DOI: https://doi.org/10.26642/sas-2025-6(12)-64-76
УДК 355.45:004.8

Даник Юрій
доктор технічних наук, професор
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
https://orcid.org/0000-0001-6990-8656

Дикий Анатолій
доктор економічних наук, доцент
Державний університет Житомирська політехніка
https://orcid.org/ 0000-0002-5819-0236

Шестаков Валерій
доктор технічних наук, доцент
Національна академія Служби безпеки України
https://orcid.org/0000-0002-5918-5121

Ширшов Роман
старший викладач
Національна академія Служби безпеки України
https://orcid.org/0009-0003-3534-8736

Аналіз та обґрунтування запровадження і використання штучного інтелекту для потреб сектору безпеки та оборони України

Анотація. У статті здійснено аналіз основних напрямів запровадження та використання технологій штучного інтелекту (ШІ) з метою забезпечення національної безпеки та оборони на тлі повномасштабної збройної агресії рф проти України, ескалації інформаційних та кіберзагроз. Автори, спираючись на вітчизняний та міжнародний досвід, виокремлюють такі ключові напрями застосування ШІ для потреб сектору безпеки та оборони України, як:

- розвідка з відкритих джерел інформації (OSINT), насамперед з чисельних ресурсів мережі «Інтернет», які не вимагають аунтентифікації доступу до їх даних, за результатами якої можливо отримати чутливу для забезпечення безпеки та обороноздатності держави інформацію щодо можливих намірів дій різноманітних деструктивних акторів, а також напрямів та результатів науково-технічного розвитку, воєнно-економічного потенціалу, настроїв у суспільстві, намірів керівництва країн, які є потенційним чи реальним джерелом небезпек і загроз тощо;
- захист критичної інфраструктури, в тому числі інформаційної, за допомогою систем виявлення поведінкових аномалій, автоматичного аналізу та класифікації загроз, вибору стратегії їх стримування та нейтралізації;
- цифрова криміналістика з автоматизованим відновленням цифрових слідів та оцінкою доказів;
- виявлення й нейтралізація деструктивних кіберінформаційних дій та дезінформаційних кампаній ворога, запобігання маніпулюванню суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної або упередженої інформації;
- забезпечення проведення інформаційних, психологічних, кібероперацій завдяки швидкій генерації контекстно-чутливого мультимедіаконтенту та оперативному виявленню вразливостей у кіберінформаційній інфраструктурі об’єктів впливу;
- визначення спроможностей військових підрозділів, моделювання бойових дій та планування операцій, підтримка прийняття рішень у процесі командування та управління за рахунок обробки та аналізу великих масивів оперативних даних;
- забезпечення ефективного застосування кіберфізичних систем поля бою, насамперед ситуативних розвідувально-ударних комплексів, безпілотних (безекіпажних) повітряних, наземних, надводних, підводних комплексів та засобів.

Окреслено основні, на погляд авторів, проблемні питання щодо подальшого запровадження та масштабування ШІ-рішень, враховуючи створення:

– дієвої системи управління процесом впровадження ШІ для потреб сектору безпеки та оборони;

– ефективної системи контролю безпечності використання ШІ-систем та цільового застосування розробок ШІ, особливо в зразках та системах озброєння та військової техніки.

Для їх вирішення запропоновано комплекс із організаційних заходів (державні стандарти, сертифікація інструментів, системна підготовки кадрів, система управління ризиками) та технологічних рішень (багаторівнева верифікація даних, федеративне навчання, резервні контури управління, людино-машинні гібридні моделі, системи прогнозування та виявлення викликів, небезпек, загроз та конфліктів у системах ШІ та взаємодіючих системах).

Отримані результати формують методологічну основу для подальшого запровадження і використання ШІ для потреб сектору безпеки та оборони України.

Ключові слова: штучний інтелект; національна безпека і оборона; сектор безпеки та оборони України; кібербезпека; конфлікти ШІ; OSINT; критична інфраструктура; цифрова криміналістика; інформаційні операції; дезінформація.

Актуальність теми. Сьогодні міжнародне середовище безпеки перебуває в стані активної трансформації та адаптації до нових геополітичних викликів та умов існування держав, їх воєнно-політичних та економічних союзів у світі, що динамічно змінюється під впливом глобальних цивілізаційних трансформацій, розвитку високих технологій, зокрема ІТ та ШІ. Одним із каталізаторів цих процесів стала широкомасштабна збройна агресія рф проти України. Однією з її особливостей є активні дії в інформаційному та кіберпросторі, широкомасштабна роботизація, інтенсивне застосування космічних систем, C4ISR, ШІ, формування передумов до створення та практичного використання зброї нових поколінь (використання спрямованої енергії, електромагнітної зброї тощо).

Можна стверджувати, що, починаючи з 2014 року, Україна стала епіцентром протистояння в протиборстві між тоталітарними режимами та демократичним світом. Від початку повномасштабного вторгнення 24 лютого 2022 року і до березня 2025 року, за даними [1], зафіксовано понад 10 тис. кібератак на об’єкти критичної інформаційної інфраструктури. Більшість із них відбулася з російського сегмента «Інтернет».

Найбільш резонансними є кібератаки на: національного оператора мобільного зв’язку «Київстар» у 2023 році, що призвело до серйозних інфраструктурних проблем по всій Україні; державні реєстри України в 2024 році, що паралізувало значну частину господарської діяльності в країні; АТ «Укрзалізниця» в 2025 році, під час якої лише оперативна реакція фахівців ІТ-підрозділів безпекових структур України дала можливість досить швидко, як для масштабів кібератаки, відновити сервіси, якими користуються громадяни.

За свідченням фахівців GCHQ (Центр урядового зв’язку Великої Британії, відповідальний за ведення радіоелектронної розвідки та за забезпечення захисту інформації органів уряду й армії) [2], атаки постійно ускладнюються, а для їх організації та проведення все частіше використовується ШІ.

Крім того, Україна тривалий час протистоїть масованим деструктивним пропагандистським кампаніям, що організовуються за допомогою штучного інтелекту. Так, для прикладу, метою російської спеціальної дезінформаційної кампанії «Doppelgänger» (розпочата в 2022 році) [3] є підрив підтримки України з боку західних країн, зокрема Німеччини, Франції та США, через поширення фейкового (текстового та відео) контенту, де відомі особи поширюють проросійські наративи, закликають до зняття санкцій з рф, зображають українських біженців у негативному світлі тощо.

Водночас досвід Сил безпеки та оборони України у відбитті агресії рф доводить, що отримати перевагу у протиборстві в інформаційній сфері, кібердомені та на полі бою можливо за рахунок комплексного та раціонального використання високих технологій, зокрема штучного інтелекту (далі – ШІ).

Відповідно до [4] ШІ визначається як організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень та алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань.

За словами радника Президента України зі стратегічних питань, обмеженість у живій силі змушує Україну шукати рішення з впровадженням технологій штучного інтелекту [5].

Аналіз останніх досліджень та публікацій. Нормативною основою використання ШІ в інтересах забезпечення національної безпеки до останнього часу була Стратегія кібербезпеки України від 2021 [6]. Наразі в Україні прийнято низку нових нормативно-правових, підзаконних та інших актів і керівних

документів, що регламентують впровадження та використання ШІ, зокрема в сфері оборони, затверджено План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025–2026 роки [7].

У наших Європейських партнерів такою основою є Регламент ЄС про ШІ (EU AI Act) [8].

Федеральним урядом США як стратегічний пріоритет визначено впровадження ШІ в сфері оборони [9].

Кодекс НАТО щодо військового застосування ШІ – NATO AI Strategy, прийнятий у 2021 році, передбачає етичні принципи використання ШІ у військовій сфері, враховуючи прозорість, підзвітність та необхідність людського контролю над критичними рішеннями [10]. Відповідно до цього кодексу Країни НАТО можуть розробляти LAWS, забезпечуючи належний контроль за їхнім використанням.

