

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У РОЗВІДУВАЛЬНІЙ ДІЯЛЬНОСТІ В УМОВАХ СУЧАСНОЇ ВІЙНИ

У статті досліджується роль штучного інтелекту (ШІ) у розвідувальній діяльності в умовах сучасної війни. Проаналізовано можливості ШІ у зборі, обробці та аналізі розвідувальної інформації, а також його вплив на процеси ухвалення рішень в умовах гібридних конфліктів. Окрема увага приділена застосуванню алгоритмів машинного навчання та нейронних мереж у задачах розпізнавання образів, прогнозування загроз і виявлення закономірностей у великих масивах даних. Показано основні виклики, пов'язані з упровадженням ШІ у розвідку, зокрема питання кіберзахисту, стійкості до інформаційних маніпуляцій та інтеграції з системами електронної боротьби. Обґрунтовано необхідність системного підходу до використання ШІ у розвідувальній діяльності для забезпечення інформаційної переваги.

Ключові слова: розвідка, штучний інтелект, машинне навчання, розвіддані, аналіз даних, військова розвідка.

Постановка проблеми. Сучасні збройні конфлікти характеризуються насиченістю інформаційного середовища, високою динамічністю, широким використанням технологій електронної боротьби та асиметричних загроз. Розвідувальні операції, які відіграють ключову роль у забезпеченні інформаційної переваги, стикаються з новими викликами: збільшенням обсягів даних, які підлягають аналізу, швидкістю прийняття рішень та потребою в інтеграції результатів із системами управління військами.

Традиційні методи аналізу інформації не забезпечують належну швидкість та ефективність ухвалення рішень у режимі реального часу. Використання ШІ відкриває нові можливості щодо автоматизації процесів збору та обробки розвідданих, підвищення точності прогнозування дій противника, створення інтелектуальних систем підтримки командирів у прийнятті рішень. Проте процес впровадження ШІ може стикнутися і з певними проблемами – від технічних, таких як стійкість алгоритмів в умовах впливу перешкод, до етичних і правових – застосування автономних систем.

Враховуючи швидкість еволюції технологій та їхню роль у сучасних конфліктах, постає необхідність у системному аналізі не тільки можливостей, які відкриваються із застосуванням ШІ в ході проведення розвідувальних заходів, але і можливих проблем, пов'язаних із цим. У цьому контексті актуальним є дослідження практичного досвіду використання таких технологій у сучасних війнах, зокрема на основі подій останніх років.

Аналіз останніх досліджень і публікацій. Питання застосування штучного інтелекту у військовій сфері активно розглядається вітчизняними та зарубіжними дослідниками. У статті [1] обґрунтовується доцільність використання алгоритмів машинного навчання для підвищення точності й швидкості обробки військової інформації.

У дослідженні [2] автори акцентують увагу на ризиках і загрозах, пов'язаних з інтеграцією інтелектуальних технологій у військові системи, зокрема на етичних і правових аспектах.

Зарубіжні дослідження приділяють значну увагу практичним аспектам застосування ШІ. На платформі IEEE Xplore опублікована стаття [3], автори якої провели аналіз оборонних проєктів США та ЄС, у яких ШІ застосовується для обробки розвідданих і прогнозування загроз.

У статті [4] досліджено трансформацію стратегій і тактик під впливом ШІ, звертається увага на ризики подвійного використання технологій та необхідність тісної взаємодії між військовою і цивільною сферами.

Особливої уваги заслуговує аналітичний звіт [5], у якому розглянуто розвиток українських систем з елементами автономності, насамперед у сфері безпілотних технологій та ситуаційної обізнаності.

Авторами публікації [6] проведено аналіз сучасних тенденцій у застосуванні ШІ для автоматизації розпізнавання цілей, обробки зображень та інтеграції розвідувальних потоків, що безпосередньо стосується інформаційного забезпечення бойових дій.

Окремий напрям досліджень охоплює роль ШІ у військових комунікаціях. У статті [7] розглядаються перспективи використання алгоритмів машинного навчання у тактичних мережах, зокрема для адаптивного управління каналами зв'язку та підвищення стійкості інформаційного обміну.

