

В. І. Барило

ТЕХНОЛОГІЇ ШТУЧНОГО ІНТЕЛЕКТУ В УДОСКОНАЛЕННІ СИСТЕМ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ

Анотація. У тезах розглянуто роль технологій штучного інтелекту (ШІ) як чинника якісного удосконалення зразків озброєння та військової техніки (ОВТ) в умовах російсько-української війни. Узагальнено основні напрями інтеграції ШІ: інтелектуальна обробка розвідувальних даних і автоматичне розпізнавання об'єктів, підвищення автономності безпілотних систем, підтримка ухвалення рішень у системах управління, супровід життєвого циклу техніки. Окремо проаналізовано використання ШІ противником для масштабування інформаційно-психологічних операцій (ІПСО) та можливості застосування ШІ для їх виявлення і протидії. Обґрунтовано необхідність відповідального застосування ШІ зі збереженням людського контролю та запропоновано шляхи удосконалення ОВТ і системи протидії ворожим ІПСО, зокрема в освітньому процесі закладів вищої освіти.

Ключові слова: штучний інтелект; озброєння та військова техніка; безпілотні системи; підтримка ухвалення рішень; радіоелектронна боротьба; інформаційно-психологічні операції; дипфейки; когнітивна стійкість.

Abstract. The theses examine the role of artificial intelligence (AI) technologies as a driver of qualitative improvement of weapons and military equipment in the context of the Russian-Ukrainian war. The main areas of AI integration are summarized: intelligent processing of intelligence data and automatic object recognition, increasing the autonomy of unmanned systems, decision support in command and control systems, and support of the equipment life cycle. The adversary's use of AI to scale up information and psychological operations (IPSO) and the potential of AI for detecting and countering them are analyzed separately. The need for responsible use of AI with preserved human control is substantiated, and ways to improve weapons and military equipment and the system for countering hostile IPSO are proposed, including within the educational process of higher education institutions.

Keywords: artificial intelligence; weapons and military equipment; unmanned systems; decision support; electronic warfare; information and psychological operations; deepfakes; cognitive resilience.

Російсько-українська війна засвідчила, що в сучасному збройному протистоянні перевагу здобуває не лише сторона з більшою кількістю озброєння, а та, яка швидше збирає, обробляє та використовує дані. Технології штучного інтелекту (ШІ) стають ключовим засобом скорочення циклу «виявлення – ухвалення рішення – ураження», підвищення живучості й ефективності зразків озброєння та військової техніки (ОВТ), а також зменшення ризиків для особового складу. Засади цього процесу закладено в Законі України «Про національну безпеку України» та Стратегії воєнної безпеки України, побудованій на концепції всеохоплюючої оборони, а Концепція розвитку штучного інтелекту в Україні визначає сферу оборони одним із пріоритетних напрямів застосування ШІ.

Навесні 2026 р. при Міністерстві оборони України створено Defense AI Center «AI», місія якого полягає в перетворенні ШІ на реальну перевагу на полі бою та прискоренні інноваційного циклу – від аналізу даних із фронту до інструментів управління й автономних систем; окремим завданням визначено формування підходів до якості, захисту, стандартизації та використання бойових даних для навчання нових систем. Побудова армії, посиленої штучним інтелектом, передбачає три напрями: ухвалення рішень на основі даних, застосування ШІ у засобах ураження та скорочення бюрократичних процедур; одним із флагманських проєктів центру є система аналізу бойових даних і планування операцій SPECTR.

Аналіз досвіду бойового застосування та відкритих джерел дає змогу виокремити п'ять основних напрямів удосконалення ОВТ на основі ШІ. Перший – інтелектуальна обробка розвідувальної інформації. Алгоритми комп'ютерного зору забезпечують автоматичне

виявлення, класифікацію та супроводження об'єктів на відео з безпілотних літальних апаратів (БпЛА), супутникових знімках і даних наземних сенсорів, а методи злиття даних формують єдину картину обстановки.

