КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (25), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.25.161176
УДК 004.89

**Трофименко Олена Григорівна**
к.т.н., доцент, доцент кафедри інформаційних технологій
Національний університет «Одеська юридична академія», Одеса, Україна
ORCID ID: 0000-0001-7626-0886
*trofymenko@onua.edu.ua*

**Логінова Наталія Іванівна**
к.п.н., доцент, завідувачка кафедри інформаційних технологій
Національний університет «Одеська юридична академія», Одеса, Україна
ORCID ID: 0000-0002-9475-6188
*loginova@onua.edu.ua*

**Соколов Артем Вікторович**
д.т.н., доцент, професор кафедри кібербезпеки
Національний університет «Одеська юридична академія», Одеса, Україна
ORCID ID: 0000-0003-0283-7229
*radiosquid@gmail.com*

**Чикунов Павло Олександрович**
к.т.н., доцент, доцент кафедри інформаційних технологій
Національний університет «Одеська юридична академія», Одеса, Україна
ORCID ID: 0000-0003-4959-774412:27
*pavel@onua.edu.ua*

**Ахмаметьєва Ганна Валеріївна**
к.т.н., доцент, доцент кафедри кібербезпеки
Національний університет «Одеська юридична академія», Одеса, Україна
ORCID ID: 0000-0002-0567-902X
*anna.odessitka@gmail.com*

# ШТУЧНИЙ ІНТЕЛЕКТ У ВІЙСЬКОВІЙ СФЕРІ

**Анотація.** Статтю присвячено висвітленню питань впровадження штучного інтелекту у військову сферу. Через стрімкий розвиток інформаційних технологій та зростання обсягів даних використання штучного інтелекту стає все більш актуальним для ефективного застосування новітніх технологій для розв'язання військових задач. Метою роботи є дослідження ролі ШІ в сучасному розвитку оборонної промисловості та аналіз сфер можливого застосування ШІ у військовій галузі. Гіпотезою дослідження є те, що використання штучного інтелекту у діяльності військових може призвести до покращення ефективності та точності прийняття рішень. У статті розглянуто основні можливості застосування штучного інтелекту у військовій сфері, специфіку та переваги його використання. Дослідження вказує на те, що впровадження штучного інтелекту може допомогти виявляти ризики та покращувати планування й прогнозування воєнних операції, а також забезпечувати автоматизацію обліку та аналізу логістичного забезпечення. Для досягнення цієї мети було використано методологію дослідження, яка поєднувала аналіз літературних джерел та проведення дослідження на основі відомостей про впровадження штучного інтелекту у військову галузь. Під час аналізу специфіки використання ШІ у діяльності військових досліджено сфери його успішного впровадження: відеоспостереження, національна безпека та боротьба з тероризмом, військова логістика, автономні та напівавтономні транспортні засоби, кібербезпека, симулятори для навчання військових, роботи зі ШІ на полі бою, медична допомога на полі бою. З'ясовано, що ШІ має великий потенціал ефективного впровадження у військовій сфері, адже впровадження алгоритмів ШІ допомагає у розв'язанні потенційно небезпечних для здоров'я людей воєнних задач та покращують ефективність зброї. Впровадження технологій ШІ в самі різні складові військової діяльності здебільшого показує значно вищу ефективність, порівняно з іншими

технологіями. Загалом технологічні інновації у поєднання зі ШІ наразі стають вирішальним фактором у визначенні успішного результату на полі бою, але вони потребують ретельної підготовки та врахування ризиків у процесі його впровадження.

**Ключові слова:** штучний інтелект (ШІ); військовий ШІ; військова галузь; кібербезпека; машинне навчання; тестування ШІ, нейронні мережі.

## ВСТУП

У сучасному світі штучний інтелект (ШІ, Artificial Intelligence, AI) швидко впроваджується в різні сфери життєдіяльності. Важливу роль він відіграє й у військових технологіях, де його використання відкриває нові горизонти ефективності, точності та обороноздатності.

**Постановка проблеми.** Український та міжнародний досвід локальних війн останніх років показує, що сучасні бойові дії переважно проводяться за умов високої інтенсивності та динаміки, що зумовлює наявність величезних потоків інформації, оброблення якої й оперативні прийняття по ній ефективних рішень потребують багато зусиль і часу, оскільки потрібно враховувати численні можливі чинники. За умов стрімкої зміни обставин на полі бою та потреби вчасного, а краще завчасного реагування і прогнозування можливих сценаріїв розвитку подій, з одного боку, та фактору людської втоми, стресового стану та складності прийняття швидких й ефективних рішень за таких умов — з іншого, впровадження алгоритмів ШІ допомагає у розв'язанні різних, потенційно небезпечних задач та покращує ефективність застосування зброї. Технологічні інновації у поєднання зі ШІ наразі стають вирішальним фактором у визначенні успішного результату бойових дій, тому дослідження спрямовані на їхній розвиток є вельми актуальними.

**Аналіз останніх досліджень і публікацій.** Дослідженню різних аспектів впровадження ШІ у військову сферу присвячені численні наукові публікації вітчизняних і закордонних вчених. Так, у статті [1] досліджено еволюцію ШІ та проаналізовано бачення компанії Gartner щодо розвитку технологій ШІ. В роботі [2] вивчено досвід Ізраїлю з використання ШІ при проведенні військових дій та проведено оцінку можливості застосування цього досвіду в Україні. Дослідження [3] розглядає специфіку застосування ШІ у сфері військової логістики. У роботі [4] відзначено, що інвестиції у розробку та впровадження ШІ та робототехніки у військову сферу дозволять зменшити ризики для життя людей і скоротити витрати на навчання, постачання та утримання персоналу. В дослідженні [5] дійшли висновку, що розуміння оброблення великих масивів даних за допомогою технологій ШІ може надати значні військові переваги, унікальні можливості розвідки та значні покращення в оборонній промисловості. Автори дослідження [6] порівняли особливості військового ШІ, який зосереджений на цілях стратегічної оборони, з цивільним ШІ. В роботі [7] аналізуються загрози використання ШІ в різних галузях та ризики впливу на виконання завдань забезпечення інформаційної безпеки і кібербезпеки, як невід'ємних складових національної безпеки.

Проведений аналіз наявних досліджень свідчить про важливість дослідження можливих сфер застосування ШІ у військовій галузі, а повсюдне впровадження технологій ШІ потребує підвищеної уваги до цього напрямку, й відповідно, глибокого висвітлення питань потенційних переваг та ризиків впровадження ШІ в оборонний сектор.