Теоретичне підґрунтя організаційно-етичних викликів застосування ШІ у бойових системах розкривається у дослідженні [8], де автори аналізують баланс між автономністю алгоритмів і контролем з боку людини.

Таким чином, сучасні українські та зарубіжні дослідження демонструють широкий спектр підходів до вивчення військового застосування ШІ: від технічних і правових аспектів до аналізу конкретних оборонних проєктів і етичних обмежень. Водночас жодна з проаналізованих праць не здійснює системного розгляду застосування ШІ саме у розвідувальній діяльності в умовах сучасної війни, що й визначає актуальність запропонованої статті.

Метою статті є комплексне дослідження ролі штучного інтелекту в ході проведення розвідувальних операцій в умовах сучасної війни.

Виклад основного матеріалу. Розвідувальна діяльність завжди була одним із ключових елементів забезпечення воєнних операцій, однак у ХХІ столітті її значення зросло до рівня стратегічного чинника, який безпосередньо визначає успіх чи невдачу збройного протистояння для однієї зі сторін. Якщо раніше основною метою розвідки було отримання інформації про сили та наміри противника для підготовки операцій, то сучасні війни, зокрема гібридного характеру, вимагають багатовимірного, безперервного та високоточного інформаційного забезпечення.

Особливістю сучасних збройних конфліктів є різке зростання обсягів даних, що надходять із різномірних джерел: технічних сенсорів, супутникових систем, безпілотних літальних апаратів, електронної розвідки, відкритих інформаційних ресурсів (OSINT), а також від агентурних мереж. Це формує проблему «інформаційного перевантаження», коли кількість даних значно перевищує можливості людини щодо їх оперативного аналізу.

У той же час характер сучасних бойових дій визначається високою швидкістю змін: обстановка на полі бою може змінюватися за лічені хвилини. Це вимагає від розвідки не лише збору відомостей, але й швидкої обробки та формування висновків у режимі реального часу. Традиційні методи, засновані на ручній аналітичній роботі, в таких умовах втрачають ефективність, оскільки не забезпечують своєчасності прийняття рішень.

Крім того, сучасна розвідка має справу з противником, який активно застосовує широкий спектр засобів маскування, дезінформації та радіоелектронної боротьби. Це ускладнює виявлення істотних ознак його діяльності, підвищує вимоги до точності аналітичних висновків і до стійкості розвідувальних систем в інформаційному середовищі.

Таким чином, розвідка, в цілому, стає досить складною інтегрованою системою, яка не може ефективно функціонувати без автоматизації процесів збору та аналізу інформації. Саме в цих умовах набуває актуальності можливість застосування штучного інтелекту для забезпечення швидкості, точності і адаптивності розвідувальної діяльності.

Сучасна розвідувальна діяльність характеризується багатоканальністю джерел інформації, серед яких провідну роль відіграють технічні засоби спостереження. Використання ШІ значно розширює можливості збору даних, дозволяючи автоматизувати процеси обробки сигналів, зображень і текстових повідомлень та підвищувати ефективність систем раннього виявлення загроз.

Одним із ключових напрямів застосування ШІ є обробка супутникових знімків та аерофотозйомки з безпілотних літальних апаратів (БПЛА). Сьогодні алгоритми комп'ютерного зору здатні автоматично виявляти військову техніку, фортифікаційні споруди, переміщення особового складу та інші об'єкти інтересу, навіть за умов часткового маскування або низької якості зображення. Це суттєво скорочує час між отриманням інформації та її використанням у процесі прийняття рішень.

Не менш важливим є застосування ШІ у сфері радіоелектронної та сигнальної розвідки (SIGINT). Алгоритми глибокого навчання дозволяють ідентифікувати різні типи сигналів, розрізняти характерні патерни у роботі засобів зв'язку противника та виявляти нетипові активності у спектрі. Це створює передумови для швидкого виявлення джерел випромінювання та можливого визначення структури ворожих мереж управління.

Окремий напрям становить автоматизація збору інформації з відкритих джерел (OSINT). ШІ дає змогу в реальному часі аналізувати великі обсяги текстових, фото- та відеоматеріалів із соціальних мереж, новинних порталів та інших відкритих ресурсів. Використання алгоритмів класифікації та

обробки природної мови (NLP) дозволяє виявляти зміни в інформаційному полі, оцінювати достовірність повідомлень та ідентифікувати джерела потенційних витоків інформації.