Другий напрям – підвищення рівня автономності безпілотних систем. Бортова обробка даних забезпечує навігацію за візуальними орієнтирами без сигналів супутникових систем і збереження керуваності БпЛА у разі втрати зв'язку з оператором унаслідок дії засобів радіоелектронної боротьби (РЕБ). За оцінкою керівництва центру «А1», саме ІІІ дає змогу дронам працювати в умовах РЕБ та автоматично виявляти ворожу техніку за лічені секунди. Водночас повної автономії на полі бою поки не досягнуто, а людський нагляд за рішеннями щодо застосування засобів ураження залишається критично важливим.

Третій напрям – інтелектуальна підтримка ухвалення рішень у системах управління військами: прогнозування дій противника, аналіз великих масивів бойових даних, генерування варіантів рішень та автоматизація штабних процедур. Дослідники обґрунтовують гібридний підхід, за якого ІІІ виконує функцію інструмента підтримки рішень командира, а не повністю автономної бойової системи.

Четвертий напрям – супровід життєвого циклу ОВТ. Аналіз телеметрії та даних експлуатації дозволяє перейти від планово-попереджувального до прогнозного технічного обслуговування, завчасно виявляти несправності. Цифрові двійники й імітаційне моделювання скорочують терміни розроблення та випробувань нових зразків, а алгоритми оптимізації підвищують ефективність логістики. П'ятий напрям – застосування ІІІ в засобах РЕБ і протиповітряної оборони для аналізу радіоелектронної обстановки, класифікації сигналів і раннього виявлення повітряних цілей за даними різномірних сенсорів.

Водночас ІІІ є технологією подвійного призначення, яку противник активно використовує в інформаційно-психологічному протиборстві. За даними Центру протидії дезінформації при РНБО України, Росія перетворила генерацію контенту за допомогою ІІІ на модульну систему атак: зафіксовано понад тисячу синтетичних відео, адаптованих під конкретні цільові аудиторії. Для військовослужбовців просуваються тези про «марність боротьби» та «коллапс фронту», дискредитується командування, а для цивільного населення й партнерів – тези про втому від війни та недоцільність підтримки України. Кінцевою метою є руйнування самого поняття об'єктивної істини, коли будь-який реальний доказ можна оголосити «черговим дипфейком». Вітчизняні дослідники наголошують, що автоматизовані системи на базі ІІІ підвищують масштабність і швидкість ІІІСО та роблять їх менш передбачуваними, а оновлена стратегія НАТО вперше визначає дезінформацію та інформаційні операції з використанням ІІІ окремим предметом занепокоєння Альянсу.

Відповідно, ІІІ має стати й ключовим інструментом захисту інформаційного простору. До перспективних напрямів належать: моніторинг медіапростору для раннього виявлення ворожих наративів і відстеження їх поширення; виявлення скоординованої неавтентичної поведінки та ботмереж на основі поведінкового й мережевого аналізу; детектування синтетичних зображень, аудіо- та відеоматеріалів шляхом мультимодального аналізу; підтвердження походження контенту за допомогою цифрових підписів і маркування. Проте дослідження засвідчують, що автоматизоване виявлення дезінформації є лише частиною рішення: моделі погано розпізнають іронію та сарказм, чутливі до мовних і культурних особливостей та якості навчальних даних, тому найефективнішими є системи з участю людини в контурі перевірки. Стратегія інформаційної безпеки України визначає протидію дезінформації та інформаційним операціям держави-агресора і розвиток медіаграмотності суспільства серед пріоритетів державної політики.

Проте вирішальним чинником протидії ІІІСО залишається когнітивна стійкість особового складу та суспільства – здатність критично оцінювати інформацію, перевіряти джерела та розпізнавати маніпулятивні прийоми. Тому значну роль відіграють заклади вищої освіти, які можуть інтегрувати до навчальних дисциплін модулі з розпізнавання ІІІ-згенерованого контенту і практикуми з верифікації інформації.

Упровадження ІІІ в ОВТ супроводжується й специфічними ризиками: вразливістю моделей до навмисного спотворення вхідних даних, «отруєння» навчальних вибірок, загрозами кібербезпеці, а також етико-правовими викликами щодо дотримання норм міжнародного гуманітарного права. На небезпеку надмірної автоматизації рішень щодо застосування сили та

необхідність збереження людського контролю над ними вказують дослідники автономних систем озброєння.

