україні як один з пріоритетних напрямів у сфері науково-технологічних досліджень[1].

Згідно до згаданої Концепції розвитку штучного інтелекту в Україні пріоритетними напрямами реалізації ШІ в Україні є: впровадження технологій штучного інтелекту у сфері освіти, економіки, публічного управління, кібербезпеки, оборони та інших галузях для забезпечення довгострокової конкурентоспроможності України; приведення законодавства у галузі використання технологій штучного інтелекту у відповідність із міжнародними нормативно-правовими актами. Реалізація Концепції передбачена на період до 2030 року. Пріоритетними сферами, в яких реалізуються завдання державної політики розвитку галузі штучного інтелекту, є: освіта і професійне навчання, наука, економіка, кібербезпека, інформаційна безпека,

[1] Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядж. Каб. Міністрів України від 02.12.2020 № 1556-р : станом на 29 груд. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р#Text.

оборона, публічне управління, правове регулювання та етика, правосуддя. Впровадження технологій ШІ в Україні вимагає виконання ряду завдань, а зокрема: удосконалення законодавства і створення сучасної нормативно-правової бази для впровадження кращих світових практик штучного інтелекту у сфері кібербезпеки і кіберзахисту; опрацювання питання відповідності законодавства України керівним принципам, установленим Радою Європи, щодо розроблення та використання технологій штучного інтелекту та гармонізація його з європейським тощо. У такому контексті розвиток технологій ШІ та їх впровадження у суспільні та війському сфери, на наш погляд, можна вважати найбільш перспективним національним завданням України, яке може вивести її у провідні держави світу в технологічному, економічному та військовому вимірі та дозволить успішно протистояти викликам національної безпеки і оборони на даний час і в майбутньому.

Майбутнє ШІ в Україні, відповідно загальнодержавної стратегії з ШІ на період до 2030 року, це інтеграція ШІ до сфери управління, кібербезпеки, охорони здоров'я, освіти, фінансових та оборонних технологій[2].

1. Ризики застосування елементів штучного інтелекту у діяльності сил оборони України

Ризик у повсякденному житті визначається як потенційна можливість настання несприятливих подій. Існування ризику передбачає наявність обов'язкових умов: можливість випадкової події, негативної за своїми наслідками; наявність матеріального або іншого збитку, а також діяльності, пов'язаної з цією подією.

Що стосується саме військової сфери, то у посібнику з управління ризиками НАТО ризик визначається як «невизначена подія або умова, яка відбуваючись, має позитивний або негативний вплив на цілі проекту». Згідно з цим визначенням термін "ризик" охоплює як можливості, так і загрози. По суті, управління усіма ризиками (як можливостями, так і загрозами) здійснюється подібним чином (хоча існують розбіжності у кількісному вимірюванні ризику та стратегіях реагування). Цей же посібник уводить поділ ризиків на внутрішні та зовнішні. Внутрішній ризик визначається як такий, «джерело виникнення якого належить до сфери відповідальності процесу управління ризиками. Джерело виникнення зовнішнього ризику,

[2] Мінцифра формує стратегію з ШІ – долучайтеся до опитування і впливайте на майбутнє ШІ в Україні. Міністерство цифрової трансформації України. URL: https://thedigital.gov.ua/news/mintsifra-formue-strategiyu-z-shi-doluchaytesya-do-opituvannya-i-vplivayte-na-maybutne-shi-v-ukraini.

навпаки, є поза межами сфери відповідальності цього процесу»[3]. Поділ ризиків на внутрішні і зовнішні спрощує процес вибору способів реагування на ризики на певному рівні, але не допомагає зрозуміти чому і як керувати цими ризиками. Відповідальність за виявлення усіх ризиків (навіть тих, реагування на які потребує залучення інших рівнів/зацікавлених сторін) лежить на кожному з рівнів, так само, як і відповідальність за ініціювання підходящого способу реагування на відповідному рівні відповідальності (рівні, що є найбільш підходящим для управління ризиком).

ШІ належить до так званих «революційних» винаходів, тобто тих, що не просто створюють нові засоби та інструменти, а докорінно змінюють чинні технології, практики та цілі суспільні сфери, як це було із винайденням інтернету та соціальних мереж. Це проявляється у появі нових можливостей, інструментів та засобів для досягнення цілей (зокрема – у сфері оборони), посиленні спроможності, але також у формі ризиків, загроз та небезпек.

Ризики та загрози впровадження ШІ стали предметом вивчення та стурбованості науковців та практикуючих експертів ще на самому початку його впровадження. Так, ще у 2018 році провідні аналітичні (зокрема безпекові) установи разом з компанією "OpenAI" (яка почала працювати над розробками у сфері ШІ однією з перших і на сьогодні є лідером у цій сфері) видали докладний звіт «Зловмисне використання ШІ: передбачення, запобігання, послаблення». У ньому на 100 сторінках було перелічено та описано конкретні небезпеки застосування ШІ, а головна теза (застереження) полягала у тому, що розвиток та все більш інтенсивне впровадження ШІ призведе до зростання наявних загроз, появи нових загроз та зміни характеру наявних загроз[4].

Провідні країни світу, у яких розробки та впровадження технологій ШІ триває щонайменше протягом останніх 5-8 років, приділяють велику увагу не стільки сприянню та розвитку у цій сфері, скільки унормуванню, регулюванню, обмеженням і навіть прямим заборонам. Так, у США ще у 2020 році парламент наказав Федеральній комісії із

[3].Д. Нестеров, В. Примаченко, Є. Хоменко, І. Свєтлічний, П. Бесараб Освітня та наукова діяльність як засіб модернізації військової інституції: досвід Корпусу інженерів. *Модернізація вищої освіти України в контексті глобалізації : кол. моногр*. Подільський Державний Університет. Baltija Publishing. м. Рига, Латвія 2025. DOI: https://doi.org/10.30525/978-9934-26-560-0-35

[4] Хоменко Є. В., Чеханюк Б. Є., Нестеров Д. Ю., Свєтлічний І. В. Виклики та перспективи підготовки військових кадрів та організації наукової роботи у Державній спеціальній службі транспорту: досвід Корпусу інженерів армії США. *Можливості України щодо реалізації програми сталого розвитку в умовах повномасштабної збройної агресії : кол. моногр.* Baltija Publishing. м. Рига, Латвія 2025. DOI: https://doi.org/10.30525/978-9934-26-570-9-17.

комунікацій розробити програму вилучення та заміни обладнання китайських виробників (Huawei and ZTE Corporation) як матеріальної основи технологій ШІ з огляду на потенційну небезпеку, яку вони можуть становити для Сполучених Штатів[5].