Важливим завданням для сучасних армій є створення розподілених сенсорних мереж, які надають можливість об'єднати різноманітні інформаційні джерела – від супутників і БПЛА до наземних сенсорів і кіберрозвідки. Штучний інтелект у таких системах виконує роль «фільтра», який зменшує надлишковість інформації, виділяє релевантні дані та передає їх у пункти управління для наступного аналізу.

Застосування ШІ в ході збору розвідувальних даних дозволяє суттєво підвищити ефективність розвідки завдяки скороченню часу між фіксацією об'єкта і його аналітичною інтерпретацією, зменшити інформаційне навантаження на аналітиків та підвищити точність виявлення загроз.

Але найціннішим є можливість штучного інтелекту не тільки зменшити надлишковість і цим прискорити виявлення об'єктів інтересу, але й обробити та проаналізувати розвіддані. На цьому етапі командуванню надаються високотехнологічні можливості щодо прийняття швидких та максимально виважених рішень.

Одним із визначальних інструментів є методи машинного навчання, які дозволяють класифікувати дані, виявляти закономірності та проводити кластеризацію інформації. Наприклад, алгоритми можуть автоматично виділяти групи сигналів, які належать до одного комплексу засобів зв'язку противника, або встановлювати відповідності між переміщенням техніки і зміною характеру радіообміну.

Нейронні мережі та алгоритми глибокого навчання знаходять застосування у розпізнаванні зображень, голосових сигналів та текстових повідомлень. Це дозволяє, зокрема, відстежувати переміщення підрозділів на основі фото- та відеоматеріалів, ідентифікувати головних осіб у радіоперехопленнях або аналізувати інформаційні повідомлення у соціальних мережах.

Особливе значення має інтеграція різноманітних джерел інформації. У сучасних умовах робота розвідувальних органів ґрунтується на комплексному використанні даних із HUMINT (агентурної розвідки), SIGINT (радіоелектронної), GEOINT (геопросторової), MASINT (інструментальної) та OSINT (відкритих джерел). ШІ здатен об'єднувати ці масиви у єдину систему, автоматично усуваючи дублювання, виявляючи суперечності та формуючи інтегровану картину обстановки.

Застосування алгоритмів аналізу природної мови (NLP) відкриває нові можливості в роботі з великими текстовими потоками – від перехоплених повідомлень до масиву публікацій у соціальних мережах. Це дозволяє не лише ідентифікувати ключові теми та настрої, але й виявляти ознаки інформаційно-психологічних операцій противника.

Ще одним перспективним напрямом є використання алгоритмів виявлення аномалій. Вони дають змогу автоматично виділяти відхилення від звичайних моделей поведінки противника – наприклад, раптову зміну маршрутів постачання або нетипову активність у радіофері. Такі сигнали можуть слугувати ранніми індикаторами підготовки до операцій чи застосування нових засобів.

Таким чином, ШІ виступає вагомим аргументом у сфері обробки та аналізу розвідданих: він в жодному випадку не замінює аналітика, але значно підвищує його продуктивність, а саме: спроможність швидко виділяти основні загрози та ухвалювати зважені рішення. У цьому контексті зростає роль людино-машинної взаємодії, коли алгоритми виконують рутинну роботу, а відповідні посадові особи можуть зосередитися на стратегічній інтерпретації результатів. Це, у свою чергу, безпосередньо впливає на якість прийнятих командуванням рішень.

Щодо застосування ШІ у прогнозуванні та підтримці прийняття рішень, то тут одним із найважливіших напрямів його застосування є прогнозування можливих дій противника та підтримка командирів у процесі ухвалення рішень. В умовах сучасної війни, де ситуація змінюється з високою динамікою, своєчасне передбачення намірів противника набуває критичного значення.

Завдяки використанню алгоритмів прогновної аналітики ШІ здатний моделювати потенційні сценарії розвитку бойових дій на основі поєднання історичних і поточних розвідданих. Це дозволяє визначати ймовірні маршрути переміщення військових підрозділів противника, прогнозувати його логістичні заходи, а також оцінювати можливість застосування певних видів озброєння у конкретних умовах.