Узагальнення викладеного дає змогу запропонувати такі шляхи удосконалення зразків ОВТ і системи протидії ворожим ІІСО:

- ✓ розбудова національної інфраструктури бойових даних (збирання, розмітка, стандартизація, захищене зберігання) як основи для навчання вітчизняних моделей ІІІ;
- ✓ перехід до модульної відкритої архітектури ОВТ з оперативним оновленням програмного забезпечення та моделей ІІІ, пріоритетний розвиток бортової обробки даних і навігації, стійких до впливу РЕБ;
- ✓ інтеграція засобів ІІІ в єдину систему ситуаційної обізнаності та управління з урахуванням стандартів сумісності НАТО;
- ✓ створення системи випробувань, верифікації та сертифікації моделей ІІІ, зокрема перевірки їх стійкості до протидії противника;
- ✓ нормативне визначення рівнів автономності ОВТ із закріпленням принципу людського контролю над застосуванням засобів ураження;
- ✓ формування єдиного контуру моніторингу інформаційного простору із засобами автоматизованого виявлення ботомереж і дипфейків та протоколом оперативного реагування;
- ✓ системна підготовка фахівців з аналізу даних, операторів безпілотних систем і фахівців зі стратегічних комунікацій, розвиток медіаграмотності курсантів і студентів.

Технології ІІІ перетворилися з допоміжного інструмента на системоутворювальний чинник удосконалення ОВТ: вони підвищують швидкість і точність розвідки, автономність безпілотних систем, якість управлінських рішень та ефективність супроводу життєвого циклу техніки. Ключовими умовами їх упровадження є якісні й захищені бойові дані, модульна архітектура ОВТ та інституційна основа, прикладом якої є Defense AI Center «A1».

Масштабування противником ІІСО за допомогою генеративного ІІІ вимагає поєднання автоматизованих засобів моніторингу й детектування синтетичного контенту з експертною перевіркою та розвитком когнітивної стійкості особового складу і суспільства. Розвиток військового ІІІ має ґрунтуватися на принципах відповідального використання, сумісних із підходами НАТО, з безумовним збереженням людського контролю над застосуванням сили. Перспективами подальших досліджень є розроблення методик оцінювання надійності моделей ІІІ у складі ОВТ та навчальних програм з протидії ІІСО для закладів вищої освіти.

Список використаних джерел:

1. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. <https://zakon.rada.gov.ua/laws/show/2469-19#Text> (дата звернення: 04.10.2026).
2. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України»: Указ Президента України від 25.03.2021 № 121/2021. <https://zakon.rada.gov.ua/laws/show/121/2021#Text> (дата звернення: 04.10.2026).
3. Міноборони: Інновації під час війни – чим займатиметься Defense AI Center «A1». Урядовий портал. 01.04.2026. URL: <https://www.kmu.gov.ua/news/minoborony-innovatsii-pid-chas-viiny-chym-zaimatymetsia-defense-ai-center-a1> (дата звернення: 04.10.2026).
4. Міноборони розробляє ІІІ-систему SPECTR для аналізу бойових даних. LB.ua. 25.09.2026. URL: https://lb.ua/tech/2026/09/25/768886_minoboroni_rozroblyaie.html (дата звернення: 04.10.2026).
5. ІІІ як інструмент когнітивної війни: росія масштабує виробництво дипфейків. АрміяInform. 23.04.2026. URL: <https://armyinform.com.ua/2026/04/23/shi-yak-instrument-kognityvnoyi-viiny-rosiya-masshtabuye-vyrobnyczstvo-dypfejktiv/> (дата звернення: 04.10.2026).

Баріло Валентина Іванівна – асистент кафедри захисту України та безпеки життєдіяльності Полтавського національного педагогічного університету імені В.Г. Короленка, м. Полтава, вул. Остроградського, 2, інд. 36000, e-mail: valusha271182@gmail.com ORCID <https://orcid.org/0009-0002-7033-798X>

Valentina Barilo— assistant at the Department of Health and Safety of Ukraine, Poltava National Pedagogical University named after V.G. Korolenka, Poltava, Ostrogradskogo St., 2, Ind. 36000, e-mail: valusha271182@gmail.com ORCID <https://orcid.org/0009-0002-7033-798X>