У 2018 році Європарламент прийняв резолюцію щодо заборони в ЄС розробки та використання автономних бойових систем, що можуть приймати рішення про застосування смертоносної сили без людського контролю. Прийнятий у 2023 році в ЄС AI Act визначає, що автономні бойові системи можуть потрапити під категорію «високого ризику», що вимагатиме суворих тестувань та сертифікації [8]. EU AI Act і нормативи GDPR задають жорсткі вимоги щодо класифікації ризиків, прозорості алгоритмів та етичного застосування високоризикових систем, враховуючи автономні бойові засоби.

Починаючи з 2021 року, світова та українська наукова спільнота демонструє помітний зсув від описових оглядів можливостей ШІ до практико орієнтованих досліджень щодо використання конкретних моделей для потреб безпеки та оборони. Зазначене можна ілюструвати динамікою англомовних публікацій (рис. 1) в яких пов’язані поняття «National Security»+«Artificial Intelligence». На гістограмі наведено фактичні дані за період з січня 2021 року до жовтня 2025 року.

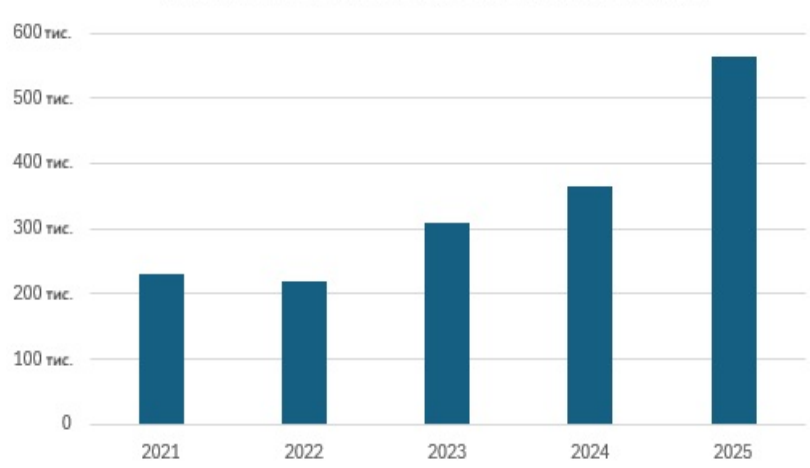

Рис. 1. Кількість публікацій з ключовими словами «National Security»+«Artificial Intelligence»

Проблематику застосування ШІ в галузі кібербезпеки, захисту критичної інфраструктури та протидії інформаційно-психологічним операціям активно досліджують українські дослідники: О.Потій [11], М.Кузьо [12], А.Петренко [13], Л.Шульга [14], І.Костюк [15], О.Поляков [16], С.Гончар [17], А.Шевченко [18] та ін. Серед іноземних науковців та експертів у сфері застосування ШІ в інтересах кібербезпеки найбільш цитовані: J.Lewis [19], M.Brundage [20], S.Avin [21], J.Clark [22].

Інтегрально питання запровадження систем та засобів з ШІ для потреб безпеки та оборони досліджується в кіберцентрах та наукових установах країн-партнерів України. У звітах NATO CCDCOE (2023) [23], NSCAI (2021) [24], а також DFRLab щодо deepfake-кампаній [25] подано аналіз використання ШІ в різних сферах забезпечення національної безпеки і окреслено: нестачу відкритих навчальних вибірок, відсутність уніфікованих метрик оцінювання та потребу в участі людини для оцінки проміжних результатів роботи ШІ-систем та корегуванні нових завдань на базі цих результатів для мінімізації ризиків автоматизації, що може бути визначено як проблемні питання використання ШІ для забезпечення національної безпеки.

Мета статті – на основі авторської методики провести аналіз сучасного стану запровадження та використання штучного інтелекту, виокремити та обґрунтувати напрями застосування штучного інтелекту в інтересах забезпечення національної безпеки і оборони, визначити основні проблемні питання подальшого запровадження систем та засобів з ШІ для потреб Сил безпеки та оборони України, запропонувати шляхи їх вирішення.

Викладення основного матеріалу. За результатами аналізу багаторічних досліджень авторів у галузі інформаційних технологій [1–25] запропоновано акцентувати увагу на вказаних далі напрямах використання ШІ для потреб Сил безпеки та оборони України.

1. Розвідка, у тому числі з відкритих джерел інформації (OSINT)

Найбільш поширене використання ШІ спостерігається для аналізу розвідувальних даних, де ШІ-системи та засоби дозволяють автоматизувати: перегляд значного обсягу цифрових ресурсів; збір та цілеспрямовану обробку великого масиву даних; аналіз складних інформаційних структур; відсіювання інформаційного шуму.

Для збирання з різних джерел, аналізу, візуалізації та інтеграції великих масивів даних (Big Data), насамперед у безпековій та оборонній сферах, використовується ШІ-система Palantir від Palantir Technologies (США). Серед ключових замовників цієї компанії – ЦРУ, ФБР, Пентагон. У 2023–2024 роках Palantir підписала меморандуми про співпрацю з Мінцифрою, МОН та Мінекономіки України. За даними [26], на базі спроможностей Palantir українські ІТ-фахівці побудували низку інструментів, які зараз активно використовують розвідувальні та аналітичні структури Сил безпеки та оборони України.

Вже сьогодні під час виконання завдань із розвідки з відкритих джерел інформації (OSINT) OSINT-дослідники за допомогою ШІ-систем отримують з великим ступенем достовірності інформацію щодо:

– намірів керівництва країн, які є потенційним чи реальним джерелом небезпек і загроз, для своєчасного попередження виникнення та/або реагування на кризову ситуацію;

– воєнно-економічного потенціалу, напрямів та результатів науково-технічного розвитку агресора та недружніх країн;

– місць тимчасової дислокації, переміщення та районів зосередження військ противника, що дозволяє своєчасно та результативно здійснювати їх вогневе ураження;

– стану інженерних загороджень противника (за результатами аналізу знімків супутникових систем дистанційного зондування Землі та інформації від різнотипних сенсорів, зокрема роботизованих засобів) для оцінювання обстановки, вироблення замислу бойових дій;

– деструктивних акторів, таких як диверсанти, колаборанти, а також можливих намірів їх дій, що дозволяє запобігти диверсіям, витоку чутливої для обороноздатності держави інформації тощо;

– настроїв у суспільстві країни-агресора, проблемних питань у різних сферах його життєдіяльності для планування та ефективної реалізації заходів контрпропаганди, доведення до її населення позиції України щодо припинення повномасштабної агресії з боку рф.

Як показано в [27], для оцінювання намірів можна використовувати баєсівську регресійну модель:

$$\text{"Оцінка"} \sim N(\mu, \sigma),\ \mu = \alpha + \beta t, \qquad (1)$$

де α – початкова оцінка, β – нахил тренду.

Для розв’язання баєсівських моделей використовуються числові методи Монте-Карло.

Крім того, результати OSINT з використанням технологій ШІ використовуються для:

– виявлення прихованих закономірностей та зв’язків фінансових транзакцій, пов’язаних із тероризмом;

– розслідування воєнних злочинів (зокрема технології розпізнавання облич, створені на основі штучного інтелекту, допомогли встановити особи окупантів, причетних до звірств у Бучі);

– прогнозування подій, що можуть становити загрозу національній безпеці.

Прикладом ШІ-системи, що використовується в OSINT Силами безпеки та оборони, є система розпізнавання облич від американської компанії «ClearView AI». ШІ має доступ до 10 мільярдів фотографій, розміщених у соціальних мережах [28]. З березня 2022 року ClearView надає технологічну підтримку Державній прикордонній службі України; Силами безпеки використовується на блокпостах для виявлення диверсантів та колаборантів; Силами оборони для ідентифікації російських військових, які беруть участь у вторгненні в Україну [29].

Як проблемне питання застосування в Україні ClearView AI слід зазначити, що в державі немає чітко унормованого законодавства стосовно застосування технологій розпізнавання облич та обробки біометричних даних у воєнний час. Як зазначається в [30], це породжує ризики для прав людини, особливо після завершення воєнного стану. Так у випадку пошкоджених або зіпсованих зображень технологія може давати хибні збіги. Використання таких результатів без перевірки може призвести до серйозних помилок та неправомірних наслідків.