**Мета статті**: дослідити роль ШІ в сучасному розвитку оборонної промисловості, проаналізувати сфери можливого застосування ШІ у військовій галузі.

## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Наразі інтеграція та залежність від технологій ШІ під час військових операцій у всьому світі стрімко зростає. Це стосується як розширення сфер застосування ШІ в оборонних стратегіях, так і зростання інвестицій у цей сектор. За прогнозами [8], у 2031 році глобальний ринок штучного інтелекту у військовій сфері становитиме приблизно 21,7 млрд доларів США, а до 2032 року він сягне 24,7 млрд доларів США із середньорічним темпом зростання 12,4% протягом прогнозованого періоду з 2024 по 2033 рік.

Представники урядів 54 держав, зокрема країни G7 і Україна, на саміті REAIM погодили спільну декларацію про регулювання норм «м'якого» міжнародного права щодо відповідальної поведінки та державного управління розробленням, розгортанням та використанням ШІ у військовій сфері [9].

Завдяки здатності ШІ розпізнавання об'єктів і звуків, розуміння мови, автономного навчання, його використання відкриває нові перспективи у різних сегментах військової справи. Так, у звіті NATO Science & Technology Organization [10] визначено сфери потенційного впливу ШІ на розвиток обороноздатності країн світу:

- *C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance)* — використання бойовими підрозділами автономних систем з підтримкою ШІ для виконання завдань, які вважаються небезпечними, кропіткими, брудними чи дорогими. Інтеграція ШІ стосуватиметься розширеної індикації та попередження, інструментів управління інформацією, моделей життя, картографування розміщення людей, аналізу соціальних мереж, підтримки прийняття рішень щодо націлювання. Для такого роду задач ШІ покращить процеси прийняття рішень у військових діях, збір, оброблення та оцінювання даних, а також допоможе у визначенні цілей;
- *зброя та її ефективне використання* — ШІ застосовуватиметься для планування траєкторії, уникнення зіткнень, вибору зброї, оцінки пошкоджень у бою та координації наслідків;
- *UxV (безпілотні авіасистеми та озброєння наступного покоління)* — ШІ впливатиме на планування траєкторії, уникнення зіткнень/роїння, допомогу операторам. Динамічне планування місій для автономних систем забезпечуватиметься інтеграцією систем глибокого навчання;
- *планування можливостей* — ШІ підтримуватиме розробку аналітичних рішень для допомоги в довгостроковому плануванні військових операцій, оцінюватиме складні фактори і ланцюги ефектів.

Наразі ШІ продовжує активно розвиватися, з'являються нові проєкти з його використанням у різних військових технологіях [11]. Дослідження та аналіз специфіки використання ШІ у покращенні діяльності військових дозволили виділили вісім сфер (рис. 1).


*Рис. 1. Сфери застосування ШІ у військовій галузі*

**Національна безпека та боротьба з тероризмом**

Інтелектуальний аналіз великих обсягів текстової, графічної, аудіо та відео інформації дозволяє виявляти потенційні терористичні загрози, формувати доказову базу для боротьби з правопорушеннями з метою їх ефективного застосування у сфері національної безпеки. Інструменти та методи, розроблені для безпеки на основі ШІ, постійно вдосконалюється й дозволяють покращити спроможність муніципальних і державних правоохоронних органів до аналізу злочинів, завдяки швидкому доступу до інформації та її інтелектуальному аналізу.

Ефективне опрацювання великих масивів необроблених даних з різних джерел можливе, завдяки застосуванню комбінації різних технологій: інтелектуальний аналіз великих даних (Data Mining), машинне навчання (Machine Learning, ML), онлайнова аналітична обробка у реальному часі (Online Analytical Processing, OLAP), нейронні мережі (Neural Network), розпізнавання образів (Pattern Recognition), обробка природної мови (Natural Language Processing, NLP), прогнозне моделювання (Predictive Modelling) та багато інших. До того ж, застосування генетичних алгоритмів (Genetic Algorithm) як евристичних алгоритмів пошуку гарно зарекомендувало себе у розв’язанні задач оптимізації і моделювання.

Впровадження зазначених технологій в інструменти аналітики та моделювання для критичної інфраструктури дозволить підвищити ступінь готовності до надзвичайних ситуацій і реагування на них, покращити обмін інформацією та комунікаційну сумісність до та після катастроф. Такий ключовий актив врешті решт підвищить ефективність операцій швидкого реагування і навіть моделювання, виявлення й оповіщення про потенційні катастрофічні загрози та попередження надзвичайних ситуацій.

**Військова логістика**

Застосування ШІ у сфері військової логістики допомагає оптимізувати прийняття швидких та ефективних рішень щодо технічного і тилового забезпечення, транспортування зброї та амуніції, постачання продовольства, зв’язку, адже комбінація цих складових є ключовою для успіху військових операцій. Логістика в армії охоплює багато різних функцій своєчасного постачання різної номенклатури озброєння,

боєприпасів, військової техніки, а також її підготовки (ремонту) і зберігання. А отже, величезні потоки динамічно змінюваних даних про наявні логістичні процеси у військовій галузі потребують своєчасного врахування, керування та оптимізації. Така задача є доволі складною, оскільки потребує врахування численних чинників з визначенням та врахуванням можливих ризиків, у тому числі через непередбачені обставини за умов воєнного стану. Саме логістичні помилки можуть спричинити невдачі на полі бою, значні втрати і збитки, тяжкі соціальні та економічні наслідки.

Автоматизація та оптимізація контролю величезних обсягів військової логістики є дуже важливою задачею будь-якої держави. Застосування для управління ланцюгом поставок технологій ШІ і машинного навчання дозволяє перевірити та впорядкувати великі масиви даних для ідентифікації та виявлення підозрілих постачальників [12]. Вже зараз технології ШІ у військовій логістичній мережі поступово замінюють людину з позиції стабілізації певних номінальних функцій, тим самим дозволяють пришвидшити логістичний процес і зробити його більш гнучким.