У розвідці все більшого значення набувають системи моделювання оперативної обстановки, що поєднують дані з різних джерел (SIGINT, GEOINT, OSINT тощо) і створюють інтегровану картину поля бою. Алгоритми ШІ у таких системах можуть автоматично виділяти вразливі місця у бойових порядках противника, прогнозувати наслідки його тактичних маневрів і пропонувати варіанти реагування.

Застосування мультиагентних систем, де віртуальні «агенти» імітують поведінку військових формувань у різних сценаріях, дозволяє швидко оцінити ефективність можливих рішень і визначити оптимальну стратегію дій у конкретній обстановці.

Окрему роль відіграють системи підтримки прийняття рішень (Decision Support Systems, DSS), які на основі ІІІ забезпечують командирів і штаб аналітичними висновками у зручному та візуалізованому форматі. Це скорочує час на оцінку обстановки, зменшує ризик людських помилок і дозволяє діяти на випередження.

Важливо підкреслити, що ІІІ у прогнозуванні та підтримці рішень не замінює військового командира, а виконує функцію інтелектуального помічника. Він пропонує варіанти дій, але остаточне рішення залишається за людиною, що забезпечує баланс між високою швидкістю алгоритмічного аналізу та відповідальністю офіцера за бойові дії.

Таким чином, застосування ІІІ у сфері прогнозування та підтримки ухвалення рішень забезпечує значну перевагу у сучасній війні, де час на аналіз і реагування часто вимірюється хвилинами, а інколи й секундами.

Але попри очевидні переваги, застосування ІІІ військовими може супроводжуватися низкою проблем і обмежень, які необхідно враховувати перед його інтеграцією у практику бойових дій. Нижче розглянемо приклади таких проблем.

Проблеми технічного характеру та надійність алгоритмів. У реальних умовах дані часто є неповними, зашумленими або навмисно викривленими противником. Алгоритми машинного навчання, що демонструють високу точність у лабораторних умовах, можуть давати помилки у бойовій обстановці. Надійність роботи ІІІ безпосередньо залежить від якості навчальних вибірок і адаптивності моделей до непередбачуваних ситуацій.

Уразливість до інформаційних маніпуляцій. Противник може цілеспрямовано вводити дезінформацію в інформаційний простір або впливати на вхідні дані сенсорів. Це створює ризик «отруєння даних» (data poisoning), коли алгоритм формує хибні висновки. Крім того, можливе використання технологій протидії нейронним мережам (adversarial attacks), здатних вводити їх в оману навіть мінімальними змінами у вхідних даних.

Кіберзахист і безпека систем. Інтеграція ІІІ у розвідувальні комплекси потребує високого рівня кіберзахисту. Атаки на інфраструктуру, яка забезпечує обчислювальні процеси, можуть призвести до блокування роботи розвідувальних систем або витоку критичної інформації. Тому безпека алгоритмів і комунікаційних каналів є першочерговою вимогою.

Етичні та правові аспекти. Використання автономних систем, що приймають рішення без прямої участі людини, породжує складні морально-правові питання. Залишається відкритим питання відповідальності за наслідки рішень, ухвалених за допомогою ІІІ. Також існує ризик надмірної автоматизації, яка може знизити рівень контролю з боку посадових осіб.

Залежність від технологічного рівня держави та партнерів. Створення і впровадження високотехнологічних систем на основі ІІІ вимагає значних ресурсів, науково-технічного потенціалу та доступу до обчислювальної інфраструктури. Країни, що не мають власних розробок у цій сфері, ризикують потрапити в залежність від зовнішніх постачальників.

Отже, впровадження ІІІ у військову розвідку є складним процесом, що поєднує технічні, організаційні, правові та етичні виклики. Подолання цих обмежень є необхідною умовою для повноцінного використання інтелектуальних технологій у сучасних збройних конфліктах.

Майбутнє військової розвідки безпосередньо пов'язане з подальшою інтеграцією технологій ІІІ. Тенденції розвитку свідчать про те, що у найближчі роки ІІІ поступово стане невід'ємною частиною багаторівневих систем збору та аналізу даних, створюючи основу для нових форм інформаційного протиборства.