За результатами проведеного аналізу, можна стверджувати, що застосування ШІ у OSINT стикається з критичними викликами інформаційного перевантаження та верифікації достовірності даних. Проблемними питаннями подальшого запровадження є: відсутність ефективних алгоритмів фільтрування релевантної інформації серед величезних масивів загальнодоступних даних, що обумовлені зростанням кількості фейкових акаунтів та ботів, через які поширюється дезінформація; складність розпізнавання контекстуальних нюансів при автоматичному аналізі текстів.

Вирішення зазначених питань можливе за рахунок поєднання організаційних заходів, таких як, визначення чітких протоколів етичного використання OSINT, навчання аналітиків принципам критичного мислення під час роботи з ШІ-інструментами, регулярне оновлення алгоритмів виявлення дезінформації та технологічних рішень: впровадження багатошарових систем верифікації інформації, які мають поєднати машинне навчання з експертною оцінкою людини; розроблення алгоритмів виявлення синтетичного контенту та deepfake-матеріалів; створення баз даних перевірених джерел.

2. Захист критичної інфраструктури, зокрема інформаційної

Найбільш динамічно ШІ запроваджуються в критичній інформаційній інфраструктурі в енергетиці, на транспорті, в системах зв'язку. ШІ-системи цілодобово стежать за станом інформаційних систем, виявляючи відхилення від норми та поведінкові аномалії, що вказують на технічний збій чи кібератаку.

У разі використання системою виявлення вторгнень (IDS) з ШІ-даних з датчиків *x*, математично ймовірність ризику p кібератаки на об'єкт критичної інфраструктури можна представити у вигляді логістичної регресії [31]:

$$p = 1/1 + e^{-(\beta_0 + \sum_{i=1}^{n} \beta_i x_i)}, \quad (2)$$

де $\beta 0,\ \beta 1,\ \ldots,\ \beta n$ – параметри моделі; $x1, x2, \ldots\ xn$ незалежні змінні.

Людина-оператор системи кіберзахисту (фахівець з кібербезпеки) додає свою оцінку h. Разом вони формують фінальну оцінку ризику *R*:

$$R = w_1 p + w_2 h\,, \quad (3)$$

при цьому $w_1 + w_2 = 1$.

Якщо R перевищує порогове значення, то система захисту критичної інфраструктури генерує сповіщення.

ШІ-агенти систем виявлення вторгнень (IDS) шляхом аналізу поведінкових моделей виявляють нові, раніше невідомі методи атак, вчаться та адаптуються до нових тактик кібератак.

Для підвищення рівня захисту критичної інфраструктури постійно здійснюється удосконалення алгоритмів швидкого виявлення багатовекторних кібератак та інтеграція багатомодальних OSINT-платформ, що поєднують мережеві трафіки й соціальні медіа [26–28].

За [29] програмно-апаратний комплекс Zvook використовує технології машинного навчання, яка дозволяє розпізнавати звуки двигунів повітряних цілей, в тому числі крилатих ракет, БПЛА, гелікоптерів та винищувачів противника. Zvook використовувався на початку повномасштабного вторгнення військ рф в Україну у взаємодії з системами протиповітряної оборони.

В цілому впровадження ШІ на об'єктах критичної інфраструктури призводить до підвищення рівня їх безпеки.

Однак цей процес стикається з проблемами надмірної залежності від автоматизованих систем, що створює ризики катастрофічних збоїв при відмові алгоритмів. Основними викликами є: складність забезпечення прозорості та підзвітності ШІ-рішень у критично важливих системах, потенційна вразливість до адверсаріальних атак, що можуть «обдурити» алгоритми машинного навчання, «отруйна дистиляція» та проблема хибних спрацювань, які можуть призвести до непотрібного вимкнення важливих систем. Додатково виникають складнощі інтеграції ШІ з системами промислової автоматизації попередніх поколінь та забезпечення кваліфікованого персоналу для обслуговування складних ШІ-систем.

Доцільно провести такі організаційні заходи: розробити національні стандарти безпеки ШІ, створити лабораторії та центри застосування та безпеки штучного інтелекту на базі закладів вищої освіти та наукових установ, створити центри кіберзахисту з функцією експертизи у сфері ШІ, та Об'єднаний центр впровадження ШІ в сфері національної безпеки і оборони, запровадити на постійній основі проведення кібернавчань з елементами використання ШІ.

До технологічних рішень пропонується зарахувати такі:

– контроль людини за прийняттям рішення ШІ-системою;

– впровадження на об'єктах критичної інформаційної системи виявлення аномалій, наприклад, на основі алгоритмів ансамблевого навчання;

– створення резервних механізмів керування ШІ-систем;

– реалізація федеративного навчання моделей ШІ, яке можна представити такою функцією [32]:

$$f(\boldsymbol{x_1}, \ldots, \boldsymbol{x_K}) = \frac{1}{K} \sum_{i=1}^{K} f_i(\boldsymbol{x_i}), \quad (4)$$

де K – кількість вузлів, x_i – вага моделі з точки зору вузла i, і f_i – локальна цільова функція вузла i, яка описує, як вага моделі x_i відповідає локальному набору даних вузла i.

Метою федеративного навчання є розв'язання оптимізаційних задач без обміну даними між агентами, а саме [32]:

$$\min_x \sum_{k=1}^{K} \frac{n_k}{n} f_k(x), \quad (5)$$

де $f_k(x)$ – середній збиток кожного клієнта k, а n_k – кількість точок даних, що належать клієнту k.

Зазвичай це досягається за допомогою ітеративних процесів, що включають клієнт-серверну взаємодію, де локальні моделі тренуються на кожному вузлі, а потім агрегуються для формування глобальної моделі.

Взаємодія відпрацьовується у ході навчань на кшталт «Locked Shields», які організовуються Об'єднаним центром передового досвіду з кібероборони НАТО [33]. Таким чином, сприяючи обміну інформацією та передовим досвідом, НАТО допомагає членам Альянсу зміцнювати захист їх національної критичної інфраструктури, зокрема інформаційної [34].

3. Цифрова криміналістика

Як зазначалось вище, за допомогою ШІ-систем експерти можуть ідентифікувати джерела атак, відновлювати хронологію подій, отримати дані, які використовуються для встановлення фактів та обставин, що мають значення для кримінального провадження.

Сучасні методи цифрової криміналістики дозволяють працювати з даними, навіть після спроби їх видалення або шифрування, що є вирішальним фактором у реагуванні на складні інциденти.

Використання ШІ у цифровій криміналістиці створює низку проблем, пов'язаних з достовірністю та правовою прийнятністю доказів, отриманих за допомогою алгоритмів машинного навчання.

Ключовими проблемами є складність пояснення логіки ШІ-систем у суді, потенційна упередженість алгоритмів, що може призвести до хибних висновків та швидка еволюція методів приховування цифрових слідів злочинцями. Додатково виникає проблема обробки великих обсягів даних у визначені терміни, що ускладнюється необхідністю дотримання процедурних норм збору доказів, а також зростаючою складністю deepfake-технологій, що можуть компроментувати достовірність цифрових доказів.

Вирішення цих питань потребує таких організаційних заходів:

– оновлення процесуального законодавства щодо врегулювання використання доказів, отриманих за допомоги ШІ-систем;

– створення програм сертифікації ШІ-інструментів криміналістики;

– імплементація міжнародних стандартів цифрової криміналістики;

– підготовка спеціалістів з використання ШІ-технологій у правоохоронній сфері;

– технологічних рішень:

– створення ШІ-систем документування, які можуть бути використані в судах, також блокчейн-систем для забезпечення цілісності цифрових доказів;

– розробка спеціалізованих алгоритмів виявлення синтетичних медіа та впровадження автоматизованих систем форензік-аналізу.

4. Виявлення деструктивних кіберінформаційних дій та дезінформаційних кампаній противника, зокрема поширення недостовірної, неповної або упередженої інформації, можливо за рахунок використання ШІ-систем моніторингу інформаційних потоків шляхом виявлення в них аномалій, наприклад, бот-активності, неприродньо-синхронізованих дій.