**Автономні та напівавтономні транспортні засоби**

До цієї категорії роботизованих, військових, транспортних засобів відносять різного плану безпілотні апарати: наземні, літальні, підводні, космічні. Так, ШІ, закладений в операційну систему Lattice, автономного підводного човна Ghost Shark від австралійської компанії Anduril використовує дані з різних сенсорів, комп'ютерне і машинне навчання. Прототипом цього проєкту є менша субмарина Dive-LD від цих же розробників, яка може опускатися на глибину до 6000 метрів, ховаючись від ворожих радарів, і працювати автономно протягом 10 днів. Для порівняння, військові підводні човни з людьми на борту занурюються не більше, ніж на кілька сотень метрів [13]. Ще одним прикладом інтеграції ШІ у військову сферу є безпілотний бойовий літак Loyal Wingman, розроблений компанією Boeing у співпраці з Королівськими австралійськими Військово-повітряними силами (ВПС). Літак може здійснювати автономні польоти, виконуючи завдання за заздалегідь запрограмованими алгоритмами або реагуючи на зміни в реальному часі. Loyal Wingman координує свої дії з пілотованими літаками, обмінюючись інформацією в реальному часі та спільно плануючи операції. ШІ аналізує великі обсяги даних, зібраних сенсорами і розвідувальними системами літака, що дозволяє швидко і точно ідентифікувати цілі, оцінювати бойову обстановку і надавати командиру необхідну інформацію для прийняття рішень. Крім того, ШІ у Loyal Wingman має здатність до самонавчання та адаптації, що підвищує його ефективність та надійність у майбутніх операціях. Літак також може бути оснащений обладнанням для електронної війни, включаючи системи радіоелектронної боротьби, які використовують ШІ для виявлення і придушення ворожих комунікацій та радарів. Використання автономних систем і можливості співпраці з пілотованими літаками відкривають нові горизонти для військової авіації, забезпечуючи підвищення ефективності і безпеки виконання місій. Впровадження систем ШІ та інтелектуальних алгоритмів у навігаційні системи сучасних військових літаків надають можливості для покращеної геолокації та ідентифікації загроз, забезпечують високоякісне інтегроване радарне попередження, гарну ситуаційну обізнаність для швидкого, оптимального прийняття рішень щодо самозахисту та виконання бойових задач. Як наслідок, продуктивність таких систем з часом лише покращується під час наземних (на симуляторах) та льотних випробувань у середовищах зі щільним сигналом [14].

Автономні транспортні засоби для кращого проходження шляху за різних умов використовують різні методи і технології штучного інтелекту: повторювані нейронні

мережі (Recurrent Neural Network, RNN), мережі довготривалої короткочасної пам'яті (Long Short-Term Memory, LSTM) і навчання з підкріпленням (Reinforcement Learning, RL). Спеціальні архітектури нейронної мережі RNN і LSTM здатні інтерпретувати довгі послідовні дані, для яких важливий хронологічний порядок. RL, як потужний інструмент у ML, дозволяє досягати оптимальних результатів у складних середовищах з багатьма правилами та залежностями. У тому самому середовищі людина може бути не в змозі визначити найкращий шлях, навіть маючи чудові знання про навколишнє середовище. Натомість безмодельні алгоритми RL швидко адаптуються до середовища, що постійно змінюється, і знаходять нові стратегії для оптимізації результатів [15]. Крім того, в безпілотних літальних апаратах (БПЛА) для донаведення застосовують технології комп'ютерного зору (Computer Vision, CV), які дозволять аналізувати відеопотоки в реальному часі, знаходити й ідентифікувати об'єкти (автомобілі, людей, артилерію тощо). Тобто в БПЛА штучний інтелект по суті виконує роль цифрового пілота, який прогнозує траєкторію руху об'єкта, розпізнає ціль, концентрується на ній і запам'ятовує її на випадок тимчасового зникнення з поля зору, щоб бути здатним потім відновити полювання.

Зазначені технології ШІ неабияк допомагають військовим, забезпечуючи роботу різноманітних типів безпілотників. Тим самим ШІ дозволяє оптимізувати планування маршрутів, контроль запасів, розподіл ресурсів, підвищуючи ефективність та знижуючи витрати.

**Відеоспостереження**

Відеоспостереження та розвідка є важливою областю виявлення військових об'єктів. Використання ШІ в системах візуального спостереження робить їхній потенціал більш стабільним і точним. Камери відеоспостереження з технологією розпізнавання об'єктів застосовуються в системах моніторингу. Вони використовують розширені алгоритми ШІ та глибокого навчання (Deep Learning, DL) для визначення цілі на зображенні. DL засноване на засадах нейронних мереж та використовує багатошарові архітектури. Наприклад, для автоматичного розпізнавання об'єктів на зображеннях їх потрібно позначати на тренувальних даних. Завдяки цьому нейромережа навчається автоматично визначати особливості об'єктів і пов'язувати їх із відповідними категоріями. Кожен шар у мережі обробляє дані, отримані від попередніх шарів, і передає їх далі [16]. Розроблена в Україні система Griselda використовує ШІ для збору розвідувальних даних. Вона розвивається стрімкими темпами, кожні два тижні відбувається новий спринт із релізом корисного функціоналу. Griselda здатна обробляти велику кількість повідомлень зі безпілотників, супутників, соцмереж та баз даних ворога за лічені секунди. Завдяки цьому стало можливим створення інтерактивної онлайн-карти бойових дій в Україні, що допомагає більш точно та оперативно опрацьовувати й оновлювати дані [17].

Вбудоване в автономну зброю відеоспостереження та розпізнавання цілей насамперед стосується удосконалення військових систем — дронів та роботизованих механізмів. За наявності системи автоматичного самонаведення операторові бойового безпілотника достатньо лише захопити ціль натисканням об'єкта на екрані. Завдяки алгоритмам комп'ютерного бачення, ML та DL, відбувається розпізнавання об'єкта на основі аналізу даних сенсорів для автоматичного наведення та прийняття рішення щодо вибудовування маршруту до цілі. Іншим прикладом такого застосування є виявлення розташування підводних мін, які створюють серйозну небезпеку для руху та транспортування кораблів.

Інтелектуальний аналіз розвідданих та інформації відеоспостережень, яка надходить водночас з різних джерел збору, допомагає вчасно виявляти підготовку можливих ворожих атак, що є важливим для сучасної галузі безпеки.

