5. MIMO Systems for Military Communication/Applications / Jindal S. K. *International Journal of Engineering Research and Application*. 2016. Vol. 6, Issue 3. P. 22–33.

6. Impact of sea cluttering and wave shadowing on U2S MIMO channel model incorporating UAV-ship 6D motion in maritime environments / N. Ahmed et al. *Vehicular Communications*. 2025. Vol. 55. Art.: 100963. DOI: https://doi.org/10.1016/j.vehcom.2025.100963

DOI https://doi.org/10.30525/978-9934-26-645-4-64

TOPICAL SECURITY RISKS AND CHALLENGES OF INTEGRATING ARTIFICIAL INTELLIGENCE INTO MILITARY APPLICATIONS

АКТУАЛЬНІ ПРОБЛЕМИ БЕЗПЕКИ ЗАСТОСУВАННЯ ЕЛЕМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ У ВІЙСЬКОВІЙ СФЕРІ: ВИКЛИКИ ТА ЗАГРОЗИ

Khomenko Yevhen Valentynovych
PhD student, Commander
Research Center
Dnipro, Ukraine
https://orcid.org/0009-0006-7006-3439

Хоменко Євген Валентинович
аспірант, Начальник
Центр досліджень
м. Дніпро, Україна

Bulhakova Svitlana Oleksandrivna
Head of Personnel Department
Research Center
Dnipro, Ukraine
https://orcid.org/0009-0001-2952-0371

Булгакова Світлана Олександрівна
начальник відділення персоналу та стройової
Центр досліджень
м. Дніпро, Україна

Svietlichnyi Igor Valeriyovych
PhD student, Head of the Research Department
Research Center
Dnipro, Ukraine
https://orcid.org/0000-0001-7328-548X
Researcher ID: LFU-5714-2024

Свєтлічний Ігор Валерійович
аспірант, начальник відділу досліджень
Центр досліджень
м. Дніпро, Україна

Повномасштабна збройна агресія рф проти України породжує нові виклики та обумовлює необхідність інноваційних трансформацій та суттєвих змін у підходах до вирішення проблеми безпеки та застосування елементів штучного інтелекту у військовій сфері, включаючи технічне забезпечення морської безпеки. Ввзаємосумісність з НАТО у галузях технічного забезпечення безпеки зумовлює необхідність розвитку спроможностей всіх складових сил оборони України. Досліджуючи досвід функціонування Корпусу інженерів армії США (далі – Корпус), з'ясовано, що виявлені підходи та інновації можуть становити інтерес для подальших прикладних та теоретичних наукових досліджень у сфері безпеки та оборони України. Корпус – складова Міністерства Армії США і водночас окрема урядова агенція зі складною, побудованою на різних принципах внутрішньою структурою, що виконує суто військові, суто цивільні та змішані функції і має 250-річну історію своєї діяльності [1].

Досвід Корпусу у контексті застосування елементів штучного інтелекту (далі – ШІ) для забезпечення безпеки та виконання завдань за призначенням характеризується дослідженням та врахуванням як ризиків і викликів, так і шляхів запобігання ним, які потребують особливої уваги. Окремі аспекти діяльності Корпусу залишаються малодослідженими в українській науковій літературі. Як зазначають дослідники (Хоменко Є. В., Бондар, В. Ю., Нестеров Д. Ю., Свєтлічний І. В., Шумлянський С. В., Ємел'янова С. М., Коротченко О. О.) більшість доступних даних базується на опублікованих звітах Корпусу та офіційних веб-сайтах [2].

Ризик у будь-якій сфері (життєдіяльності) визначається як потенційна можливість настання несприятливих подій. Існування ризику передбачає наявність обов'язкових умов – можливість настання випадкової події, негативної за своїми наслідками, наявність матеріального або іншого збитку від такої події, а також діяльності, пов'язаної з цією подією. Ризико-орієнтовані підходи передбачають ідентифікацію, оцінку, планування заходів протидії, впровадження контролю та моніторинг ризиків з урахуванням постійних змін середовища і загроз [3]. 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 проєкту» [4]. 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 (існують розбіжності у кількісному вимірюванні ризику та стратегіях реагування). 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).

У сфері безпеки та 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 комунікаційних та інформаційно-комунікаційних систем, функціонування внутрішнього контролю та досягати визначених мети (місії), стратегічних та інших цілей діяльності установи. Фундаментальна невизначеність пов'язана з тим, що наразі неможливо передбачити, яким шляхом буде розвиватися штучний інтелект, а отже – й які саме ризики та загрози виникатимуть у процесі цього розвитку [5].