Алгоритми ШІ-систем аналізують зміст контенту інформаційних потоків, розпізнають текст і зображення, характерні мовні звороти пропаганди, повторюваних шаблонів, перевіряють контент на достовірність інформації, виявляють фейкові акаунти.

Так для аналізу, класифікації тексту та генерації людської мови в ШІ-системах активно використовується Python-бібліотека Natural Language Toolkit (NLTK). Інтеграція NLTK до ШІ-систем дозволяє: аналізувати лінгвістичну структуру, виявляти зміст та емоційне забарвлення тексту; будувати семантичні моделі для діалогових агентів (чат-ботів, голосових асистентів) [35]. Подібно до NLTK для аналітики соцмереж використовується Python-бібліотека SpaCy. ШІ-системи з SpaCy дозволяють виявляти іменовані сутності: людей, організацій, локацій, дат тощо.

Для оцінювання якості класифікатора тесту використовується метрика: precision (точність) – частка результатів, знайдених у вибірці, які справді належать до шуканого класу, recall (повнота) – показує частку релевантних документів, які вдалося знайти; F1 – норма [36]:

$$precision = \frac{relevant\ document \cap retrieved\ document}{retrieved\ document}. \quad (6)$$

Найкращий результат для задач класифікації дорівнює 1, що означає, що всі відібрані зразки належать до свого класу. Такі документи вважаються правильно класифікованими:

$$recall = \frac{relevant\ document \cap retrieved\ document}{relevant\ document}. \quad (7)$$

Значення F1 обчислюється через показники precision та recall. Зазвичай використовують F_1, тобто зважене гармонійне середнє між ними:

$$\mathrm{F1} = 2 \times \frac{recall \times precision}{recall + precision}. \quad (8)$$

Найкраще значення F1 = 1,0, що відповідає ідеальній точності та повноті. Найгірше – 0, якщо хоча б один показник дорівнює нулю.

Впровадження ШІ-систем дозволяє підвищити оперативність виявлення факту деструктивних кіберінформаційних дій та дезінформаційних кампаній, визначити їх джерела, канали та виконавців,

аутентифікувати замовників. Зазначене надає змогу спланувати та вжити необхідні заходи запобігання маніпулюванню суспільною свідомістю, підвищити результативність заходів контрпропаганди.

Виявлення дезінформації за допомогою ШІ стикається з проблемою нестабільності критеріїв істинності та контекстуальної залежності інформаційних суджень. Основними проблемами є неможливість алгоритмів адекватно оцінювати нюанси політичного та культурного контексту, схильність до помилкових спрацювань при ідентифікації легітимного контенту як дезінформації та швидка адаптація пропагандистських методів до існуючих систем виявлення. Додатково виникають ризики цензурування через надмірне покладання на автоматизовані системи модерації, «отруєння» даних навчання ШІ-моделей спеціально підготовленою дезінформацією та складність розрізнення між різними типами неточної інформації – від ненавмисних помилок до злочинної пропаганди.

Вирішення цих проблем потребує впровадження гібридних систем, які поєднують автоматизоване виявлення підозрілого контенту з обов'язковою експертною перевіркою людьми.

Технологічні рішення містять розробку моделей для підвищення точності виявлення, створення систем перехресної перевірки фактів через множинні джерела для верифікації автентичності контенту.

Організаційні механізми передбачають:

– створення незалежних фактчекінгових центрів з використанням ШІ-інструментів;

– розробку стандартів та навчальних програм медіаграмотності для населення;

– впровадження систем громадського модерування та забезпечення прозорості алгоритмів виявлення дезінформації для запобігання зловживанням.

5. Забезпечення проведення інформаційних, психологічних, кібероперацій

За допомогою технологій ШІ можна швидко створювати контент для різних аудиторій: тексти, зображення, аудіо, відео. ШІ-системи здатні моделювати психологічні портрети особистостей та аудиторій. Інструменти ШІ за лічені хвилини здатні генерувати переконливе повідомлення потрібною мовою, враховуючи культурні особливості цільової групи. Крім того, ШІ дозволяє прогнозувати, як певні повідомлення сприйматимуться, і підбирати оптимальний стиль комунікації.

Так оцінювання ефективності інформаційної операції можливе за допомогою моделі Neural ODE (Neural Ordinary Differential Equations – Нейронні Звичайні Диференціальні Рівняння), що оперує двома стійкими станами – позитивною та негативною думкою та враховує внутрішній зворотний зв'язок $ax(1 - x^2)$, згасання $(-bx)$, дію зовнішніх імпульсів cE [27]:

$$\frac{dx}{dt} = ax(1 - x^2) - bx + cE, \quad \frac{dE}{dt} = -dE + I(t), \tag{9}$$

де x – стан думки, E – зовнішній вплив (медіа акції, події), $I(t)$ – імпульс (заяви лідерів, новини).

Модель демонструє, що думка може різко змінювати знак під впливом серії подій або одного сильного імпульсу (кризи, заяви лідерів). Вона може бути навчена обернено (inverse problem) для оцінки параметрів за наявними часовими рядами даних.

Все це дозволяє фахівцям з інформаційних, кібер-, психологічних операцій робити відповідні впливи точковими, адресними та масштабованими.

Основним проблемним питанням використання ШІ під час проведення інформаційних та психологічних операцій є складність розрізнення легітимних, санкціонованих дій від пропаганди протидіючої сторони, спеціального (цільового) контенту від дезінформації.

6. Підтримка прийняття рішень у процесі командування та управління

Можливість командирам спрямовувати та координувати діяльність підпорядкованих військ (сил) у ході виконання бойових завдань визначена концепцією командування і управління (Command and Control (C2)) [37]. В арміях країн НАТО, як і в Збройних силах України, [38] зазначена концепція еволюціонує до Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance (C4ISR). Вона поєднує принципи, технології та організаційні рішення командування, управління, зв'язку, комп'ютерних систем, розвідки, спостереження та розвідки цілей у єдиному кіберінформаційному просторі та дозволяє інтегрувати інформаційні потоки з різнотипних джерел інформації (безпілотників, супутників, радіолокаційних засобів, кіберрозвідки тощо) створює основу для інтелектуальних бойових (кіберфізичних) систем.

Зазначені концепції передбачають, що в умовах кризової ситуації в протиборстві сторін А та В $KS_{A,B}$ перевагу $P_{A,B}$ отримує та сторона, управлінський цикл Tl якої буде коротшим за протидіючу:

$$\forall KS_{A,B}\ \exists P_{A,B} \Leftrightarrow\ (Tl_A < Tl_B\ ), \tag{10}$$

де Tl_A, Tl_B – час виконання управлінського циклу відповідно стороною А, В.

За [39] у разі впровадження ШІ-систем для обробки та аналізу даних з різнотипних (різновидових) джерел інформації в процесі командування та управління забезпечується:

– створення загальної картини бойових дій майже в реальному часі (оперативної обстановки);

– визначення спроможностей військових підрозділів (сил) щодо виконання бойових завдань;

– моделювання бойових дій;

– вироблення замислу та планування операцій тощо.

Так для визначення спроможності виконання військовим підрозділом бойового завдання на поточний момент часу t, ШІ-система має проаналізувати чисельні та якісні показники щодо стану: наявного особового складу (персоналу) з відповідним рівнем підготовки; озброєння та військової техніки; забезпеченості придатними до застосування матеріально-технічними засобами. У [40] рівень спроможності запропоновано визначати індексом G_F:

$$G_F(t) = \omega(t)G_H(t)G_T(t)G_S(t)G_P(t)\,,\ 0 \le G \le 1, \tag{11}$$

де $\omega(t)$ характеризує наявність зв'язку з пунктом управління військового підрозділу, $\omega(t) = \{0,1\}$; $G_H(t)$, $G_T(t)$, $G_S(t)$, $G_P(t)$ – індекси, що чисельно характеризують відповідно спроможність персоналу, озброєння, за рівнем запасів та підготовленістю персоналу.