Яскравим прикладом застосування технологій ШІ є ідентифікація загиблих російських військових, а також пошук причетних до злочинів російських воєнних злочинців. При чому ці технології добре працюють з різними носіями цифрових зображень, і навіть в режимі реального часу. Після «захоплення обличчя» інтелектуальні відеореєстратори каталогізують пошукові дані, зіставляючи обличчя, при цьому можуть враховуватись додаткові метадані: стать, головні убори, колір волосся, перуки, окуляри тощо. Тим самим широкі можливості інтелектуального пошуку покращують результати пошуку, забезпечуючи швидку та точну ідентифікацію. Технологія розширеного виявлення периметра (Advanced Perimeter Detection, APD) використовує алгоритми глибокого навчання для аналізу та розпізнавання рис обличчя, а також для відстеження місця розташування з урахуванням можливого руху людини чи то іншого об'єкта стеження. APD покладається на алгоритми ШІ, які постійно навчаються та адаптуються до різних середовищ. Ця здатність машинного навчання дозволяє системам спостереження і розвідки з часом підвищувати свою точність виявлення людей або транспортних засобів, записувати метадані про їх переміщення та розташування, зменшуючи помилкові спрацьовування та негативні результати [18]. Застосування алгоритмів NLP в системі Griselda дозволяє виявляти ключові дані (імена, адреси, дати, номера телефонів) за певними критеріями текстового пошуку. Нині алгоритми NLP є незамінними для аналізу видобутих розвідданих.

Але на цьому можливості ШІ щодо відеостеження за великими територіями, виявлення підозрілих дій та відстеження людей чи то транспортних засобів у режимі реального часу не вичерпуються. Ще одним напрямом є скоординована атака «роєм», де дрони можуть одночасно обстрілювати цілі, здійснюючи скоординовану ройову атаку. Також вони можуть ефективно використовуватись для виведення з ладу чи знищення ППО противника, спотворення зображення засобів на радарах противника, виявлення місць розташування радарів противника та передачі інформації операторам [19].

**Кібербезпека**

Через високий рівень ризиків витоків даних у військових та оборонних мережах важко переоцінити переваги застосування технологій ШІ для кібербезпеки. Величезні обсяги розвідувальних даних з одного боку та небезпеки їх витоків з іншого зумовлюють високий рівень пріоритету кібербезпеки для армії та уряду будь-якої держави світу. ШІ може відігравати важливу роль у профілактичних заходах для військових, щоб ідентифікувати та оцінювати зловмисне програмне забезпечення. Ідентифікація технічних та програмних інструментів для імплантації зловмисного програмного забезпечення та подальша нейтралізація кіберзагроз у військовій сфері за допомогою машинного навчання можлива ще до того, як зловмисне програмне забезпечення почне активуватися. ШІ і машинне навчання аналізують поведінку мережі, виявляють аномалії, відрізняючи законні транзакції від шахрайських. Машине навчання використовується для пошуку та виявлення зловмисних сценаріїв, первинних заражень, визначення пріоритетів впливу та стримування загроз вторгнення в систему безпеки військової мережі. Алгоритми ШІ сканують та вивчають поведінку файлів та вміст електронних листів на ознаки фішингу, щоб виявити шаблони, схожі на зловмисне програмне забезпечення. Це робить його чудовим інструментом у виявленні нових, незнайомих штамів шкідливих програм, які традиційне антивірусне програмне забезпечення може пропустити.

Загрози кібербезпеці мають різні форми та розміри. Хакери полюють за секретами як військових, так і приватних організацій. Використання технологій ШІ у формі інтелектуальних агентів є доволі ефективним інструментом для захисту від кібератак та оцінювання вразливостей і ризиків у кіберпросторі. Автоматизація на основі ШІ спрощує рутинні завдання логічних перевірок відповідності законодавчим правилам і нормам кібербезпеки та захисту персональних даних, дозволяючи командам із кібербезпеки зосередитися на більш важливих справах, що допускає номінальне залучення до процесів із заміщенням осіб із числа військових. Оптимізація робочих процесів відбувається за рахунок сповіщення та попередження персоналу відділу кібербезпеки про наявні виявлені невідповідності та ризики загроз [17]. Під час потокового аналізу великих обсягів даних у режимі реального часу ШІ здатен визначати закономірності та надавати рекомендації щодо можливостей усунення виявлених вразливостей.

Кваліфіковані зловмисники вишукують і винаходять нові способи та інструменти проникнення, щоб завдати серйозної шкоди. Вони здійснюють атаки й використовують різноманітні способи поширення шкідливого програмного забезпечення, яке може залишатися прихованими в системі тривалий час. Наразі кіберзлочинність викрадає приблизно 1% світового ВВП [20]. Кіберзагрози стрімко розвиваються, тому застосування брандмауерів і антивірусного програмного забезпечення вже недостатньо. Потрібні більш розумні інструменти на основі ШІ, які з часом лише підвищують ефективність та точність виявлення загроз, покращують розуміння активних кіберзагроз, відкривають нові можливості для забезпечення кібербезпеки, включаючи профілактичні заходи.

Добре зарекомендувала себе синергічна взаємодія між платформою розширеного виявлення та реагування на інциденти безпеки (eXtended Detection and Response, XDR), операційним центром безпеки (Security Operations Center, SOC), зосередженим на управлінні загрозами і вразливостями, проактивному моніторингу інцидентів, та набором інструментів і методів для дослідження подій, важливих для кібербезпеки (Security Information and Event Management, SIEM) [16]. Саме SIEM із використанням ШІ та машинного навчання дає змогу стандартизовано використовувати дані журналізації транзакцій з різних інструментів безпеки та забезпечує розширений моніторинг великих наборів даних шляхом збору й аналізу подій безпеки і контекстних джерел даних у реальному часі. Хмарна платформа XDR за допомогою ШІ оптимізує процеси виявлення, дослідження, реагування та моніторингу кіберзагроз у реальному часі. XDR враховує найдрібніші деталі, сприяючи виявленню раніше непомічених загроз. Завдяки використанню потужностей аналізу великих даних, XDR надає кібербезпековим командам гнучкість, масштабованість та можливість автоматизації виявлення загроз. Ці інструменти із застосуванням технологій ШІ допомагають інтенсифікувати проактивне виявлення та аналіз потенційних кіберзагроз у поєднанні з діями реагування на інциденти та загрози у боротьбі з кіберзлочинністю [21].

Загалом традиційне антивірусне програмне забезпечення покладається на відомі сигнатури шкідливих програм, а ШІ відстежує і вивчає дії зловмисного програмного забезпечення, щоб знайти навіть невідомі варіанти. Система безпеки на основі ШІ сканує на наявність зловмисного програмного забезпечення та ізолює підозрілі файли або ж блокує доступ у разі несанкціонованих спроб зловмисників отримати конфіденційні дані. Тим самим ШІ допомагає експертам з кібербезпеки зменшити ризики злому та посилити безпеку шляхом аналізу та виявлення загроз. Хоча програмні системи кібербезпеки на базі ШІ мають певні ризики та вади, проте партнерство між людьми та ШІ здатне створити більш безпечне майбутнє в діяльності військовослужбовців.