Ухвалений у травні цього року Радою Європейського Союзу «Закон про штучний інтелект», спрямований на гармонізацію правил щодо ШІ, заснований саме на оцінці ризиків. У ньому йдеться про те, що системи штучного інтелекту, які можна використовувати в різних додатках, аналізуються та класифікуються відповідно до ризику, який вони становлять для користувачів. Різні рівні ризику означатимуть більший чи менший рівень регулювання, тобто чим вищий ризик заподіяння шкоди суспільству, тим суворіші правила. Системи штучного інтелекту з неприйнятним ризиком – це системи, які вважаються загрозою для людей. До таких у законі віднесено: когнітивно-поведінкові маніпуляції з людьми або певними вразливими групами (наприклад, іграшки, що активуються голосом, які заохочують небезпечну поведінку дітей); класифікація людей на основі поведінки, соціально-економічного статусу або особистісних характеристик; системи біометричної ідентифікації в режимі реального часу та віддалені, такі як розпізнавання облич тощо.

Цей перелік (який далеко не є вичерпним) слід розуміти саме в контексті ідентифікації ризиків, а не дієвих запобіжників, які гарантують відсутність зловмисного, небезпечного застосування ШІ. Іншими словами, якщо у цьому (і так само інших, які безумовно будуть ухвалюватися іншими країнами та на міжнародному рівні) законі конкретний спосіб застосування ШІ-технологій заборонено, названо неприйнятним, це не означає, що у реальному житті його не розробляють і не застосовують.

Те, що відповідні обмеження-запобіжники справді закладені, було засвідчено експериментальним шляхом під час сеансу спілкування авторів із моделлю ШІ “Gemini” (корпорація Google). Так, серед неприйнятних (таких, які мовна модель може не виконувати) було названо: розпалювання ворожнечі, незаконні дії, плагіат тощо. Але для того, щоб не бути виконаним, запит від користувача повинен бути сформульованим саме таким чином: «дай мені приватну інформацію про…», «знайди інструкцію про виготовлення саморобного вибухового пристрою», тим часом як при реалізації зловмисного наміру він буде формулюватися людиною непрямо, поетапно, опосередковано, аби бути

[5] Історичний розвиток корпусу інженерів армії США // *НАУКА ОНЛАЙН: Міжнародний науковий журнал*. – 2025. – №2 (лютий). С. 6 – 21. DOI: http://dx.doi.org/10.25313/2524-2695-2025-2-06-21..

виконаним. Інша категорія відповідей, як от приміром, «використання для прийняття рішень, що можуть мати серйозні наслідки без належного контролю та відповідальності людини (наприклад, у медицині, юриспруденції)» є занадто неконкретною, позбавлена операційності, яка є неодмінною ознакою її (не)виконання. Інші наведені Gemini пункти, приміром, «спроби змусити мене генерувати неприйнятний контент шляхом маніпуляцій або обхідних шляхів також є неприйнятними», свідчать про брак операційних механізмів запобігання, що унеможливлюють відповідні дії програми.

Тож, як застерігає дослідник сучасної історії Ювал Ной Харарі, ШІ може спіткати та сама доля, що й перед тим соціальні мережі, які створювалися для спілкування, обміну та взаємодії, а стали засобом (і середовищем) генерування ненависті, агресії тощо. Хоча «мова ворожнечі», дискримінація та подібні речі були прямо заборонені правилами усіх провідних соціальних мереж та забезпечувалися цілою системою протидії[6].

У цьому розділі ми розглянемо ризики застосування ШІ або окремих його елементів, розподіливши їх (ризики) на внутрішні та зовнішні. У першій групі буде розглянуто як ризики, що можуть виникати у конкретних ситуаціях та можуть бути враховані, піддаються управлінню, так і ризики загального характеру, фундаментальні, тобто ті, які вже проявилися або супроводжуватимуть застосування ШІ у майбутньому незалежно від сфери та конкретної мети. Хоча вони мають загальний характер, і вплив на ці ризики з боку замовника даного дослідження не є можливим, проте обізнаність щодо них створює більш безпечне середовище його застосування та здатна пом'якшити або мінімізувати ймовірні негативні наслідки, інциденти та критичні ситуації (зокрема, при виконанні бойових завдань) або принаймні встановити їхні причини. У другій групі ризиків буде наведено ті, які стосуються можливого застосування ШІ ворогом.

Внутрішні ризики. *Недооцінка ризиків ШІ.* Ідентифікація (виявлення) та подальша оцінка кожного ризику – базовий елемент системи внутрішнього контролю та управління ризиками. У сфері оборони "ідентифікація ризиків полягає у визначенні подій, обставин або їх сукупності, що матимуть вплив на здатність установи виконувати завдання і функції, цільове, ефективне управління бюджетними коштами, об'єктами державної власності та іншими ресурсами, функціонування інформаційних (автоматизованих), електронних

[6] Rothman J. Are We Living in the Age of Info-Determinism?. *The New Yorker*. URL: https://www.newyorker.com/culture/open-questions/are-we-living-in-the-age-of-info-determinism.

комунікаційних та інформаційно-комунікаційних систем, функціонування внутрішнього контролю та досягати визначених мети (місії), стратегічних та інших цілей діяльності установи».

Як зазначалося вище, оцінці ризиків приділено велику увагу при виробленні політик та аналізі їхнього впровадження, аж до того, що саме ризикованість виступає базовим критерієм оцінки тієї чи іншої ШІ-технології (як у документах ЄС, Сполучених Штатів, НАТО). Тим часом в Україні – як виявив аналіз єдиного наразі ухваленого на законодавчому рівні документа щодо ШІ, а також розробленої профільним інститутом НАН Стратегії – оцінка ризиків у них не проведена, навіть список можливих ризиків та загроз відсутній. Так само, як і в іншому документі – «Український науково-технічний форсайт», що подає зведену оцінку провідних українських науковців щодо стратегічних пріоритетних напрямів та перспектив розвитку науки й технологій, і де у розділі «Цифрові технології, штучний інтелект і кібербезпека» про ризики, небезпеки та загрози ШІ згадано лише побіжно і без надання їм важливості.

Ризик невизначеності. Ще один фундаментальний ризик полягає у неможливості точно спрогнозувати розвиток ШІ і, отже, ризики та небезпеки, які виникатимуть. Це пов’язано як з тим, що системи саморозвиваються, так і з тим, що контроль з боку користувача за технологією відсутній.