Першим масштабним військовим проєктом США з впровадження ШІ для автоматизації обробки величезних обсягів різнотипних розвідувальних даних став Algorithmic Warfare Cross-Functional Team (AWCFT). Його реалізація Project Maven застосовує алгоритми комп'ютерного зору для:

– розпізнавання, класифікації та відстеження об'єктів на відео (наприклад, транспортних засобів, людей, техніки);

– автоматичного виявлення цілей.

Використання Project Maven прискорює цикл «спостереження – орієнтація – рішення – дія» (OODA loop) та дозволяє утворювати цифрове поле бою (Digital Battlefield), що відповідає сучасній бойовій концепції Joint All-Domain Command and Control (JADC2).

Таким чином, швидкість та точність аналізу ШІ-системами великих масивів даних з різнотипних (різновидових) джерел інформації може забезпечити скорочення часу ухвалення рішень і, як наслідок, оперативну перевагу над противником, який не має подібних можливостей.

Однак досі не мають якісних рішень проблеми оперативної аналітичної обробки великих масивів даних. Проблеми розмірності даних і динаміки інформаційних потоків в єдиному кіберінформаційному просторі вимагають проведення фундаментальних досліджень у сфері математики (теорії графів, мереж), розпізнавання образів (класифікація, кластерний аналіз, нейронні мережі), лінгвістики, цифрової обробки сигналів, нелінійного аналізу тощо.

7. Забезпечення ефективного застосування кіберфізичних систем (КФС) поля бою, насамперед ситуативних розвідувально-ударних контурів (комплексів) (РУК), безпілотних літальних апаратів, роботизованих наземних, морських, повітряних і космічних комплексів тощо

Досвід відбиття повномасштабної агресії рф проти України доводить, що сучасне протиборство є асиметричним, характеризується відсутністю чіткої лінії фронту, набуває багаторівневого та об'ємного характеру, здійснюється професійними малочисельними штурмовими та іншими групами з комплексним застосуванням безпілотних (роботизованих) апаратів та комплексів, засобів та систем розвідки, кінетичного та/або некінетичного ураження, логістичного забезпечення тощо.

Просторово-рознесені, різнорідні, різновидові сили та засоби в районі бойових дій за допомогою систем зв'язку автоматизованими інформаційно-управляючими системами S_{CC} (ІУС) інтегруються на час T виконання завдання (ведення дій) в ситуативні РУК S, кортеж якого можливо представити так [40]:

$$S(T): \left\{ \bigcup_{r}^{R} \{S_r(t)\}, \bigcup_{n=1}^{N} |M_n(t)|, FS(T) \right\}, \tag{12}$$

де

$\bigcup_{r}^{R} \{S_r\} = \{S_{Ex}, S_{Dc}, S_{Ac}, S_{CC}\}$ – сукупність різнорідних елементів розвідки $S_{Ex} = \bigcup_{j} UEx_j$,

автоматизації управління $S_{Dc} = \bigcup_{n} UDc_n$, ураження $S_{Ac} = \bigcup_{m} UAc_m$;

$\bigcup_{n=1}^{N} |M_n(t)|, \quad t \le T$ – сукупність планів (сценаріїв) застосування елементів (різнорідних зв'язків);

$FS(T)$ – цільова функція (призначення).

ІУС забезпечує орган управління необхідною оперативною інформацією: вирішення завдання щодо формування та корегування відповідно до обстановки, що склалася, конфігурації РУК, раціонального розподілу завдань за спроможностями наявних сил і засобів; командування та управління застосуванням складових елементів контуру відповідно до затвердженого замислу дій в єдиному управлінському циклі «виявлення – рішення – удар».

За своєю природою, відповідно до NIST, IEC, ISO та ДСТУ ISO/IEC 30182:2019, такий комплекс являє собою кіберфізичну систему.

Кількість можливих варіантів N_S конфігурацій такої кіберфізичної системи становить:

$$N_S = \prod_{i=1}^{I} N_{S_i} = \prod_{i=1}^{I} \prod_{j=1}^{J_i} Un_{ij}, \quad (13)$$

де I – кількість функціональних підсистем, $I = 3$; Ji – кількість елементів i-ї підсистеми.

Задача вибору раціонального варіанта КФС є багатокритеріальною, рішення якої потребує аналізу великої кількості показників сил і характеристик засобів протиборства, їх стан на поточний час, оперативної обстановки та умов протиборства в районі бойових дій.

Потенціал застосування ШІ щодо інтелектуалізації завдань раціонального розподілу наявних різнорідних та різновидових сил і засобів, формування конфігурації динамічної кіберфізичної системи та її корегування відповідно до обстановки, що склалася, командування та управління застосуванням складових елементів системи відповідно до затвердженого замислу дій демонструють програми DARPA Mosaic Warfare і Air Force Multi-Domain Command and Control.

За свідченням [41], інтеграцію ШІ в бойові безпілотники визнано однією з цілей у розвитку бойових платформ, насамперед морських.

Штучний інтелект та суміжні технології (комп'ютерне бачення, автономне управління, алгоритми планування маршруту, адаптивна навігація) додають роботизованим наземним, морським, повітряним комплексам можливості щодо:

– автономної навігації. ШІ-системи дозволяють: прокладати маршрут руху, уникаючи фізичних перешкод (наземні, повітряні, надводні об'єкти, хвилі) дію засобів радіоелектронної боротьби (глушіння GPS, радіоперешкоди) противника; реагувати на зміни погодних умов; утримувати позицію або маршрут, використовуючи інші дані (інерційні системи, візуальні орієнтири, локальні сенсори);

– розпізнавання об'єктів. За допомогою камер, тепловізорів і алгоритмів комп'ютерного бачення КФС спроможна здійснювати розвідку, розпізнавати необхідні об'єкти протидіючої сторони. У подальшому виділяти з об'єктів цілі для ураження чи коригування вогню;

– адаптивне управління й ухиляння від загроз. У разі виявлення динамічного об'єкта та ідентифікації його як загрози (наприклад, ракета або дрон), ШІ забезпечує маневрування, зміну траєкторії руху або активацію засобів захисту.

За свідченням [42], на основі комп'ютерного зору здійснюється пошук рішення створення БпЛА-перехоплювача для знищення ворожих БпЛА-розвідників, що дозволить заощадити ресурси ППО.

В цілому можна стверджувати, що впровадження ШІ в кіберфізичні системи дозволить:

– зменшити трафік між елементами кіберфізичної системи за рахунок обробки, фільтрування, виділення важливих даних на борту роботизованого засобу;

– збільшити час функціонування за рахунок управління енергетичною підсистемою (коли перейти в режим енергозбереження, коли активувати двигуни, як оптимізувати стан акумуляторів тощо);

– отримати синергію від застосування різнотипних дронів, коли дрони працюють у «рої» або групі з різними завданнями [43].

У ході аналізу виявлено, що перед автономністю на основі ШІ стоять два основні виклики:

– середовища (повітряне, морське, наземне) вимагають різних технічних рішень щодо управління, забезпечення роїння;

– складна координація дронів у «рої», де дрони спілкуються, приймають рішення та спільно адаптуються. Це вимагатиме значного прогресу в сенсорах, алгоритмах штучного інтелекту, протоколах зв'язку та можливостях прийняття рішень у режимі реального часу.

При цьому такі системи вже слабо контролюються людиною. В результаті, як зазначено в [44], відбувається формування та розвиток багатоаспектної та багаторівневої системи конфліктів ШІ різної природи та їх причинно-наслідкового розвитку: між ШІ-системами, керованими людиною, згідно з її волею та під її управлінням; між ШІ поза системою «людина – ШІ».

Попри зазначене, КФС знаходять все більшого застосування в протиборстві конфліктуючих сторін, як на рівні держав, так і недержавних структур, терористичних організацій тощо.

Висновки. Основними напрямами запровадження та використання ШІ для потреб сектору безпеки та оборони є: розвідка з відкритих джерел інформації, підвищення рівня безпеки об'єктів критичної інформаційної інфраструктури, цифрова криміналістика, забезпечення організації та ведення інформаційних та психологічних операцій, виявлення і нейтралізація ворожого інформаційного впливу та дезінформаційних кампаній. ШІ є частиною роботизованих систем, які використовуються на передовій, мізками кіберфізичних систем.