**Симулятори для навчання військових**

Симуляції на основі ШІ пропонують реалістичне середовище для тренувань військових, дозволяючи їм відпрацьовувати бойові сценарії та набувати нових здібностей. Впровадження ШІ в автоматизовані інтелектуальні тренажери є гарним засобом симуляції різноманітних, складних ситуацій і задач під час підготовки військових. При цьому важливо, що технологія інтелектуальної системи навчання забезпечує високий рівень взаємодії та глибокий якісний аналіз, щоб допомогти відточити навички військовослужбовців у навчанні. Поширено такі симулятори використовуються як віртуальні тренажери для навчання бойових льотчиків. Оскільки експлуатація літаків і повітряного простору стає дедалі складнішою, то використання тільки традиційних методів навчання не дозволяє всебічно підготувати пілотів до непередбачуваної природи реальних умов польоту. Використання технологій ШІ та ML в пілотних навчальних програмах можуть симулювати широкий спектр сценаріїв: від поломки обладнання до несприятливих погодних умов. Керовані ШІ симулятори польотів здатні створювати високодеталізовані динамічні середовища, які з неймовірною точністю імітують реальний світ. Навчальні програми зі ШІ пропонують сценарії, які адаптуються в режимі реального часу до дій пілота, забезпечуючи рівень інтерактивності та реалізму, який раніше був недосяжний. Так, система Air-Guardian, розроблена в Лабораторії комп'ютерних наук і штучного інтелекту Массачусетського технологічного інституту (MIT CSAIL) стежить за очима, щоб визначати предмети на численних моніторах, на яких спрямовує погляд пілот, і тим самим в нейронній системі формуються так звані карти помітності. Ці карти помітності в Air-Guardian допомагають пілотам і системі ШІ розпізнавати за допомогою маркерів уваги потенційні ризики та реагувати на них набагато раніше, ніж традиційні системи [22].

Наразі ведуться розробки над навігаційними системами на основі ШІ, які не залежатимуть від супутників, які є цілями під час війни і можуть бути виведені з ладу. Тож замість використання супутникової навігації військові зацікавлені у навігаційній системі на основі ШІ, яка використовуватиме магнітні поля Землі. Для цього відповідну інтелектуальну систему треба навчити звертати увагу на магнітне випромінювання Землі і при цьому ігнорувати сторонні сигнали, наприклад, електромагнітні сигнали, створювані самими літаками [23].

Перспективи розвитку і використання таких інтелектуальних систем для симуляторів та кооперативного керування виходять за межі авіації й поширюється на широкий спектр робототехніки, завдяки їх диференційованості та адаптивності через наскрізний процес навчання до вимог ситуації.

**Роботи зі ШІ на полі бою**

На відміну від автономних та напівавтономних транспортних засобів зі ШІ, роботи зі ШІ зосереджені переважно не на розв'язанні логістичних задач, а саме на бойових задачах в ролі автономних систем озброєння. Системи озброєння на основі ШІ можуть автономно ідентифікувати, відстежувати та вражати цілі за мінімальної участі людини. Тим самим мінімізуються ризики шкоди життю та здоров'ю людей, а водночас зростає ефективність військових операцій.

Так, автоматичні турелі ТГП і Волля (Wolly) від української компанії DevDroid є кулеметними установками, які дозволяють керувати кулеметом дистанційно через комп'ютер і використовують комп'ютерний зір для пошуку та відстеження цілей — безпілотників та ворожих солдатів. Нейромережа вміє знаходити їх на відстані до 1000 метрів. Заявлено, що на модуль ТГП можна встановити автомати й кулемети: ПКТ, АК-

47, АК-74 і Grot. Ця турель може працювати без підзарядки протягом 7 діб, а важить від 35 кілограмів (легка версія) до 110 кілограмів (важка версія для бойових машин). Wolly має зменшену вагу та доступна для пересування однією людиною. Системи працюють з використанням ШІ в двох режимах: ручному й автоматичному. Бойові модулі Wolly і ТГП автоматично знаходять цілі на полі бою, наводяться на них, налаштовують балістику, а від оператора потрібно лише натиснути кнопку «вогонь». При цьому оператор може перебувати в безпечному місці за 100 метрів від вогневої позиції. Для, того аби ТГП могла вести вогонь по рухомій мішені, розробники оснастили її датчиком орієнтації, надали можливість рухатися у трьох площинах і навіть при нахилі у 30 градусів вирівнювати зброю по горизонту та правильно вираховувати балістику [24].

Іншим відомим прикладом роботизованих мобільних систем зі ШІ є робопес Spot від американської корпорація Boston Dynamics, який допомагає знешкоджувати мінометні снаряди та касетні боєприпаси і тим самим дозволяє зменшити ризики підриву людей при розмінуванні. Біологічний робот Spot має камери і датчики спереду, ззаду та з боків, може автономно пересуватися, знаходити та уникати перешкоди, слідувати заздалегідь визначеному маршруту, а також розпізнавати сигнали оточення та діяти за відповідними сформованими програмами навчання. Цей робот гарно показав себе в ролі сапера при розмінуванні деокупованих територій України. Він за допомогою маніпулятора може перетягувати у спеціальні ями непідірвані міни з метою їх нейтралізації, підривати разом до 100 снарядів, вміє автоматично, без допомоги людини повторювати виконання завдань, навіть у густих лісових масивах і в польових умовах між деревами [25].

Використання ШІ для покращення наведення зброї дозволили створити «розумні гвинтівки», які самі розпізнають ціль. «Розумний приціл» автоматичної гвинтівки від американської компанії Tracking Point здатен розпізнавати цілі в об’єктиві, маркувати їх і допомагати точному наведенню прицілу. Захоплена в прицілі ціль позначається відповідним маркером і буде стріляти тільки, коли стрілок правильно наведе дуло гвинтівки. При захопленні цілі приціл аналізує 16 різних параметрів. які можуть вплинути на точність, а саме: температура повітря, напрямок і швидкість вітру, тремтіння рук, віддача, вологість і падіння кулі під дією сили тяжіння тощо [26].