Перспективним напрямом є створення комплексів, де алгоритми ІІІ здатні не лише аналізувати інформацію про електромагнітну активність, але й адаптивно перешкоджати діям противника. У сфері кіберрозвідки ІІІ може автоматично виявляти аномалії у мережевому трафіку та передбачати кібератаки ще до їх реалізації.

Розвідка майбутнього передбачатиме створення єдиних інформаційних середовищ, де об'єднуються відомості з супутників, БПЛА, сенсорних мереж, соціальних медіа та кіберпростору. ІІІ відіграватиме центральну роль у такій інтеграції, забезпечуючи автоматичну валідацію, очищення та уніфікацію інформації.

Міжнародний досвід свідчить про те, що військові структури США, НАТО, Ізраїлю та інших держав активно розвивають напрями застосування ШІ у розвідці. Для України важливо вивчати цей досвід, водночас розробляючи власні технології, адаптовані до умов гібридної війни та ресурсних обмежень. Особливе значення має розвиток співпраці з партнерами у сфері обміну даними, створення спільних дослідницьких програм і підготовки кадрів.

У подальшому потребують опрацювання питання забезпечення стійкості алгоритмів до інформаційних атак, розробка методів пояснюваного ШІ (Explainable AI) для підвищення довіри до систем, а також розробки стандартів безпеки та етичного використання ШІ у військовій сфері.

Таким чином, перспективи розвитку свідчать про трансформацію військової розвідки в інтегровану інтелектуальну систему, де людина і машина діятимуть у тісній взаємодії. ШІ стане не просто інструментом автоматизації, а найважливішим елементом забезпечення інформаційної переваги у сучасних і майбутніх війнах.

Висновки

Розвідувальна діяльність у сучасній війні набуває стратегічного значення, визначаючи здатність військ діяти на випередження та забезпечувати інформаційну перевагу. У цих умовах використання штучного інтелекту відкриває нові можливості для збору, обробки та аналізу даних, прогнозування загроз і підтримки процесу прийняття рішень.

Аналіз наукових публікацій засвідчив, що, хоча питання впровадження ШІ у військовій сфері досліджується досить активно, більшість робіт зосереджені на загальних технічних, правових та етичних аспектах. Недостатньо висвітленим залишається саме вузький сегмент – застосування ШІ у розвідувальній діяльності в умовах сучасних збройних конфліктів.

Основні результати дослідження свідчать про те, що ШІ здатний істотно підвищити ефективність збору даних завдяки автоматизованому аналізу супутникових і аерофотознімків, сигналів зв'язку та інформації з відкритих джерел.

Використання алгоритмів машинного навчання і нейронних мереж дозволяє інтегрувати різноманітні потоки інформації, забезпечуючи формування комплексної картини обстановки.

У сфері прогнозування та підтримки рішень ШІ виступає інтелектуальним помічником, здатним моделювати сценарії дій противника й пропонувати оптимальні варіанти реагування.

Водночас існують суттєві перепони: технічна надійність алгоритмів, ризик інформаційних маніпуляцій, потреба у кіберзахисті, а також правові та етичні аспекти використання автономних систем.

Напрямок подальших досліджень є розроблення науково обґрунтованих підходів до комплексного впровадження технологій штучного інтелекту у систему військової розвідки. Передусім доцільним є вивчення можливостей інтеграції ШІ з автоматизованими системами управління, радіоелектронною боротьбою та кіберрозвідкою для створення єдиного інформаційного середовища ситуаційної обізнаності. Окремого значення набуває формування математичних моделей прогнозування дій противника та оцінки розвідувальної обстановки із застосуванням когнітивних і гібридних підходів машинного навчання. Для України особливо важливим завданням є розвиток власних технологій у цій сфері та підготовка спеціалістів, здатних ефективно застосовувати інтелектуальні системи у військовій розвідці.

Отже, застосування штучного інтелекту у розвідувальній діяльності в умовах сучасної війни не є лише технічною інновацією, а виступає фундаментальним чинником трансформації всієї системи військового управління та забезпечення переваги на полі бою.

Перелік джерел посилання

1. Трофименко О., Логінова Н., Соколов А., Чикунів П., Ахматєєва Г. Штучний інтелект у військовій сфері. *Cybersecurity and Computer Technologies*. Київський університет імені Бориса Грінченка. URL: <https://surl.li/lsbdzc> (дата звернення: 10.07.2025).