Однак, попри зусилля держави в галузі ШІ, на наш погляд, основними проблемними питання щодо подальшого запровадження та масштабування ШІ-рішень для потреб сектору безпеки та оборони України залишаються:

– недосконаліть правового регулювання штучного інтелекту (в тому числі у сферах безпеки (кібербезпеки), оборони);

– недосконаліть механізмів прийняття управлінських рішень у сфері запровадження і використання ШІ для потреб сектору безпеки та оборони України;

– низький рівень фінансування наукової діяльності у сфері ШІ;

– повільне впровадження технологій штучного інтелекту в кіберфізичні системи порівняно із провідними країнами світу, країною агресором, що призводить до збільшення всіх видів ресурсів для отримання переваги над противником;

– недостатня кількість фахівців, насамперед випускників вищих військових навчальних закладів, необхідна для: організації бойового застосування кіберфізичних систем; здійснення командування та управління з використанням можливостей ШІ-систем;

– невизначеність участі людини в циклі верифікації прийнятого ШІ-системами рішення та легітимізації результатів їх роботи.

Для їх вирішення запропоновано комплекс із організаційних заходів:

– створення дієвої системи управління процесом впровадження ШІ для потреб сектору безпеки та оборони. Для цього профільним науковим установам необхідно замовити: розроблення вимог до такої системи; прогнозування та визначення механізмів впровадження та подальшого використання технологій ШІ для потреб сектору безпеки та оборони України;

– створення ефективної системи контролю безпечності використання ШІ-систем та цільового застосування розробок ШІ, особливо в зразках і системах озброєння та військової техніки. Для цього потрібно розробити національні стандарти та/або імплементувати стандарти стратегічних партнерів у сфері ШІ до українських реалій, запровадити систему сертифікації ШІ-систем та технологій машинного навчання;

– розробити візію та розгорнути систему підготовки кадрів із розроблення, впровадження та застосування ШІ-систем;

– подальше налагодження співпраці з відповідними структурами країн-партнерів, міжнародними організаціями щодо визначення «правила гри» для ШІ, недопущення неконтрольованого розповсюдження та використання технологій ШІ у злочинних цілях;

– запровадження економічних стимулів для наукових установ і закладів вищої освіти, що проводять дослідження у сфері ШІ; пільгових умов приватному сектору, що бере участь у впровадженні технологій ШІ в пріоритетних для забезпечення обороноздатності держави галузях економіки.

Серед технологічних рішень пропонується:

– впровадження багаторівневої верифікації даних, людино-машинних гібридних моделей;

– федеративне навчання;

– резервування контурів управління;

– розроблення та впровадження системи прогнозування та своєчасного виявлення викликів, небезпек, загроз та конфліктів, у системах ШІ і взаємодіючих системах, створення дієвої системи управління ризиками при роботі з ШІ.

Проведені моделювання, аналіз та оцінювання показали, що подальше впровадження ШІ для потреб сектору безпеки та оборони України сприятиме зменшенню обсягу витрат, підвищенню ефективності виконання завдань із забезпечення безпеки та оборони держави.

Список використаної літератури:

1. Система виявлення вразливостей і реагування на кіберінциденти та кібератаки / Державна служба спеціального зв'язку та захисту інформації України [Електронний ресурс]. – Режим доступу : https://scpc.gov.ua/uk.
2. Attacks will get through': head of GCHQ urges companies to do more to fight cybercrime / The Guardian [Electronic resource]. – Access mode : https://www.theguardian.com/technology/2025/oct/23/gchq-companies-cyber-crime-threat.
3. Doppelgänger Operation / EU DisinfoLab [Electronic resource]. – Access mode : https://www.disinfo.eu/doppelganger-operation/.
4. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text.
5. Україна використовує штучний інтелект у безпілотних системах на передовій – Камишін / Укрінформ [Електронний ресурс]. – Режим доступу : https://www.ukrinform.ua/rubric-ato/4003602-ukraina-vikoristovue-stucnij-intelekt-u-bezpilotnih-sistemah-na-peredovij-kamisin.html.
6. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021 [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/go/447/2021.
7. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025-2026 роки : Розпорядження Кабінету Міністрів України від від 09.05.2025 № 457-р. [Електронний ресурс]. – Режим доступу : https://zakon.rada.gov.ua/laws/show/457-2025-p#Text.
8. Regulation (EU) 2024/1689 (EU AI Act) / EUR-Lex [Electronic resource]. – Access mode : https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

9. Artificial Intelligence for National Security: The Predictability Problem / M.Taddeo, M.Ziosi, A.Tsamados and other. –2022 [Electronic resource]. – Access mode : https://cetas.turing.ac.uk/sites/default/files/2022-09/research_report_ai_predictability_problem_vfinal_3.pdf.
10. AI Strategy (2021) / NATO [Electronic resource]. – Access mode : https://www.nato.int/cps/en/natohq/official_texts_227237.htm.
11. Олександр Потій: кібербезпека залишається такою самою ареною бойових дій, як і інші домени / Державна служба спеціального зв'язку та захисту інформації України [Електронний ресурс]. – Режим доступу : https://cip.gov.ua/ua/news/oleksandr-potii-kiberbezpeka-zalishayetsya-takoyu-samoyu-arenoyu-boiovikh-dii-yak-i-inshi-domeni.
12. *Кузо М.О.* Порівняльний аналіз методик оцінювання ризиків інформаційної безпеки у вищих навчальних закладах : дипломна робота магістра за спеціальністю «125 – кібербезпека» / *М.О. Кузо.* – Тернопіль : ТНТУ, 2019. – 106 с.
13. Петренко А. Як кібератаки впливають на сектор видобутку вуглеводнів / NadraInfo [Електронний ресурс]. – Режим доступу : https://nadra.info/2024/10/artem-petrenko-how-cyberattacks-affect-the-hydrocarbon-sector/.
14. *Шульга Л.* Дослідження методів та моделей оцінювання кіберзахисту критичної інфраструктури держави / *Л.Шульга* // Сучасний захист інформації. – 2024. – № 3 (59). – С. 6–19.
15. Костюк І. Як штучний інтелект уже давно вирішує за нас / Osvitoriya Media [Електронний ресурс]. – Режим доступу : https://osvitoria.media/experience/yak-shtuchnyj-intelekt-uzhe-davno-vyrishuye-za-nas/.
16. *Поляков О.М.* Активізація міжнародної співпраці у сфері забезпечення кібербезпеки: шляхи удосконалення в реаліях сьогодення / *О.М. Поляков* // Інформація і право. – 2021. – № 2.
17. *Гончар С.Ф.* Методологія оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури : дис. д-ра техн. наук / *С.Ф. Гончар.* – Київ, 2020.
18. *Шевченко А.* Аналіз застосування методів машинного навчання на основі штучних нейронних мереж у прикладних задачах виявлення та класифікації кіберзагроз / *А.Шевченко, Г.Застело, Є.Шпачинський* // Information Technology and Security. – 2019. – Vol. 7, Iss. 1 (12). – P. 79–90 [Електронний ресурс]. – Режим доступу : https://ela.kpi.ua/items/1da6e657-b91a-4842-85f7-ea72ae928ad2.
19. Artificial Intelligence and National Security / Center for Strategic and International Studies
20. *Brundage M.* The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation / *M.Brundage* // Future of Humanity Institute, University of Oxford. – 2018.
21. *Avin S.* Filling gaps in trustworthy development of AI / *S.Avin and other*// Science. – 2021. – Vol. 374. – № 6573. – P. 1327–1329.
22. *Clark J.* Artificial Intelligence and National Security: The Importance of the AI Ecosystem / *J.Clark* // Brookings Institution. – 2020.
23. The NATO Cooperative Cyber Defence Centre of Excellence / CCDCOE.
24. Final Report. Arlington 2021 / National Security Commission on Artificial Intelligence.
25. The evolving role of AI-generated media in shaping disinformation campaigns / DFRLab [Electronic resource]. – Access mode : https://dfrlab.org/2025/05/01/the-evolving-role-of-ai-generated-media-in-shaping-disinformation-campaigns/.
26. Очі розвідки на полі бою, розмінування і укриття: що таке Palantir, як допомагає Україні у війні / 24Tv [Електронний ресурс]. – Режим доступу : https://24tv.ua/palantir-ukrayini-shho-za-it-kompaniya-yak-dopomagaye-rozvidtsi_n2726271.
27. *Pavlyshenko B.* AI Approaches to Qualitative and Quantitative News Analytics on NATO Unity / *B.Pavlyshenko.* – 2025. DOI: 10.48550/arXiv.2505.06313.
28. Технологію розпізнавання облич ClearView AI будуть використовувати українські військові / Forbes Ukraine [Електронний ресурс]. – Режим доступу : https://forbes.ua/innovations/tekhnologiyu-rozpiznavannya-oblich-clearview-ai-vvazhayut-nelegalnoyu-i-nebezpechnoyu-ii-budut-vikoristovuvati-ukrainski-viyskovi-16032022-4696.
29. *Гусак Ю.А.* Сучасні аспекти використання штучного інтелекту збройними силами України в умовах воєнного стану / *Ю.А. Гусак, С.В. Кітік, Д.В. Кандуєв* // Актуальні проблеми вітчизняної юриспруденції. – 2023. – № 2. – С. 91–95. DOI: /10.32782/39221475.
30. Наскільки «прозора» законність діяльності Clearview AI в Україні? / Лабораторія цифрової безпеки [Електронний ресурс]. – Режим доступу : https://dslua.org/publications/clearview-ai-v-ukraini/.
31. *Кузьмін О.Є.* Методи та моделі економіко-математичного аналізу : навч. посіб / *О.Є. Кузьмін, А.І. Грабченко, Л.М. Коваль*. – Львів: НУ «Львівська політехніка», 2019. – 412 с.
32. Що таке федеративне навчання (Federated Learning)? / The Transmitted [Електронний ресурс]. – Режим доступу : https://thetransmitted.com/adlucem/shho-take-federatyvne-navchannya-federated-learning.
33. Locked Shields 2025 Showcased Nations' Commitment to Defending Cyberspace / CCDCOE [Electronic resource]. – Access mode : https://ccdcoe.org/news/2025/locked-shields-2025-showcased-nations-commitment-to-defending-cyberspace/.
34. Cyber defence / NATO [Electronic resource]. – Access mode : https://www.nato.int/cps/en/natohq/topics_78170.htm.
35. NLTK Documentation / NLTK [Electronic resource]. – Access mode : https://www.nltk.org/index.html.
36. An adaptive approach to detecting fake news based on generalized text features / CEUR-WS [Electronic resource]. – Access mode : https://ceur-ws.org/Vol-3387/paper23.pdf.
37. Доктрина / Головне управління доктрин та підготовки генерального штабу Збройних Сил України.
38. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про Стратегічний оборонний бюлетень України» : Указ Президента України від 17 вересня 2021 року №473/2021 [Електронний ресурс]. – Режим доступу : https://www.president.gov.ua/documents/4732021-40121.