Поки людство не дійшло до того, щоб застосовувати на полі бою повністю автономну зброю на основі ШІ. Проте різними арміями світу стрімко розробляються, тестуються, вдосконалюються та впроваджуються численні роботизовані комплекси і зброя з використанням технологій ШІ, завдяки їх надзвичайній ефективності, порівняно з дорогими, застарілими військовими системами.

**Медична допомога на полі бою**

Захист здоров’я та життя солдатів на полі бою — одна з головних цілей впровадження сучасних технологій для цілей стратегічного планування та прийняття рішень військовими командирами.

Швидка медична допомога не завжди доступна на полі бою, як через відсутність медиків у певному районі, так і через травми поза рамками навичок наявного медика, або через хибні підходи при сортуванні важкопоранених. Переважно на полі бою попит на медичний потенціал значно перевищує наявний потенціал. Важко переоцінити важливість залучення роботизованих транспортних систем на основі ШІ, здатних вивезти пораненого з поля бою в більш безпечне місце, де йому зможуть надати необхідну медичну допомогу та стабілізувати стан здоров’я.

Системи ШІ мають великий потенціал щодо використання у військовій медицині, допомагаючи в прийнятті рішень та оптимізуючи бойові медичні операції. На жаль є

певні складнощі та перешкоди, як складність та багатофакторність таких систем, так і через дорожнечу. Військові системи охорони здоров'я складно трансформувати. Перешкоди на шляху реалізації можливостей ШІ для військової медицини зумовлені відсутністю високоякісної інфраструктури великих даних, ручного введення даних в електронну медичну карту та паралельне традиційне ведення історії лікування в паперовій формі.

Хоча ШІ не є панацеєю для вирішення всіх проблем, його потенційно потужні інструменти дозволять значно оптимізувати надання медичної допомоги пораненим. Застосування ШІ сприятиме прийняттю рішень у широкому діапазоні медичних можливостей, як-от: сортування масових поранених, вибір платформи евакуації, географічний розподіл медичних підрозділів, матеріально-технічне поповнення та акредитація постачальників [27].

Важливим є розробка та застосування алгоритмів ШІ щодо оптимізації сортування поранених за місцем травми та масових втрат. Адже критично важливо швидко та коректно розподілити втрати, визначивши військовослужбовців, які ще можуть безпечно повернутися до виконання обов'язків, і тим самим збільшити бойовий потенціал війська, а яких потрібно евакуювати та визначити рівень догляду, які вони потребують. Адже люди можуть ухвалювати відповідні рішення не оптимально, лише на основі зовнішнього вигляду пацієнта та обмеженого набору деяких інших даних. Сильна сторона ШІ полягає в тому, що пошук закономірностей у величезних обсягах даних може пришвидшити та покращити процес вибору ефективних рішень щодо сортування, адже ШІ особливо ефективний із зображеннями та голосовими даними. При цьому сортування травмованих пацієнтів можна буде робити за допомогою моніторингу короткого аудіо/відеозапису в поєднанні з даними фізіологічних і біомедичних параметрів (температура тіла, частота серцевих скорочень, ЕЕГ, ЕКГ тощо) із переносних пристроїв у режимі реального часу. Це дозволяє лікарям працювати більш продуктивно.

Крім того, ШІ можна поєднувати з роботизованими хірургічними системами і роботизованими наземними платформами для виконання дистанційної хірургічної підтримки та рятувальних операцій у зонах бойових дій. Наприклад, медичні консультації можуть бути запропоновані через автоматизовану платформу.

Потенціал ШІ для військової медицини є значним, але треба розвинути критичну інфраструктуру, перш ніж системи військової охорони здоров'я зможуть оптимально використовувати цю трансформаційну технологію для контролю, діагностування та лікування постраждалих від травм на полі бою. Медичний ШІ зможе допомагати медикам діагностувати травми, спостерігати за пацієнтами та надавати допомогу, коли негайна евакуація пацієнта неможлива. Крім того, програмні алгоритми ШІ надаватимуть медику певну підтримку в ухваленні рішень щодо вибору засобів лікування травматичних ушкоджень важкопоранених бійців.

## ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Під час аналізу специфіки використання ШІ у покращенні діяльності військових досліджено сфери його успішного впровадження: відеоспостереження, національна безпека та боротьба з тероризмом, військова логістика, автономні та напівавтономні транспортні засоби, кібербезпека, симулятори для навчання військових, роботи зі ШІ на полі бою, медична допомога на полі бою. ШІ має великий потенціал ефективного впровадження у військовій сфері. Впровадження технологій ШІ в самі різні складові

військової діяльності здебільшого показує значно вищу ефективність, порівняно з іншими технологіями.