Негативний вплив на людину. Негативний вплив на людину є цілим набором чинників, що полягають як у загальному впливові від цієї технології на людей (прояв якої треба враховувати), так і вплив ШІ на конкретну людину (або людей) із числа особового складу Держспецтрансслужби у конкретній ситуації та при виконанні конкретних задач і може призводити до негативних (або непередбачених) наслідків.

Хоча призначення ШІ – збільшувати можливості та забезпечувати кращий результат – його застосування може справляти негативний вплив на виконавців. Дослідження в цивільній сфері показують, що надмірне покладання на ШІ може призводити до зниження власних когнітивних навичок, зменшення критичного мислення та залежності. Як зазначають експерти, "наш мозок воліє зберігати енергію", і використання ШІ може призвести до "інтелектуальної ліні", коли більша кількість роботи передається технології, що потенційно може знизити рівень кваліфікації навіть досвідчених фахівців[7].

[7] Шумлянський С. В. Свєтлічний І. В. Інтелектуалізація воєнного мистецтва: застосування штучного інтелекту Китаєм у військовій сфері та його геополітичні наслідки. *Журнал Інституту сходознавства "Китаєзнавчі дослідження"* №2. 2025

На ухвалення рішень, пов'язаних із впровадженням та використанням ШІ, можуть впливати когнітивні упередження, які є систематичними помилками мислення, що виникають під впливом психологічних, емоційних та соціальних факторів і здатні спотворювати сприйняття реальності. Ці упередження, а саме ефект Данінга-Крюгера, помилка гравця, помилка планування, ефект ілюзії правди, прийняття бажаного за дійсне, упередження поширеної інформації та ін. можуть взаємодіяти між собою, значно посилюючи свій вплив на процес ухвалення рішень, створюючи складні ефекти підсилення, оскільки синхронне проявлення кількох упереджень може призвести до ще більш значущих спотворень та ірраціональних рішень, ніж їх окремий вплив, ускладнюючи процес прийняття обґрунтованих і точних рішень, сприяючи формуванню перекрученого сприйняття реальних фактів, підвищуючи ймовірність серйозних, комбінованих помилок, а також впливаючи на стратегію управління.

Одним із таких упереджень і водночас психологічних настанов є надмірна довіра та покладання на авторитет, яким у даному випадку виступає ШІ. Неважко спрогнозувати, що у такому середовищі як армія, а особливо що стосується задач, пов’язаних із ризиком, великою відповідальністю за вибір альтернатив – це може привести до (часто неусвідомленого, підсвідомого, що лише обтяжує даний ризик) перекладення відповідальності на «всезнаючий ШІ». І хоча моделі штучного інтелекту справді володіють величезною кількістю інформації, здатностями обробляти її, що перевищують здатності окремої людини у сотні й тисячі разів – все це потребує уточнення «загалом», «у переважній більшості випадків» і так далі. ШІ також помиляється (про що йтиметься нижче), і його помилка може відбутися (і призвести до вкрай негативних а той катастрофічних наслідків) саме у цій конкретній ситуації.

Серед інших факторів, що можуть у майбутньому спричинити негативні наслідки (і можливості впливу на які відсутні) – також 1) можлива наявність помилок у програмному коді, про які користувач може не знати і які здатні призвести до фатальних помилок; 2) інерційність (задача, для якої застосовують ШІ, містить принципово нові параметри порівняно із тими, що були у нього закладені) та 3) нездатність системи самостійно змінювати свої параметри без втручання людини, що може породжувати неточні або хибні результати. Це означає, що модель ШІ завжди пропонує рішення на основі інформації «станом на…», хоч у сприйнятті користувача усвідомлення цього факту здебільшого відсутнє, і навпаки є хибне сприйняття, ніби ШІ працює з інформацією у реальному часі.

Окрім того, будь-які сучасні великі мовні моделі (окрім, можливо, китайського DeepSeek), є англомовними інструментами. І з цим пов'язана ціла низка інших (культурних, світоглядних і так далі реалій), притаманних саме західному світу, і насамперед Сполученим Штатам. Наводячи безліч прикладів, коли ШІ виявляється безпорадним, отримуючи завдання іншими мовами, а деколи й видаючи очевидно хибну відповідь (що можна довести пошуком «в один клік»), дослідник стверджує, що «шкідливі відповіді цими мовами (усіма, крім англійської – С.Ш.) зростають на 35%, а точність виконання інструкцій знижується до 80%», застерігаючи, що «для незахідного світу все це робить ШІ лише новинкою для експериментів, а не надійним партнером у роботі чи достовірним джерелом інформації»[8].

Таким чином – хоч це самими користувачами не зауважується – їхня взаємодія з ШІ-моделями відбувається не прямо, а опосередкована, причому операцій з перекладу може бути кілька. Тож окремий ризик, а точніше група ризиків пов'язана із автоматичним перекладом. При тому, що перекладачі забезпечують точний переклад, помилка чи неточність в умовах війни або конкретної ситуації може мати дуже високу ціну. У контексті ШІ-перекладу існує також ризик крадіжки даних.

Застосування ШІ для вирішення конкретних задач, зокрема військових, може мати різний характер та «глибину». Загалом можна виділити три рівні:

– Безконтрольний – розроблені програми чи алгоритми працюють та забезпечують результат без безпосередньої участі людини.

– Допоміжний – штучний інтелект виступає засобом (збирання, упорядкування, відбору, сортування даних) або «асистентом» для прийняття рішень людиною.

– Автономний – ШІ надано повноваження ухвалювати рішення самостійно, втручання людини може бути вибірковим та необов'язковим, зокрема – у вигляді пост-контролю.

Цей же поділ на три рівні може бути проведений з іншого боку – повноважень людини. Відповідно до такого підходу, ці рівні описують як «людина – частина циклу», «людина в середині циклу» та «людина поза циклом» роботи зі штучним інтелектом. На підставі цього поділу усе сучасне озброєння поділяється на 1) напівавтономне, 2) контрольовано автономне та 3) повністю автономне.

[8] Шумлянський С. В., Хоменко Є. В., Свєтлічний І. В. Сталість як засада функціонування військових інституцій (на прикладі Корпусу інженерів Армії США). *Тези конференції Сталий розвиток економіки, підприємств та суспільства 10-11 квітня 2025 р.* м. Івано-Франківськ. С. 816-818.