Штучний інтелект (далі – ШІ) є технологією подвійного призначення, а тому несе значні загрози. Це означає, що ШІ зазвичай пропонує рішення на основі того набору знань, які мав під час свого останнього оновлення. Проте в користувача часто виникає помилкове враження, ніби штучний інтелект завжди працює із найсвіжішою інформацією тут і зараз. Додатково варто зазначити, що всі сучасні великі мовні моделі працюють головним чином англійською мовою. Це тягне за собою, як зазначає Станіслав Шумлянський [6], багато культурних і світоглядних обмежень, характерних для західної культури. На практиці це видно по тому, що при роботі іншими мовами ШІ може видавати некоректні або навіть очевидно неправильні відповіді, які легко перевірити. Штучний інтелект може використовуватись як для наступальних, так і для оборонних цілей, а також у сфері інформаційної та кібервійни, що здатне радикально вплинути на характер сучасних конфліктів та зробити їх значно більш руйнівними. Його застосування дає змогу багатократно підвищити результативність розвідки й спостереження, дозволяючи швидко й ефективно аналізувати великі обсяги супутникових знімків, виявляти військові об'єкти та пересування сил, а також зміни у рельєфі місцевості – це забезпечує перевагу у ситуаційному контролі. У галузі кібербезпеки і інформаційних операцій штучний інтелект розширює можливості захисту і проведення атак, дозволяє швидко прогнозувати, виявляти та нейтралізувати загрози в кіберпросторі та інформаційному середовищі.

Усвідомлення ризиків, загроз для кібербезпеки, потенційної упередженості алгоритмів, соціально-економічних впливів та етичних питаннь лежить в основі відповідального впровадження ШІ. Успішне та безпечне використання технологій в оборонній сфері залежить від ретельного аналізу, створення продуманих стратегій зниження ризиків, постійного моніторингу й збереження контролю людини. Управління ризиками штучного інтелекту має два головні напрями: перший полягає у впровадженні засобів захисту і протидії для кожного з виявлених ризиків із фокусом на протидію ворожому застосуванню ШІ (наприклад, підвищення кіберзахисту, виявлення аномалій, прикриття моделей від цільових атак); другий – у встановленні і дотриманні чітких протоколів, регламентів і заходів безпеки під час використання ШІ на всіх рівнях оборонних структур. Вказане допоможе обмежити й контролювати сфери застосування ШІ та знизити ймовірність помилок й людського фактора [7]. Подальші дослідження доцільно спрямовувати на використання ШІ в освіті, створення пояснюваних систем ШІ, динамічних моделей оцінки ризиків і засобів протидії, особливо у період повоєнного відновлення.

На сьогодні Україна використовує багато систем штучного інтелекту у сфері оборони [8] і війна стала військовою лабораторією штучного інтелекту для компаній Palantir, Microsoft, Amazon, Google, Clearview AI та інших, які співпрацювали з українськими збройними силами, надаючи передові технології [9]. ШІ вже широко застосовується та охоплює майже усі види діяльності збройних сил та оборонного відомства. Наразі в Україні немає чітко визначених нормативно-правових актів, які б регулювали специфічні аспекти використання ШІ у сфері оборони, тому питання забезпечення безпеки використання ШІ у військовій сфері потребує подальших наукових досліджень.

Література:

1. Хоменко Є. В., Свєтлічний І. В., Чеханюк Б. Є., Бондар В. Ю. Історичний розвиток корпусу інженерів армії США. *Міжнародний науковий журнал Наука онлайн.* 2025. № 2 (лютий). С. 6–21. DOI: http://dx.doi.org/10.25313/2524-2695-2025-2-06-21. URL: https://nauka-online.com/publications/other/2025/2/06-21/

2. Шумлянський С. В., Хоменко Є. В., Свєтлічний І. В. Сталість як засада функціонування військових інституцій (на прикладі Корпусу інженерів Армії США). *Сталий розвиток економіки, підприємств та суспільства* : матеріали ІІ міжнар.наук.-практ. конф. Івано-Франківськ, 10–11 квітня 2025 р. С. 816–818. https://doi.org/10.5281/zenodo.15383186

3. Краснов Р. В., Шумлянський С. В., Свєтлічний І. В. Використання штучного інтелекту у військовій галузі: ризики та загрози для особового складу. *Human rights and public governance* : Scientific monograph. Riga, Latvia : Baltija Publishing, 2025. 772 с. С. 356–376. https://doi.org/10.30525/978-9934-26-608-9-19

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. Нестеров Д. Ю., Примаченко В. Ф., Хоменко Є. В., Свєтлічний І. В., Бесараб П. М. Освітня та наукова діяльність як засіб модернізації військової інституції: досвід Корпусу інженерів. *Модернізація вищої освіти України в контексті глобалізації* : кол. моногр. Кам'янець-Подільський. Подільський Державний Університет. Рига, Латвія: Baltija Publishing, 2025. С. 75–84 DOI: https://doi.org/10.30525/978-9934-26-560-0-35.