При цьому важливо зважати на ризики, пов'язані з використанням систем ШІ, які зростають разом з їхніми перевагами. Переважно потенційні небезпеки використання ШІ стосуються відсутності простежуваності та прозорості в реалізації ШІ, дезінформації та аномалій у навчальних вибірках і як наслідок помилок у прийнятті рішень. Можуть виникати певні прорахунки операторів ШІ. Крім того, при зборі інформації не виключені порушення конфіденційності персональних даних. Врахування потенційних ризиків ШІ та значимість переваг над недоліками спонукають держави до розробки й впровадження інноваційних інтелектуальних технологій і зброї, доповненої ШІ, задля посилення свого військового потенціалу та забезпечення національної безпеки. Тим самим технології ШІ здатні впливати на стратегічну стабільність між державами.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Хаустова, В. Є., Решетняк, О. І., Хаустов, М. М., & Зінченко, В. А. (2022). Напрямки розвитку технологій штучного інтелекту в забезпеченні обороноздатності країни. *Бізнес Інформ, 3,* 17–26. https://doi.org/10.32983/2222-4459-2022-3-17-26
2. Гбур, З. В. (2021). Можливість адаптації Ізраїльського досвіду використання штучного інтелекту у бойових діях на Сході. *Інвестиції: практика та досвід, 12,* 54–61. 10.32702/2306-6814.2021.12.54
3. Maslii, O., Yaniuk, S., Ollo, V., Firsov, A., & Poliashov, S. (2023). Application of artificial intelligence in the field of military logistics in the context of the technical means of logistics services in the modern period. *Collection of scientific works of Odesa Military Academy, 2(20),* 131–138. https://doi.org/10.37129/2313-7509.2023.20.131-138
4. Agarwala, N. (2023). Robots and Artificial Intelligence in the Military. *Obrana a strategie, 23(2),* 83–100. https://doi.org/10.3849/1802-7199.23.2023.02.083-100
5. Nalbant, K., & Bozkurt, B. (2022). Interaction of Artificial Intelligence in the Attack and Defense Industries Using Next-Generation Military Technologies. *Journal of Electromagnetics, 5,* 1–9.
6. Bansi, K., & Shivam, P. (2023). Collision Between Military Artificial Intelligence and Civilian Artificial Intelligence. *OSR Journal of Computer Engineering (IOSR-JCE), 25(6),* 38–48. https://doi.org/10.9790/0661-2506013848
7. Скіцько, О., Складанний, П., Ширшов, Р., Гуменюк, М., & Ворохоб, М. (2023). Загрози та ризики використання штучного інтелекту. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22),* 6–18. https://doi.org/10.28925/2663-4023.2023.22.618
8. *Global AI in Military Market By Component*. (n. d.). https://market.us/report/artificial-intelligence-in-military-market/
9. *REAIM 2023 Call to Action.* (n. d.). https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/publications/2023/02/16/reaim-2023-call-to-action
10. *Science & Technology Trends 2020-2040. Exploring the S&T Edge. NATO Science & Technology Organization*. (n. d.). Office of the Chief Scientist, Brussels, Belgium. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf
11. *The Top 10 AI Applications for Military Use*. (n. d.). https://www.linkedin.com/pulse/top-10-ai-applications-military-use-markets-us-icjgf/
12. *Artificial Intelligence for Military Logistics – Current Applications*. (n. d.). https://emerj.com/ai-sector-overviews/artificial-intelligence-military-logistics/
13. *ANDURIL*. (n. d.). https://www.anduril.com/
14. *BAE Systems awarded contract to produce warfare systems for the F-15 Eagle*. (n. d.). https://www.aeroflap.com.br/en/bae-systems-recebe-contrato-para-producao-de-sistemas-de-guerra-para-o-f-15-eagle/
15. *What is Reinforcement Learning?* (n. d.). https://aws.amazon.com/what-is/reinforcement-learning/
16. Трофименко, О. Г., & Кіх, Я. Т. (2023). Застосування алгоритмів штучного інтелекту для військових задач. *Сучасні технології в енергетиці, електромеханіці, системах управління та машинобудуванні: матер. VI всеукр. наук.-практ. інтернет-конференції.*

17. Трофименко, О. Г., & Яремчук, М. В. (2023). Штучний інтелект у військовій сфері. *Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика*: *матер. міжнар. наук.-практ. конф.,* 144–148. https://doi.org/10.32837/11300.27179
18. Shopsin, J. (n. d.). *What is Artificial Intelligence in CCTV?* https://www.securitycameraking.com/securityinfo/what-is-artificial-intelligence-in-cctv/
19. Трофименко, О. Г., & Кіх, Я. Т. (2024). Використання штучного інтелекту у військовий технологіях. *Інформаційне суспільство: проблеми та перспективи : матер. IX всеукр. наук.-практ. конф.*, 76–79. https://doi.org/10.32837/11300.27842
20. *AI-Powered Cybersecurity: Top Use Cases in 2023*. (n. d.). https://hackernoon.com/ai-powered-cybersecurity-top-use-cases-in-2023
21. *SIEM / XDR / SOAR Solutions for SOC*. (n. d.). https://nxgsecure.com/siem-xdr-soar-solutions-for-soc/
22. *AI copilot enhances human precision for safer aviation*. MIT News. (n. d.). https://news.mit.edu/2023/ai-co-pilot-enhances-human-precision-safer-aviation-1003
23. *US Air Force Shows Fighter Plane Piloted by AI*. (n. d.). https://learningenglish.voanews.com/a/us-air-force-shows-fighter-plane-piloted-by-ai/7615055.html
24. *DevDROID*. (n. d.). https://devdroid.tech/catalog
25. *Як штучний інтелект допомагає Україні боротися з ворогом.* (n. d.). https://info.nic.ua/uk/blog-uk/artificial-intelligence-2/
26. *AI Rifles and Future Mass Shootings*. (n. d.). https://theincidentaleconomist.com/wordpress/ai-rifles-and-future-mass-shootings/
27. Donham, B. P. (n. d.). *Data Desert: Military Medicine's Artificial Intelligence Implementation Barriers.* https://military-medicine.com/article/4256-data-desert-military-medicine-s-artificial-intelligence-implementation-barriers.html

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023

**Olena Trofymenko**
PhD, Associate Professor, Associate Professor at the
Department of Information Technologies
National University "Odesa Law Academy", Odesa, Ukraine
ORCID ID: 0000-0001-7626-0886
*trofymenko@onua.edu.ua*

**Nataliia Loginova**
PhD, Associate Professor, Head of the Department of Information Technologies
National University "Odesa Law Academy", Odesa, Ukraine
ORCID ID: 0000-0002-9475-6188
*loginova@onua.edu.ua*

**Artem Sokolov**
Doctor of Technical Sciences, Professor at the Department of Cyber Security
National University "Odesa Law Academy", Odesa, Ukraine
ORCID ID: 0000-0003-0283-7229
*radiosquid@gmail.com*

**Pavlo Chykunov**
PhD, Associate Professor, Associate Professor at the
Department of Information Technologies
National University "Odesa Law Academy", Odesa, Ukraine
ORCID ID: 0000-0003-4959-774412:27
*pavel@onua.edu.ua*

**Hanna Akhmametieva**
PhD, Associate Professor, Associate Professor at the Department of Cyber Security
of the National University "Odesa Law Academy", Odesa, Ukraine
ORCID ID: 0000-0002-0567-902X
*anna.odessitka@gmail.com*

# ARTIFICIAL INTELLIGENCE IN THE MILITARY

**Abstract.** The article is devoted to research of the application of artificial intelligence in the military sphere. Due to the rapid development of information technologies and the growth of data volumes, the use of artificial intelligence is becoming more and more relevant for the effective application of the latest technologies for solving military tasks. The purpose of the research is to determine how the use of artificial intelligence can help improve the performance of the military. The research hypothesis is that the use of artificial intelligence in military operations can lead to improved efficiency and accuracy of decision-making. The paper discusses the main possibilities of using artificial intelligence in the military sphere and the specifics and advantages of its use. Research indicates that the implementation of artificial intelligence can help identify risks and improve the planning and forecasting of military operations, as well as enable the automation of logistics accounting and analysis. To achieve this goal, a research methodology was used, which included the analysis of literary sources and conducting research based on information about the application of artificial intelligence in the military industry. During the analysis of the specifics of the use of AI in improving the activities of the military, the areas of its successful implementation were researched: video surveillance, national security and the fight against terrorism, military logistics, autonomous and semi-autonomous vehicles, cyber security, simulators for military training, AI operations on the battlefield, medical assistance on the battlefield. It has been found that AI has great potential for effective implementation in the military sphere because the implementation of AI algorithms helps in solving military tasks potentially dangerous to human health and improves the effectiveness of weapons. The implementation of AI technologies in various components of military activity mostly shows significantly higher efficiency when compared to other technologies. In general, technological innovation in combination with AI is currently becoming a decisive factor in determining a successful outcome on the battlefield, but it requires careful preparation and consideration of risks in the process of its implementation.