39. AI in War Games and C4ISR / ITHY [Electronic resource]. – Access mode : https://ithy.com/article/ai-wargaming-c4isr-lpafq444.
40. *Danyk Y.* Method of Cyber-Resilience Information-Control System Synthesis of Mosaic Structure / *Y.Danyk, V.Shestakov* // Emerging Networking in the Digital Transformation Age (TCSET 2022), 2022. – pp. 358–366. DOI: 10.1007/978-3-031-24963-1_20.
41. Step by Step, Ukraine Built a Technological Navy / USNI Proceedings [Electronic resource]. – Access mode : https://www.usni.org/magazines/proceedings/2025/may/step-step-ukraine-built-technological-navy.
42. Чи змінять війну дрони зі штучним інтелектом: що про них кажуть в Україні та світі / 24Tv [Електронний ресурс]. – Режим доступу : https://24tv.ua/droni-zi-shtuchnim-intelektom-yak-pratsyuyut-zakinchat-viynu_n2542448.
43. Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare / CSIS [Electronic resource]. – Access mode : https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare.
44. An Approach to the Formation of Artificial Intelligence Development Threat Indicators / Y.Danyk, M.Klymash, V.Shestakov, A.Masiuk // Digital Ecosystems: Interconnecting Advanced Networks with AI Applications (TCSET 2024) ; eds. A.Luntovskyy, M.Klymash, I.Melnyk and other. – Springer, 2024. – Vol. 1198. – P. 734–745. DOI: 10.1007/978-3-031-61221-3_35.

References:

1. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy, «Systema vyiavlennia vrazlyvostei i reahuvannia na kiberintsydenty ta kiberataky», [Online], available at: https://scpc.gov.ua/uk
2. «Attacks will get through': head of GCHQ urges companies to do more to fight cybercrime», *The Guardian*, [Online], available at: https https://www.theguardian.com/technology/2025/oct/23/gchq-companies-cyber-crime-threat
3. «Doppelgänger Operation», *EU DisinfoLab*, [Online], available at: https https://www.disinfo.eu/doppelganger-operation/
4. Kabinet Ministriv Ukrainy (2020), *Pro skhvalennia Kontseptsii rozvytku shtuchnoho intelektu v Ukraini*, Rozporiadzhennia vid 02.12.2020 r. No. 1556-r., [Online], available at: https https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text
5. «Ukraina vykorystovuie shtuchnyi intelekt u bezpilotnykh systemakh na peredovii – Kamyshin», *Ukrinform*, [Online], available at: https https://www.ukrinform.ua/rubric-ato/4003602-ukraina-vikoristovue-stucnij-intelekt-u-bezpilotnih-sistemah-na-peredovij-kamisin.html
6. Verkhovna Rada Ukrainy (2021), *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku «Pro Stratehiiu kiberbezpeky Ukrainy»*, Ukaz Prezydenta Ukrainy vid 26.08.2021 r. No. 447/2021, [Online], available at: https https://zakon.rada.gov.ua/go/447/2021
7. Kabinet Ministriv Ukrainy (2025), *Pro zatverdzhennia planu zakhodiv z realizatsii Kontseptsii rozvytku shtuchnoho intelektu v Ukraini na 2025-2026 roky*, Rozporiadzhennia vid vid 09.05.2025 r. No. 457-r., [Online], available at: https://zakon.rada.gov.ua/laws/show/457-2025-p#Text
8. Regulation (EU) 2024/1689 (EU AI Act), *EUR-Lex*, [Online], available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
9. Taddeo, M., Ziosi, M. and Tsamados, A. (2022), «Artificial Intelligence for National Security: The Predictability Problem», [Online], available at: https://cetas.turing.ac.uk/sites/default/files/2022-09/research_report_ai_predictability_problem_vfinal_3.pdf
10. «AI Strategy (2021)», *NATO*, [Online], available at: https://www.nato.int/cps/en/natohq/official_texts_227237.htm
11. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy, «Oleksandr Potii: kiberbezpeka zalyshaietsia takoiu samoiu arenoiu boiovykh dii, yak i inshi domeny», [Online], available at: https://cip.gov.ua/ua/news/oleksandr-potii-kiberbezpeka-zalishayetsya-takoyu-samoyu-arenoyu-boiovikh-dii-yak-i-inshi-domeni
12. Kuzo, M.O. (2019), *Porivnialnyi analiz metodyk otsiniuvannia ryzykiv informatsiinoi bezpeky u vyshchykh navchalnykh zakladakh*, dyplomna robota mahistra za spetsialnistiu «125 – kiberbezpeka», TNTU, Ternopil, 106 p.
13. «Petrenko A. Yak kiberataky vplyvaiut na sektor vydobutku vuhlevodniv», *NadraInfo*, [Online], available at: https://nadra.info/2024/10/artem-petrenko-how-cyberattacks-affect-the-hydrocarbon-sector/
14. Shulha, L. (2024), «Doslidzhennia metodiv ta modelei otsiniuvannia kiberzakhystu krytychnoi infrastruktury derzhavy», *Suchasnyi zakhyst informatsii*, No. 3 (59), pp. 6–19.
15. «Kostiuk I. Yak shtuchnyi intelekt uzhe davno vyrishuie za nas», Osvitoriya Media, [Online], available at: https://osvitoria.media/experience/yak-shtuchnyj-intelekt-uzhe-davno-vyrishuye-za-nas/
16. Poliakov, O.M. (2021), «Aktyvizatsiia mizhnarodnoi spivpratsi u sferi zabezpechennia kiberbezpeky: shliakhy udoskonalennia v realiiakh sohodennia», *Informatsiia i pravo*, No. 2.
17. Honchar, S.F. (2020), *Metodolohiia otsiniuvannia ryzykiv kiberbezpeky informatsiinykh system obiektiv krytychnoi infrastruktury*, dys. d-ra tekhn. nauk, Kyiv.
18. Shevchenko, A., Zastelo, H. and Shpachynskyi, Ye. (2019), «Analiz zastosuvannia metodiv mashynnoho navchannia na osnovi shtuchnykh neironnykh merezh u prykladnykh zadachakh vyiavlennia ta klasyfikatsii kiberzahroz», *Information Technology and Security*, Vol. 7, Iss. 1 (12), pp. 79–90, [Online], available at: https://ela.kpi.ua/items/1da6e657-b91a-4842-85f7-ea72ae928ad2
19. «Artificial Intelligence and National Security», *Center for Strategic and International Studies*
20. Brundage, M. (2018), «The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation», *Future of Humanity Institute*, University of Oxford.
21. Avin, S. and oth. (2021), «Filling gaps in trustworthy development of AI», *Science*, Vol. 374, No. 6573, pp. 1327–1329.
22. Clark, J. (2020), «Artificial Intelligence and National Security: The Importance of the AI Ecosystem», *Brookings Institution*.