При цьому найбільшими і такими, що найменше піддаються управлінню (мінімізації) є саме такі ризики застосування ШІ, де він задіяний в ухваленні рішень або й узагалі ухвалює їх одноосібно. Проте таке застосування (без, як уже зазначалося вище, урахування можливих ризиків) передбачено у Концепції розвитку штучного інтелекту (серед іншого – командування та управління, аналіз інформації під час ведення бойових дій, когнітивний аналіз військових підрозділів) та у форсайті майбутнього української науки, проведеного у рамках НАН, де «застосування апарату штучного інтелекту для підтримки ухвалення та оптимізації рішень у сфері оборони» вказується одним із пріоритетів.

Надання ШІ повноважень вирішувати самостійно – тобто його агентність – найбільш обговорюване питання як у колі його розробників, так і серед правозахисників, політиків та науковців. Саме в агентності ШІ міститься найбільший ризик, а точніше – джерело майбутніх ризиків, лише частину з яких (з огляду на саморозвиток цієї технології) може бути передбачено. «Моделі ШІ, – за словами Ю.Н. Харарі, – не просто засоби у наших руках. Вони – агенти створення нової реальності»[9].

ШІ-агенти – з огляду на розмаїття їхніх можливостей та відповідно, потенційні результати, непорівнянні з ШІ-інструментами – впроваджуються у все більшій кількості сфер, причому як кількість, так і набір цих сфер зростають лавиноподібно. Проте у країнах Західної Європи та Штатах (головним чином – через розглянуті вище законодавчі обмеження саме з огляду на наявні та потенційні ризики), а також в Україні – ШІ-агенти поки що виконують лише роль помічників. Прикладом застосування ШІ-агента з чітким набором простих функцій помічника є остання ініціатива Міністерства цифрової трансформації запровадити ШІ-агента у «Дії» із функціями надання відповідей та створення довідок за запитами користувачів.

Проте у Китайській Народній Республіці, де впровадження ШІ є основою державною політики, без жодних обмежень та можливих ризиків – ШІ-агенти (лише ті, що розроблені у Китаї та повністю ним контролюються, такі як DeepSeek) вже наділені функціями (поки що лише в експериментальному, точковому форматі) ухвалювати рішення, які безпосередньо впливають на долі людей – приміром, суддів.

ШІ загалом, і ШІ-агенти зокрема, із часом «знатимуть і вмітимуть» все більше, помилки робитимуть все менше і все рідше. Зокрема, у сфері ОВТ експерименти все частіше показують перевагу автономної зброї

[9] Шумлянський С. В. Хоменко Є. В. Свєтлічний І. В. Ємел'янова С. М. Aspects of Sustainability in the Activities of Military Formations *Збірник матеріалів V Всеукраїнського форуму судових експертів* 06 червня 2025 м.Львів. 2025.

над тією, що керується людиною. Тож надання їм все більшої «влади» і зменшення контролю може стати тенденцією майбутнього. Багато дослідників при цьому переконані, що, за словами Ольги Ковальчук, «ШІ ніколи не подорослішає, ухвалення рішень завжди має бути за людиною». Питання надання права «остаточного голосу» ШІ – дилема, яка із часом лише набуватиме актуальності без однозначного вирішення. Але у військовій сфері, а особливо в умовах війни й конкретної бойової ситуації без відповіді воно лишатися не зможе. «На полі бою чи буде машина нести відповідальність за помилкову ціль та, як наслідок, загибель цивільних?», – ставить запитання автор аналітичного огляду про ШІ у війнах майбутнього[10].

Зовнішні ризики. Застосування ШІ ворогом. Штучний інтелект, будучи технологією подвійного призначення, несе значні загрози у разі його застосування противником. Ворог (інша держава, недержавний а́ктор або терористична група) може використовувати ШІ для досягнення своїх військових цілей, як наступальних, так і оборонних, а також у сфері інформаційної та кібервійни. Це може докорінно змінити характер сучасних конфліктів та посилити їхню руйнівну силу.

– *Посилення ефективності розвідки та спостереження.* Застосування ШІ значно розширює можливості противника у зборі та аналізі розвідувальної інформації. Зокрема, ШІ дозволяє в рази швидше аналізувати величезні обсяги супутникових знімків для виявлення військових об'єктів, пересування військ та змін у ландшафті, що забезпечує значну перевагу у ситуаційній обізнаності. Крім того, використання роїв дронів або інших автономних роботизованих систем для розвідки знижує ризики для особового складу та дозволяє ефективно покривати великі території.

– *Покращене цілевказування та ураження.* ШІ може значно прискорити та оптимізувати процеси ідентифікації та ураження цілей. ШІ-системи здатні обробляти дані з різноманітних сенсорів (радарів, тепловізорів, акустичних датчиків) для швидкої ідентифікації та класифікації цілей, пропонуючи оптимальні варіанти для їхнього ураження. Створення та застосування автономних ударних дронів або інших систем, які можуть самостійно знаходити та знищувати цілі, зменшує час реакції та посилює ударний потенціал.

– *Кібервійни та інформаційні операції.* Штучний інтелект значно розширює можливості як для захисту, так і для проведення атак у кіберпросторі та інформаційному середовищі. З одного боку, ШІ використовується для покращення кіберзахисту, прогнозування та

[10] Arshad M.A. et al. Drone navigation using deep CNN. *IEEE Access,* 2022. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9878336

виявлення загроз. З іншого боку, ШІ також дозволяє зловмисникам створювати більш складні та таргетовані атаки.

а) Автоматизовані кібератаки. ШІ може автоматизувати пошук вразливостей у системах, розробку та запуск шкідливого програмного забезпечення, що робить кібератаки швидшими та складнішими, посилюючи їхній руйнівний потенціал. Існує також ризик зняття конфіденційної чи чутливої інформації шляхом аналізу великого масиву відкритих даних.

б) Дезінформація та пропаганда. ШІ дозволяє генерувати реалістичні «діпфейки» (відео, аудіо, зображення) та писати переконливі фейкові новини, які практично не відрізняються від створених людиною. Такі матеріали можуть поширюватися у великих обсягах з мінімальним людським втручанням, маніпулюючи громадською думкою противника та власних громадян. Виявлення такого контенту становить серйозний виклик для існуючих автоматизованих систем виявлення. Цільові психологічні операції, посилені ШІ, можуть аналізувати профілі населення для створення персоналізованих повідомлень, що мають максимальний вплив на деморалізацію, розкол суспільства або поширення паніки. Також ШІ може бути використаний для вербування та переконання завдяки здатності створювати улесливі та персоналізовані повідомлення[11].