6. Хоменко Є. В., Бондар В. Ю., Свєтлічний І. В., Шумлянський С. В. Перспективи розвитку наукової і науково-технічної діяльності в Держспецтрансслужбі та окремі вектори змін. *V Всеукраїнський форум судових експертів* : збірник матеріалів. Львів, 6 червня 2025 р. Одеса : Юридика, 2025. С. 490–493. URL: https://ondise.minjust.gov.ua/wp-content/uploads/2025/08/forum_ondise_law__2025.pdf

7. Свєтлічний І. В., Шумлянський С. В., Будз В. П. Застосування штучного інтелекту у забезпеченні виконання військових завдань: ризики та загрози. *Актуальні засади логістики та підтримки військ у російсько-українській війні*: матеріали наук.-практ. семінару. Київ, 30 квітня 2025 р. Київ : НУО. 2025. С. 86–90. https://www.scribd.com/document/922719667/Nuou-eBook

8. Будз В. П., Костиря С. В., Свєтлічний І. В. Розмінування як основа повоєнного відновлення України. *Воєнні конфлікти та техногенні катастрофи: історичні та психологічні наслідки* : збірник тез V Міжнародної наукової конференції «Воєнні конфлікти та техногенні катастрофи: історичні та психологічні наслідки», 15–16 квітня 2025 р. / упоряд. А. А. Криськов, М. Я. Блавіцький, Н. В. Габрусєва. Тернопіль : ФОП Паляниця В. А., 2025. С. 128–130. URL: https://tntu.edu.ua/storage/pages/00001091/Zbirnyk_VC-2025.pdf

9. Краснов Р. В., Свєтлічний І. В., Ємел'янова С. М. Алгоритмічні методи протидії перманентним ризикам ШІ у контексті правового

забезпечення військового управління із застосуванням машинного навчання. *Міжнародна науково-практична конференція «Проблеми правового забезпечення оборони України»* 10.09.2025 м. Київ. НУО 2025. С. 100-105. URL: https://ippi.org.ua/sites/default/files/problemi_pravovogo_zabezpechennya_oboroni_ukrayini._zbirnik_materialiv_2025_1.pdf

DOI https://doi.org/10.30525/978-9934-26-645-4-65

GRAPHICAL HARDWARE FOR TRAINING SYSTEMS BUILDING

ГРАФІЧНІ АПАРАТНІ ЗАСОБИ ПОБУДОВИ ТРЕНАЖЕРНИХ СИСТЕМ

Shapo Vladlen Feliksovych
PhD, Associate Professor,
Weaponry Department Professor
Naval Institute of the National
University "Odesa Maritime Academy"
Odesa, Ukraine

Шапо Владлен Феліксович
кандидат технічних наук, доцент,
професор кафедри озброєння
Інститут Військово-морських сил
Національного університету
«Одеська морська академія»
м. Одеса, Україна

Досвід сучасної війни в Україні показав, що сучасні інформаційні технології (ІТ) грають величезну роль на усіх рівнях: тактичному, оперативному та стратегічному, від окремого бійця до величезних військових угрупувань, на відстанях від кількох метрів до сотень кілометрів. Різноманітними обчислювальними системами оснащені численні безпілотні апарати (наземні, повітряні, надводні, підводні), які також можуть поєднуватися у рої, приціли снайперських гвинтівок, командно-штабні машини (КШМ), радіолокаційні станції (РЛС), центри прийняття рішень та управління військами, окремі танки, кораблі, літаки, гелікоптери, ракети, мережеві вузли передавання даних, супутникові системи зв'язку і т.д. Саме якісне та високопрофесійне засвоєння можливостей подібної техніки дозволить отримати принципово нові можливості та забезпечити перемогу над у кілька разів кількісно переважаючим ворогом.

Але сучасна військова техніка, ставши у ряді випадків дуже складною і надаючи принципово нові можливості, є при тому дуже коштовною і може коштувати до кількох десятків мільйонів доларів або євро (танки, кораблі, літаки і т.д.). Її практичне освоєння