**Keywords:** artificial intelligence (AI); military AI; military industry; cyber security; machine learning; AI testing; neural networks.

## REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Khoustova, V. E., Reshetnyak, O. I., Khoustov, M. M., & Zinchenko, V. A. (2022). Directions of development of artificial intelligence technologies in ensuring the country's defense capability. *Business Inform, 3*, 17-26. https://doi.org/10.32983/2222-4459-2022-3-17-26
2. Gbur, Z. V. (2021). Possibility of Adapting Israeli Experience in the Use of Artificial Intelligence in Combat in the East. *Investments: practice and experience, 12*, 54-61. 10.32702/2306-6814.2021.12.54
3. Maslii, O., Yaniuk, S., Ollo, V., Firsov, A., & Poliashov, S. (2023). Application of artificial intelligence in the field of military logistics in the context of the technical means of logistics services in the modern period. *Collection of scientific works of Odesa Military Academy, 2(20)*, 131–138. https://doi.org/10.37129/2313-7509.2023.20.131-138
4. Agarwala, N. (2023). Robots and Artificial Intelligence in the Military. *Obrana a strategie, 23(2)*, 83–100. https://doi.org/10.3849/1802-7199.23.2023.02.083-100
5. Nalbant, K., & Bozkurt, B. (2022). Interaction of Artificial Intelligence in the Attack and Defense Industries Using Next-Generation Military Technologies. *Journal of Electromagnetics, 5*, 1–9.
6. Bansi, K., & Shivam, P. (2023). Collision Between Military Artificial Intelligence and Civilian Artificial Intelligence. *OSR Journal of Computer Engineering (IOSR-JCE), 25(6)*, 38–48. https://doi.org/10.9790/0661-2506013848
7. Skitsko, O., Skladannyi, P., Shyrshov, R., Humeniuk, M., & Vorokhob, M. (2023). Threats and risks of the use of artificial intelligence. *Electronic Professional Scientific Journal «Cybersecurity: Education, Science, Technique», 2(22)*, 6–18. https://doi.org/10.28925/2663-4023.2023.22.618
8. *Global AI in Military Market By Component*. (n. d.). https://market.us/report/artificial-intelligence-in-military-market/
9. *REAIM 2023 Call to Action.* (n. d.). https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/publications/2023/02/16/reaim-2023-call-to-action
10. *Science & Technology Trends 2020-2040. Exploring the S&T Edge. NATO Science & Technology Organization*. (n. d.). Office of the Chief Scientist, Brussels, Belgium. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf
11. *The Top 10 AI Applications for Military Use*. (n. d.). https://www.linkedin.com/pulse/top-10-ai-applications-military-use-markets-us-icjgf/
12. *Artificial Intelligence for Military Logistics – Current Applications*. (n. d.). https://emerj.com/ai-sector-overviews/artificial-intelligence-military-logistics/
13. *ANDURIL*. (n. d.). https://www.anduril.com/
14. *BAE Systems awarded contract to produce warfare systems for the F-15 Eagle*. (n. d.). https://www.aeroflap.com.br/en/bae-systems-recebe-contrato-para-producao-de-sistemas-de-guerra-para-o-f-15-eagle/
15. *What is Reinforcement Learning?* (n. d.). https://aws.amazon.com/what-is/reinforcement-learning/
16. Trofymenko, O. G., & Kikh, Y. T. (2023). Application of artificial intelligence algorithms for military tasks. *6th All-Ukrainian scientific and practical Internet conference "Modern technologies in energy, electromechanics, control systems and mechanical engineering".*
17. Trofymenko, O. G., & Yaremchuk, M. V. (2023). Artificial intelligence in the military sphere. *International scientific and practical conference "Cyberspace in conditions of war and global challenges of the 21st century: theory and practice*", 144–148. https://doi.org/10.32837/11300.27179
18. Shopsin, J. (n. d.). *What is Artificial Intelligence in CCTV?* https://www.securitycameraking.com/securityinfo/what-is-artificial-intelligence-in-cctv/
19. Trofymenko, O. G., & Kikh, Y. T. (2024). Application of artificial intelligence in military technologies. *9th All-Ukrainian scientific and practical conference "Information society: problems and prospects"*, 76–79. https://doi.org/10.32837/11300.27842
20. *AI-Powered Cybersecurity: Top Use Cases in 2023*. (n. d.). https://hackernoon.com/ai-powered-cybersecurity-top-use-cases-in-2023
21. *SIEM / XDR / SOAR Solutions for SOC*. (n. d.). https://nxgsecure.com/siem-xdr-soar-solutions-for-soc/
22. *AI copilot enhances human precision for safer aviation*. MIT News. (n. d.). https://news.mit.edu/2023/ai-

co-pilot-enhances-human-precision-safer-aviation-1003
23. *US Air Force Shows Fighter Plane Piloted by AI*. (n. d.). https://learningenglish.voanews.com/a/us-air-force-shows-fighter-plane-piloted-by-ai/7615055.html
24. *DevDROID*. (n. d.). https://devdroid.tech/catalog
25. *How artificial intelligence helps Ukraine fight the enemy.* (n. d.). https://info.nic.ua/uk/blog-uk/artificial-intelligence-2/
26. *AI Rifles and Future Mass Shootings*. (n. d.). https://theincidentaleconomist.com/wordpress/ai-rifles-and-future-mass-shootings/
27. Donham, B. P. (n. d.). *Data Desert: Military Medicine's Artificial Intelligence Implementation Barriers.* https://military-medicine.com/article/4256-data-desert-military-medicine-s-artificial-intelligence-implementation-barriers.html