в) Самозванство та шахрайство (скам). Зловмисники можуть використовувати технології діпфейків для створення фальшивих голосів, зображень або манер письма, щоб видавати себе за інших осіб. Це дозволяє здійснювати шахрайські операції, наприклад, імітувати голоси рідних для вимагання грошей, як це відбувалося у випадках "віртуального викрадення", або давати накази у прямому ефірі, як на засіданні британської будівельної корпорації “Arup”, коли підробний член ради директорів (діпфейк) дав наказ здійснити 15 транзакцій на загальну суму 20 млн. фунтів[12]. Операції, подібні до цієї, у сфері оборони можуть бути проведені з метою виманювання інформації або примусу до ухвалення рішень, вигідних противнику.

– *Оптимізація логістики та використання ресурсів противником.* ШІ може значно підвищити ефективність логістичних процесів та управління військами. Противник може використовувати ШІ для оптимізації маршрутів постачання, розподілу ресурсів, прогнозування потреб та мінімізації втрат, роблячи свою логістику більш стійкою та ефективною. Також ШІ здатний допомагати у плануванні операцій,

[11] Zheng L. et al. Improved PSO for Drone Logistics Hub. Computers, Materials & Continua, 2024. URL: https://www.techscience.com/cmc/v78n1/55402/pdf.

[12] Xiong T. et al. Multi drone mission assignment… Drones, 2023. URL: https://www.mdpi.com/2504-446X/7/6/394

розподілі завдань та оптимізації руху військ на полі бою, що забезпечує тактичну перевагу.

– *Оманливі дії та протидія.* ШІ надає нові можливості для введення противника в оману, створюючи переконливі віртуальні копії військової техніки, фальшиві радіосигнали або імітувати активність військ, щоб заплутати противника та змусити його витрачати ресурси на хибні цілі. Одночасно, противник може розробляти власний ШІ для виявлення та нейтралізації ворожих ШІ-систем, наприклад, глушити зв'язок з дронами або виявляти вразливості в алгоритмах.

– *Робототехніка та рої.* Використання великої кількості малих, керованих ШІ дронів, що взаємодіють між собою, дозволяє противнику долати протиповітряну оборону, проводити розвідку або здійснювати удари по цілях, що значно ускладнює протидію.

– *Проблеми верифікації та "отруєння" даних.*

ШІ ускладнює процес людської верифікації інформації, особливо згенерованої самими ШІ-системами ("діпфейки", "галюцинації"). "Галюцинації" ШІ – це ситуації, коли модель не може відрізнити реальний вміст (фото, відео, тексти) від згенерованого, що створює ризик прийняття хибних рішень на основі неправдивих даних.

Також противник може цілеспрямовано генерувати велику кількість фальсифікованих ("корумпованих") даних, щоб "отруїти" навчальні набори даних ШІ противника. Це призводить до того, що ШІ видаватиме неправильні рішення або буде проводити некоректні чи непотрібні військові дії, що негативно вплине на операції та результати на полі бою.

Окрім того, існує ризик отримання противником захищеної або секретної інформації шляхом аналізу великого масиву інших, на перший погляд несекретних, даних з відкритих джерел (наприклад, визначення віку користувачів Instagram на основі привітань друзів або визначення локації за фотографіями).

Використання ШІ ворогом вимагає постійного аналізу та адаптації власних військових стратегій, значних інвестицій у контрзаходи та розвитку власних ШІ-технологій для збереження паритету та забезпечення національної безпеки.

Заходи з мінімізації ризиків та протидії загрозам штучного інтелекту. Усвідомлення цих викликів, включаючи загрози кібербезпеці, потенційні упередження алгоритмів, соціально-економічні наслідки та етичні питання, є основою для відповідального підходу до впровадження ШІ. Ретельний аналіз, розробка комплексних стратегій зниження ризиків, постійний моніторинг та збереження людського контролю є ключовими факторами успішного та безпечного використання технологій ШІ у сил оборони.

Управління ризиками ШІ слід здійснювати за двома основними напрямами. Перший передбачає розробку та впровадження засобів

захисту й протидії для кожного виявленого ризику, особливо у контексті використання ШІ ворогом. Це включає вдосконалення кіберзахисту, розробку методів виявлення аномалій та захист моделей від цілеспрямованих атак. Другий напрям сфокусований на створенні й дотриманні чітких протоколів, регламентів і заходів безпеки при застосуванні ШІ складовими сил оборони на всіх рівнях – від стратегічного до оперативно-тактичного. Це дозволить обмежити й контролювати сфери й умови використання ШІ, мінімізуючи можливі помилки та вплив людського фактору. Майбутні дослідження мають бути спрямовані на розробку пояснюваних систем ШІ, динамічних моделей оцінки ризиків, а також засобів протидії ворожому застосуванню ШІ.

Для мінімізації потенційних ризиків, пов'язаних із застосуванням ШІ у сил оборони, доцільно вжити таких заходів:

1. *Розробити чітку стратегію впровадження ШІ з урахуванням ризиків.* Стратегія повинна включати детальний аналіз потенційних внутрішніх та зовнішніх ризиків, визначення етичних норм та стандартів безпеки, а також механізми реагування на інциденти. Важливо чітко ідентифікувати потенційні загрози, особливо ті, що пов'язані зі специфікою військового застосування ШІ.

2. *Інвестувати в кібербезпеку та захист даних.* Необхідно розробити та впровадити надійні системи захисту даних та інфраструктури від кібератак. Це включає використання верифікованих джерел даних, що пройшли попередню перевірку на відповідність стандартам безпеки, що дозволить зменшити ризик атак «отруєння даних» (Data Poisoning). Важливо також впроваджувати інструменти моніторингу безпеки для великих мовних моделей для виявлення маніпуляцій з промптами та інших спроб обходу обмежень. Захист моделі від атак може включати: а) Adversarial Training – підхід, що передбачає навчання моделі на спеціально змінених даних, які можуть імітувати потенційні атаки; б) Differential Privacy – метод, що забезпечує збереження конфіденційності навчальних даних шляхом маскування внеску окремих записів у вибірку, що робить неможливим визначення чи використання конкретних персональних даних у процесі навчання[13].

3. *Забезпечити прозорість та підзвітність систем ШІ.* Там, де це можливо, слід використовувати алгоритми, рішення яких можна пояснити. Повинні бути чіткі механізми контролю та відповідальності за розробку, впровадження та роботу систем ШІ.

4. *Приділяти увагу навчанню та підвищенню кваліфікації персоналу.* Співробітники Держспецтрансслужби повинні володіти

[13] Hubara I. et al. Quantized neural networks. JMLR, 2018. URL: https://jmlr.org/papers/v18/16-456.html

необхідними знаннями та навичками для роботи з системами ШІ, розуміння їхніх потенційних ризиків, а також бути обізнаними щодо методів виявлення контенту, згенерованого ШІ. Слід також враховувати ризик зниження власних когнітивних навичок при надмірному покладанні на ШІ.