23. «The NATO Cooperative Cyber Defence Centre of Excellence», *CCDCOE*.
24. «Final Report. Arlington 2021», *National Security Commission on Artificial Intelligence.*
25. «The evolving role of AI-generated media in shaping disinformation campaigns», *DFRLab*, [Online], available at: https://dfrlab.org/2025/05/01/the-evolving-role-of-ai-generated-media-in-shaping-disinformation-campaigns/
26. «Ochi rozvidky na poli boiu, rozminuvannia i ukryttia: shcho take Palantir, yak dopomahaie Ukraini u viini», *24Tv*, [Online], available at: https://24tv.ua/palantir-ukrayini-shho-za-it-kompaniya-yak-dopomagaye-rozvidtsi_n2726271
27. Pavlyshenko, B. (2025), «AI Approaches to Qualitative and Quantitative News Analytics on NATO Unity», doi: 10.48550/arXiv.2505.06313.
28. «Tekhnolohiiu rozpiznavannia oblych ClearView AI budut vykorystovuvaty ukrainski viiskovi», *Forbes Ukraine*, [Online], available at: https://forbes.ua/innovations/tekhnologiyu-rozpiznavannya-oblich-clearview-ai-vvazhayut-nelegalnoyu-i-nebezpechnoyu-ii-budut-vikoristovuvati-ukrainski-viyskovi-16032022-4696
29. Husak, Yu.A, Kitik, S.V. and Kanduiev, D.V. (2023), «Suchasni aspekty vykorystannia shtuchnoho intelektu zbroinymy sylamy Ukrainy v umovakh voiennoho stanu», *Aktualni problemy vitchyznianoi yurysprudentsii*, No. 2, pp. 91–95, doi: /10.32782/39221475.
30. «Naskilky «prozora» zakonnist diialnosti Clearview AI v Ukraini?», *Laboratoriia tsyfrovoi bezpeky*, [Online], available at: https://dslua.org/publications/clearview-ai-v-ukraini/
31. Kuzmin, O.Ye., Hrabchenko, A.I. and Koval, L.M. (2019), *Metody ta modeli ekonomiko-matematychnoho analizu*, navch. posib, NU «Lvivska politekhnika», Lviv, 412 p.
32. «Shcho take federatyvne navchannia (Federated Learning)?», The Transmitted, [Online], available at: https://thetransmitted.com/adlucem/shho-take-federatyvne-navchannya-federated-learning
33. «Locked Shields 2025 Showcased Nations' Commitment to Defending Cyberspace», *CCDCOE*, [Online], available at: https://ccdcoe.org/news/2025/locked-shields-2025-showcased-nations-commitment-to-defending-cyberspace/
34. «Cyber defence», *NATO*, [Online], available at: https://www.nato.int/cps/en/natohq/topics_78170.htm
35. «NLTK Documentation», *NLTK*, [Online], available at: https://www.nltk.org/index.html
36. «An adaptive approach to detecting fake news based on generalized text features», *CEUR-WS*, [Online], available at: https://ceur-ws.org/Vol-3387/paper23.pdf
37. «Doktryna», *Holovne upravlinnia doktryn ta pidhotovky heneralnoho shtabu Zbroinykh Syl Ukrainy*.
38. Verkhovna Rada Ukrainy (2021), *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 20 serpnia 2021 roku «Pro Stratehichnyi oboronnyi biuleten Ukrainy»*, Ukaz Prezydenta Ukrainy vid 17 veresnia 2021 r. No. 473/2021, [Online], available at: https://www.president.gov.ua/documents/4732021-40121
39. «AI in War Games and C4ISR», *ITHY*, [Online], available at: https://ithy.com/article/ai-wargaming-c4isr-lpafq444
40. Danyk, Y. and Shestakov, V. (2022), «Method of Cyber-Resilience Information-Control System Synthesis of Mosaic Structure», *Emerging Networking in the Digital Transformation Age (TCSET 2022)*, pp. 358–366, doi: 10.1007/978-3-031-24963-1_20.
41. «Step by Step, Ukraine Built a Technological Navy», *USNI Proceedings*, [Online], available at: https://www.usni.org/magazines/proceedings/2025/may/step-step-ukraine-built-technological-navy
42. «Chy zminiat viinu drony zi shtuchnym intelektom: shcho pro nykh kazhut v Ukraini ta sviti», *24Tv*, [Online], available at: https://24tv.ua/droni-zi-shtuchnim-intelektom-yak-pratsyuyut-zakinchat-viynu_n2542448
43. «Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare», *CSIS*, [Online], available at: https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare
44. Danyk, Y., Klymash, M., Shestakov, V. and Masiuk, A. (2024), «An Approach to the Formation of Artificial Intelligence Development Threat Indicators», Digital Ecosystems: Interconnecting Advanced Networks with AI Applications (TCSET 2024), in Luntovskyy, A., Klymash, M., Melnyk, I. et al. (ed.), Springer, Vol. 1198, pp. 734 – 745, doi: 10.1007/978-3-031-61221-3_35.

Danyk Y., Dykyi A, Shestakov V., Shyrshov R.

Implementation and Use of Artificial Intelligence for the Needs of Ukraine's Security and Defense Sector.

Abstract. The article substantiates the necessity of systematically introducing artificial-intelligence (AI) technologies into Ukraine's security and defense sector amid Russia's armed aggression and the escalation of cyber-threats. Drawing on domestic and international experience, the authors identify five key areas of AI application:

OSINT for monitoring troop movements, detecting sabotage, and forecasting crises;

protection of critical information infrastructure through behavioral analytics and anomaly-detection systems;

digital forensics with automated restoration of digital traces and evidence evaluation;

support to information and psychological operations via rapid generation of context-sensitive multimedia content;

detection and neutralization of adversary disinformation campaigns.

The main barriers to scaling AI solutions are outlined: information overload, scarcity of validated datasets, adversarial attacks, algorithmic opacity, and the ethical-legal constraints of autonomous systems. To overcome these challenges, the authors propose a set of organizational measures (state standards, tool certification, systematic workforce training) and technological measures (multi-level data verification, federated learning, backup control loops, and human-machine hybrid models).

The results provide a methodological foundation for state policy, the design of mission-critical digital platforms, and the enhancement of Ukraine's national-security legal and regulatory framework.

Keywords: artificial intelligence; AI conflicts; national security and defence; cybersecurity; OSINT; critical infrastructure; digital forensics; information operations; disinformation.

Стаття надійшла до редакції 10.11.2025.