2. Гуржій С. Тенденції застосування технологій штучного інтелекту у військово-технічній сфері. *Інститут проблем інформаційного суспільства*. URL: <https://surl.li/uhscoq> (дата звернення: 12.07.2025).

3. Zhang Y., Dai Z., Zhang L., Wang Z., Chen L. and Zhou Y. Application of Artificial Intelligence in Military: From Projects View. *IEEE Xplore Digital Library*. 2021. URL: <https://surl.li/epzoix> (дата звернення: 25.08.2025).
4. Atkinson R. Artificial Intelligence in Modern Warfare. *Military Review*. U.S. Army University Press. 2024. URL: <https://surl.li/uahqij> (дата звернення: 05.06.2025).
5. Bondar K. Ukraine's Future Vision and Current Capabilities for AI-Enabled Autonomous Warfare. *Center for Strategic and International Studies (CSIS)*. 2024. URL: <https://surl.li/kzyuct> (дата звернення: 17.05.2025).
6. Pusztaszeri A., Harding E. Technological Evolution on the Battlefield. *Center for Strategic and International Studies (CSIS)*. 2024. URL: <https://surl.li/igzrlt> (дата звернення: 20.08.2025).
7. Baeza V. M., Parada R., Salor L. C., Monzo C. AI-Driven Tactical Communications and Networking for Defense: A Survey and Emerging Trends. 2025. URL: <https://surl.li/yqjyxa> (дата звернення: 14.09.2025).
8. Feldman P., Dant A., Dreany H. War Elephants: Rethinking Combat AI and Human Oversight. 2024. URL: <https://surl.li/lrroel> (дата звернення: 03.09.2025).

Стаття надійшла до редакції 26.09.2025 р.

UDC 355.45:004.8

K. Tkachenko, S. Kravchenko, O. Novykova

APPLICATION OF ARTIFICIAL INTELLIGENCE IN INTELLIGENCE ACTIVITIES UNDER MODERN WARFARE CONDITIONS

The article explores the role of artificial intelligence (AI) in intelligence activities during modern warfare. It substantiates that the rapid development of information technologies, the increasing volumes of data, and the complexity of armed conflicts require the integration of machine learning algorithms and neural networks into the processes of collecting, processing, and analyzing intelligence data. The study demonstrates that modern intelligence faces the challenge of information overload and the necessity of timely interpretation of heterogeneous data sources – from satellite imagery and signals of electronic intelligence to open-source information and social media. The application of AI enables automated object detection, signal classification, text analysis, as well as integration of data from different domains (HUMINT, SIGINT, GEOINT, OSINT) into a unified operational picture. Particular attention is paid to the use of predictive analytics and multi-agent models that support commanders in decision-making, especially in forecasting enemy actions. The article outlines key challenges hindering the widespread adoption of AI: the technical reliability of algorithms, the risk of manipulation and disinformation, cybersecurity threats, and legal and ethical constraints. It emphasizes the prospects for further research in the development of cognitive systems, the integration of AI with electronic warfare and cyber intelligence, and the advancement of national technological solutions in Ukraine. The scientific novelty of the study lies in its focus on the use of AI specifically in military intelligence, which allows for substantiating its role as a key instrument of achieving information superiority in modern wars. The practical significance of the research is determined by the formation of a foundation for the development of intelligent systems that enhance the analytical capabilities of military structures and ensure effective command and control under the high dynamics of combat operations.

Keywords: artificial intelligence, military intelligence, modern warfare, data analysis, threat prediction, information superiority.

Ткаченко Кирило Миколайович – доктор філософії, заступник начальника кафедри військового зв'язку та інформатизації, Національна академія Національної гвардії України
<https://orcid.org/0000-0001-7678-0363>

Кравченко Сергій Опанасович – кандидат військових наук, доцент, доцент кафедри сухопутних військ, Національний університет оборони України
<https://orcid.org/0000-0001-8188-3113>

Новикова Олена Олександрівна – кандидат технічних наук, доцент, професор кафедри військового зв'язку та інформатизації, Національна академія Національної гвардії України
<https://orcid.org/0000-0003-3557-5210>