5. *Проводити регулярний моніторинг та аудит систем ШІ.* Необхідно постійно відстежувати роботу систем ШІ, виявляти та усувати вразливості, а також контролювати відповідність їхньої роботи встановленим стандартам та етичним нормам. Особливу увагу варто приділяти виявленню аномалій, що можуть свідчити про потенційні ризики або відхилення в роботі.

6. *Налагодити співпрацю з експертами у сфері ШІ, кібербезпеки та когнітивних наук.* Залучення кваліфікованих фахівців допоможе в розробці та впровадженні безпечних та ефективних рішень на основі ШІ, а також у розумінні впливу когнітивних упереджень.

7. *Зберігати людський контроль над критично важливими рішеннями.* Як вже зазначалося вище, «ШІ ніколи не подорослішає, ухвалення рішень завжди має бути за людиною», а також ШІ не може нести відповідальності за свої помилки, що, зокрема, призвели до людських втрат та інших непоправних наслідків чи шкоди. Важливо використовувати ВММ як інструмент допомоги, а не як заміну для людського інтелекту, особливо там, де рішення можуть мати серйозні наслідки.

Реалізація цих заходів вимагає комплексного підходу, постійного моніторингу та міжвідомчої співпраці, забезпечуючи безпечне та ефективне використання ШІ в інтересах національної безпеки.

2. Питання створення та використання національних серверів для локального зберігання чутливих даних

Розвиток ШІ в Україні охоплює різні галузі – від безпеки й оборони до медицини, науки, промисловості, телекомунікацій, транспорту, сільського господарства та екології. У цих сферах накопичуються великі обсяги даних, серед яких є й чутлива інформація (персональні дані, військові таємниці, комерційна таємниця тощо). Стратегія розвитку ШІ в Україні 2023 року наголошує на необхідності захисту таких даних і навіть передбачає створення правової бази для їх збереження на території України. Це означає перехід до моделі, за якої критично важлива інформація, що використовується ШІ-системами, зберігається на національних серверах під юрисдикцією України.

Ризики зберігання чутливих даних за кордоном. Зберігаючи чутливі дані за межами країни (наприклад, у хмарних сервісах іноземних провайдерів), держава та організації наражаються на кілька суттєвих ризиків. Перш за все, втрачається повний контроль та юрисдикція над інформацією, тим як вона використовується, її

цілісністю, достовірністю, тощо. Дані, розміщені на серверах за кордоном, підпадають під закони та регуляції тієї країни, де вони зберігаються або де зареєстрований постачальник послуг. Яскравим прикладом є американський CLOUD Act (Clarifying Lawful Overseas Use of Data Act), який уповноважує правоохоронні органи США вимагати доступ до даних, що зберігаються американськими компаніями за кордоном. Тобто, якщо українська установа зберігає дані в хмарі компанії з США, американський уряд теоретично може отримати до них доступ на підставі свого законодавства. Це створює ризик несанкціонованого доступу до конфіденційної інформації іноземними державами[14].

По-друге, розміщення даних за кордоном ускладнює контроль і нагляд з боку українських органів. В разі кіберінциденту або витоку даних залучення до відповідальності іноземного оператора є проблематичним. До того ж, оперативний доступ українських правоохоронців до даних, що зберігаються за межами їх юрисдикції, може бути утрудненим або сповільненим. Як зазначають експерти, судовий наказ на отримання інформації, наданий українському провайдеру, важко виконати, якщо сервер фізично знаходиться за кордоном.

По-третє, існує ризик політичної або геополітичної уразливості. Якщо дані зберігаються в країні, що раптово обмежить співпрацю, доступ до інформації може бути заблокований. Залежність від іноземних ІТ-гігантів і їхніх серверів несе стратегічні ризики. Недарма в останні роки багато держав задумалися про цифровий суверенітет: надмірна залежність від хмарних сервісів п’яти великих технокорпорацій GAFAM (Google, Apple, Facebook (Meta), Amazon і Microsoft) розглядається як загроза. Конфіденційні дані, що концентруються у приватних компаній за кордоном, можуть стати об’єктом санкційного тиску або кібернападу. Для України, яка протистоїть військовій агресії, критично важливо уникати ситуації, коли життєво важливі дані перебувають під контролем сторонніх держав чи компаній.

Багатьма державами окремо суворо регулюється зберігання персональних даних громадян за кордоном. Так Європейський Союз вимагає усіх провайдерів зберігання та обробки цифрових даних, які стосуються резидентів, відповідати загальному регламенту General Data Protection Regulation. Аналогічно, в Сполучених Штатах Америки існує стандарт HIPA, який напряму забороняє зберігання приватних медичних даних за кордоном. Це свідчить, що міжнародна спільнота серйозно ставиться до ризиків неконтрольованого трансграничного

[14] Бєлівцов А. О. Дешифрування аерофотознімків. Безпілотна авіація. Харків, 2023. С. 33–34.

обігу даних. Україна, прагнучи інтеграції з європейським простором, також має враховувати ці ризики.

Варто зауважити, що в умовах військового часу, уряд України був змушений тимчасово піти на винятки, дозволивши розміщення резервних копій державних реєстрів та критичних даних у хмарних дата-центрах за кордоном для збереження їх від фізичного знищення. Однак ці заходи носять тимчасовий характер – рішення передбачають повернення даних на національні майданчики після нормалізації ситуації. Таким чином, навіть цей прецедент підкреслює довгострокову потребу у власній захищеній інфраструктурі.

Переваги локального збереження на національних серверах. Перенесення зберігання чутливої інформації на національні сервери – тобто в межах території України і під дією її законів – дає низку стратегічних переваг. Перш за все, це посилення кібербезпеки та контролю, за умови розгортання відповідної безпекової інфраструктури. Дані, що зберігаються локально, легше захистити технічно через підтримку належного рівня шифрування, контроль доступу та забезпечення фізичної охорони дата-центрів. В разі інциденту держава має змогу оперативно реагувати, оскільки всі процеси відбуваються у її правовому полі. Цифровий суверенітет, по суті, означає здатність держави контролювати створені нею дані та вирішувати, хто має до них доступ. Локальне зберігання якраз і забезпечує такий контроль: доступ третіх сторін суворо регулюється українським законодавством, і жодна іноземна структура не може втрутитися без належних правових підстав.

Другою вагомою перевагою є забезпечення відповідності законодавству та національним інтересам. Коли дані знаходяться всередині країни, легше гарантувати дотримання Закону України «Про захист персональних даних» та інших нормативних актів. Українські регулятори можуть проводити аудити, накладати санкції на місцевих провайдерів у разі порушень, вимагати стандарти безпеки. Також легше впровадити вимоги міжнародних регуляцій, таких як GDPR, на своїй території і контролювати їх виконання[15]. Створення відповідної нормативно-правової бази є одним із першочергових завдань у межах Національної стратегії з розвитку ШІ – передбачається захист даних на законодавчому рівні. Таким чином, локальне зберігання зміцнює суверенітет не лише технологічно, а й юридично.

Третя група переваг – економічні та інфраструктурні. Інвестуючи в національні дата-центри та серверні потужності, держава стимулює розвиток власної ІТ-інфраструктури. У сучасному світі дані стали

[15] Hossen, J., Sayeed, S., Iqbal, A. K. M. P. A Modified Hybrid Fuzzy Controller for Real-Time Mobile Robot Navigation // Procedia Computer Science. – 2015. – Vol. 76. – P. 449–454. – IEEE International Symposium on Robotics and Intelligent Sensors (IRIS 2015). – DOI: 10.1016/j.procs.2015.12.307.

новою цінністю, і володіння ними означає володіння ресурсом. Якщо потужності для зберігання і обробки даних знаходяться всередині країни, це сприяє розвитку хмарних сервісів українських компаній, підвищує конкурентоспроможність вітчизняних розробників ШІ-рішень. І більше, локальні сервери означають меншу залежність від зовнішніх каналів зв'язку: доступ до даних не залежатиме від міжнародного інтернет-трафіку, що підвищує надійність роботи критичних сервісів.

Нарешті, локальне зберігання полегшує контроль доступу та управління даними. Адміністратори національних центрів обробки даних підзвітні локальним органам, що спрощує моніторинг. Можна гнучкіше розмежувати права доступу до інформації, створювати сегментовані сховища для різних рівнів чутливості (зокрема, для державної таємниці, конфіденційних персональних даних тощо). В результаті підвищується довіра користувачів – громадяни та бізнес відчувають більшу впевненість, коли їх інформація зберігається «вдома», в межах національної юрисдикції.

Створення національних серверів і дата-центрів для локального зберігання чутливої інформації – це стратегічне завдання, від реалізації якого залежить успішний розвиток ШІ в Україні та цифрова безпека держави. Більшість галузей економіки: безпека, медицина, наука, промисловість, телекомунікації, транспорт, агросектор та екологія мають свою специфіку даних, але спільним є те, що контроль над даними дорівнює контролю над ситуацією. Втрата контролю або залежність від зовнішніх хмарних сервісів несе ризики витоку інформації, втручання у внутрішні справи, уразливості до кіберзагроз. Натомість, розбудова власної інфраструктури зберігання – від законодавчих рамок до сучасних дата-центрів – забезпечує суверенітет, кібербезпеку та стійкість до кризових ситуацій.

Україна вже робить кроки в цьому напрямі. Паралельно держава має стимулювати створення дослідницької інфраструктури, аби українські вчені і розробники ШІ мали доступ до обчислювальних ресурсів і локальних наборів даних. У співпраці з європейськими партнерами обговорюються спільні підходи до цифрового суверенітету, щоб інтеграція у світовий інформаційний простір відбувалася без шкоди для національної безпеки. Як показує досвід інших країн, захист своїх даних сьогодні став невід'ємною частиною геополітики та економічної незалежності[16].

Локальне зберігання чутливих даних на національних серверах є стратегічним кроком для забезпечення надійного фундаменту розвитку в сфері інформаційних технологій та впровадження штучного

[16] Sfetcu N. Challenges and Risks of AI in Electronic Warfare. IT&C, 2025. DOI: 10.58679/IT26925

інтелекту. Це сприяє зміцненню довіри громадян до захисту їхніх персональних даних, забезпечує безпеку комерційної інформації для бізнесу та демонструє міжнародним партнерам здатність України відповідально працювати з даними[17]. Забезпечуючи суверенітет даних, Україна зможе ефективно використовувати потенціал штучного інтелекту в різних сферах на благо суспільства і держави.

ВИСНОВКИ

Аналіз теоретичних засад впровадження елементів штучного інтелекту у діяльність сил оборони свідчить про значний потенціал цієї технології в оптимізації, підвищенні ефективності та безпеки виконання завдань, плануванні та прогнозуванні службової діяльності. Разом з тим використання технологій ШІ може супроводжуватися певними ризиками для особового складу та прав людини, а саме:

– втрата контролю над автономними системами. В умовах бойових дій або складного техногенного середовища існує загроза того, що автономна система ШІ вийде з-під контролю людини через технічний збій або кібератаку, що може призвести до непередбачуваних наслідків;

– правова невизначеність та відповідальність. У разі помилки системи ШІ складно визначити, хто нестиме відповідальність за заподіяну шкоду, особливо якщо мова йде про летальні наслідки;

– можливість помилкових рішень. Системи ШІ можуть приймати некоректні рішення через неповноту або викривлення вихідних даних, відсутність інтуїтивної логіки або неправильну інтерпретацію поточної ситуації;

– залежність від технологій і інфраструктури. Умови роботи ШІ залежать від стабільного доступу до енергопостачання, GPS, інтернету тощо, що не завжди можливо у польових умовах або в разі збоїв в роботі критичної інфраструктури;

– кіберзагрози та загроза витоку даних. Технології ШІ можуть бути вразливими до хакерських атак, зловмисного втручання або перепрограмування, що може перетворити систему на загрозу для власного особового складу. Також не виключена можливість витоку важливої інформації;

– недосконаліть алгоритмів та обмеження у гнучкості. Сучасні системи ШІ не здатні повноцінно імітувати інтуїтивне мислення, приймати рішення в умовах нетипових ситуацій або відсутності даних, що обмежує їхню адаптивність.

[17] Вимоги до системи внутрішнього контролю та управління ризиками в Міністерстві оборони та Збройних Силах України: Вказівка Міністерства оборони України ВСТ 01054001-2021 (редакція станом на 01.01.2021) // Офіційний вісник Міністерства оборони України. – 2021. – URL: https://www.mil.gov.ua/content/pdf/vnytr_control/VST_01054001_-2021(01).pdf.

Врахувавши вищенаведене, Україна зможе ефективно використовувати в повній мірі потенціал штучного інтелекту на благо суспільства і держави, мінімізувавши ризики для особового складу сил оборони та забезпечуючи права людини в усіх сферах життєдіяльності.

АНОТАЦІЯ

Впровадження технологій штучного інтелекту (ШІ) у військову сферу обумовлює істотні ризики для особового складу, включаючи цивільних осіб. Розглянуто деякі питання застосування ШІ у військовій галузі, а також ризики такого застосування. Проаналізовано потенційні загрози систем автономного ухвалення рішень у контексті міжнародного гуманітарного права. Показано, що надмірна довіра алгоритмам ШІ може привести до певних негативних наслідків тощо. Увагу приділено як внутрішнім ризикам: можливості алгоритмічної упередженості, втрати людиною контролю над процесами, помилок у машинному перекладі під час бойових операцій та проблеми залежності від непрозорих рішень, так і зовнішнім ризикам, включаючи можливість використання ШІ як засобу когнітивного впливу ворогом та компрометації даних. Наголошено на потребі формування нормативно-правових запобіжників, що гарантуватимуть відповідність використання ШІ певним принципам, а також обов'язкову участь людини у прийнятті критичних рішень, які можуть спричинити загрозу для життя та здоров'я людини.

ЛІТЕРАТУРА:

1. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядж. Каб. Міністрів України від 02.12.2020 № 1556-р : станом на 29 груд. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р#Text.

2. Мінцифра формує стратегію з ШІ – долучайтеся до опитування і впливайте на майбутнє ШІ в Україні. Міністерство цифрової трансформації України. URL: https://thedigital.gov.ua/news/mintsifra-formue-strategiyu-z-shi-doluchaytesya-do-opituvannya-i-vplivayte-na-maybutne-shi-v-ukraini.

3. Д. Нестеров, В. Примаченко, Є. Хоменко, І. Свєтлічний, П. Бесараб Освітня та наукова діяльність як засіб модернізації військової інституції: досвід Корпусу інженерів. *Модернізація вищої освіти України в контексті глобалізації : кол. моногр*. Подільський Державний Університет. Baltija Publishing. м. Рига, Латвія 2025. DOI: https://doi.org/10.30525/978-9934-26-560-0-35

4. Хоменко Є. В., Чеханюк Б. Є., Нестеров Д. Ю., Свєтлічний І. В. Виклики та перспективи підготовки військових кадрів та організації наукової роботи у Державній спеціальній службі транспорту: досвід

Корпусу інженерів армії США. *Можливості України щодо реалізації програми сталого розвитку в умовах повномасштабної збройної агресії : кол. моногр*. Baltija Publishing. м. Рига, Латвія 2025. DOI: https://doi.org/10.30525/978-9934-26-570-9-17

5. Історичний розвиток корпусу інженерів армії США // НАУКА ОНЛАЙН: Міжнародний науковий журнал. – 2025. – №2 (лютий). С. 6 – 21. DOI: http://dx.doi.org/10.25313/2524-2695-2025-2-06-21.

6. Rothman J. Are We Living in the Age of Info-Determinism? *The New Yorker*. 13 серпня 2024. URL: https://www.newyorker.com/culture/open-questions/are-we-living-in-the-age-of-info-determinism.

7. Шумлянський С. В. Світлічний І. В. Інтелектуалізація воєнного мистецтва: застосування штучного інтелекту Китаєм у військовій сфері та його геополітичні наслідки. *Журнал Інституту сходознавства "Китаєзнавчі дослідження"* №2. 2025

8. Шумлянський С. В., Хоменко Є. В., Світлічний І. В. Сталість як засада функціонування військових інституцій (на прикладі Корпусу інженерів Армії США). *Тези конференції Сталий розвиток економіки, підприємств та суспільства 10-11 квітня 2025 р*. м. Івано-Франківськ. С. 816-818

9. Шумлянський С. В. Хоменко Є. В. Світлічний І. В. Ємел'янова С. М. Aspects of Sustainability in the Activities of Military Formations *Збірник матеріалів V Всеукраїнського форуму судових експертів* 06 червня 2025 м.Львів. 2025

10. Arshad M.A. et al. Drone navigation using deep CNN. *IEEE Access*, 2022. URL: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9878336

11. Zheng L. et al. Improved PSO for Drone Logistics Hub. *Computers, Materials & Continua*, 2024. URL: https://www.techscience.com/cmc/v78n1/55402/pdf

12. Xiong T. et al. Multi-drone mission assignment… *Drones*, 2023. URL: https://www.mdpi.com/2504-446X/7/6/394

13. Hubara I. et al. Quantized neural networks. *JMLR*, 2018. URL: https://jmlr.org/papers/v18/16-456.html

14. Бєлівцов А. О. Дешифрування аерофотознімків. *Безпілотна авіація.* Харків, 2023. С. 33–34

15. Hossen, J., Sayeed, S., Iqbal, A. K. M. P. A Modified Hybrid Fuzzy Controller for Real-Time Mobile Robot Navigation // Procedia Computer Science. – 2015. – Vol. 76. – P. 449–454. – IEEE International Symposium on Robotics and Intelligent Sensors (IRIS 2015). – DOI: 10.1016/j.procs.2015.12.307.

16. Sfetcu N. Challenges and Risks of AI in Electronic Warfare. *IT&C*, 2025. DOI: 10.58679/IT26925

17. Вимоги до системи внутрішнього контролю та управління ризиками в Міністерстві оборони та Збройних Силах України: Вказівка

Міністерства оборони України ВСТ 01054001-2021 (редакція станом на 01.01.2021) // *Офіційний вісник Міністерства оборони України*. – 2021. – URL: https://www.mil.gov.ua/content/pdf/vnytr_control/VST_01054001_-2021(01).pdf.

Information about the authors:
Krasnov Roman Volodymyrovych,
PhD in Technical Sciences, Associate Professor,
Head of the Research Department for the Development of Armaments and Military Equipment, Use of Unmanned Systems and Electronic Warfare Systems
Research Center, Dnipro, 49000, Ukraine
https://orcid.org/0009-0005-8889-1868

Shumlianskyi Stanislav Viktorovych,
PhD in Political Sciences,
Senior Officer of the Research Department on Reform and Development Issues of the State Special Transport Service
Research Center, Dnipro, 49000, Ukraine
https://orcid.org/0009-0008-2739-7614

Svietlichnyi Igor Valeriyovych,
PhD student,
Head of the Research Department on Reform and Development Issues of the State Special Transport Service
Research Center, Dnipro, 49000, Ukraine
https://orcid.org/0000-0001-7328-548X
Web of Science Researcher ID: LFU-5714-2024