

<https://doi.org/10.31891/2219-9365-2024-78-25>

УДК 004

САВЧЕНКО Ярослав

Приватний вищий навчальний заклад «Європейський університет»
<https://orcid.org/0009-0008-0381-0224>
e-mail: yaroslav.savchenko@e-u.edu.ua

ЯРОВИЙ Роман

Приватний вищий навчальний заклад «Європейський університет»
<https://orcid.org/0000-0001-8978-8137>
e-mail: roman.yaroviy@e-u.edu.ua

КОЛОДІНСЬКА Яніна

Приватний вищий навчальний заклад «Європейський університет»
<https://orcid.org/0000-0002-3330-7565>
e-mail: yanina.kolodinska@e-u.edu.ua

ЛЕВЧЕНКО Сергій

Приватний вищий навчальний заклад «Європейський університет»
<https://orcid.org/0009-0006-8497-0515>
e-mail: sergiy.levchenko@e-u.edu.ua

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ ТА МАШИННОГО НАВЧАННЯ В УМОВАХ ВІЙСЬКОВОГО СТАНУ

Ця стаття присвячена ролі штучного інтелекту (ШІ) та машинного навчання (МН) у військових операціях. Розглянуті можливості використання цих технологій для підвищення ефективності розвідки, прогнозування конфліктів, виявлення кібератак та управління автономними системами на полі бою. Детально проаналізовано методи створення систем на основі ШІ та МН, включаючи збір та передобробку даних, тренування моделей та їх застосування для прийняття рішень у реальному часі. Результати досліджень показують значний потенціал цих технологій для вдосконалення військових операцій та забезпечення безпеки військового персоналу.

Ключові слова: штучний інтелект, машинне навчання, військові операції, розвідка, прогнозування конфліктів, кібербезпека, автономні системи, нейронні мережі, аналіз даних, безпілотні транспортні засоби.

SAVCHENKO Yaroslav, YAROVIIY Roman, KOLODINSKA Yanina, LEVCHENKO Sergiy
Private Higher Educational Establishment "European University"

THE ROLE OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN THE CONDITIONS OF MARITAL STATE

Artificial intelligence (AI) and machine learning (ML) have already found widespread use in many fields, including medicine, finance, and transportation. In the military, these technologies can significantly improve operational efficiency, reduce risk to the military, and enable more accurate and prompt decision-making. However, the use of AI and MN in military operations raises a number of important scientific and practical challenges, such as ensuring the reliability of systems, preventing misuse of technologies, and solving ethical issues.

This article focuses on the role of artificial intelligence (AI) and machine learning (ML) in military operations. The possibilities of using these technologies to improve the effectiveness of intelligence, predicting conflicts, detecting cyberattacks and managing autonomous systems on the battlefield are considered. The methods of creating systems based on AI and MN are analyzed in detail, including data collection and processing, model training and their application for real-time decision-making. Research results show the significant potential of these technologies to improve military operations and ensure the safety of military personnel.

Artificial intelligence and machine learning have great potential to transform military operations, increasing their effectiveness and security. The use of these technologies in intelligence, forecasting, cyber security and autonomous systems is already showing significant benefits. However, there are challenges related to system reliability, data security, and ethical issues. Further research should be aimed at solving these problems, as well as at expanding the use of AI and MN in the military sphere.

Keywords: artificial intelligence, machine learning, military operations, intelligence, conflict prediction, cyber security, autonomous systems, neural networks, data analysis, unmanned vehicles.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Штучний інтелект (ШІ) та машинне навчання (МН) вже знайшли широке застосування у багатьох сферах, включаючи медицину, фінанси та транспорт. У військовій сфері ці технології можуть значно підвищити ефективність операцій, знизити ризики для військових та забезпечити більш точне та оперативне прийняття рішень. Проте використання ШІ та МН у військових операціях піднімає низку важливих наукових та практичних завдань, таких як забезпечення надійності систем, запобігання зловживанню технологіями та вирішення етичних питань.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

Використання ШІ та МН у військових операціях є актуальною темою наукових досліджень. Ці питання вчені аналізують і оцінюють на різних рівнях, використовуючи різні методи аналізу та оцінки. Даній проблематиці присвячено наукові доробки як вітчизняних, так і закордонних дослідників [1-3].

Зокрема, багато досліджень присвячено використанню ШІ для розвідки та спостереження, для автоматичного аналізу зображень та відео. Інші дослідження фокусуються на прогнозуванні конфліктів та оптимізації логістичних операцій за допомогою МН. Також важливим напрямом є використання ШІ у кібербезпеці, де системи МН використовуються для виявлення аномалій у мережевому трафіку. Автономні системи, такі як безпілотні транспортні засоби, також є об'єктом активних досліджень, особливо у контексті оптимізації маршрутів та прийняття рішень на полі бою.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою цієї статті є огляд сучасних напрямів використання ШІ та МН у військових операціях, аналіз їхніх переваг та викликів, а також обговорення перспектив подальших досліджень у цій сфері.

ВИКЛАДЕННЯ ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Штучний інтелект (ШІ) та машинне навчання (МН) мають потенціал кардинально змінити методи розвідки та спостереження у військових операціях. Ці технології відкривають нові можливості для аналізу та обробки великих обсягів даних, що дозволяє виявляти ворожі об'єкти, рух військ та інші потенційно важливі події на полі бою.

РОЗВІДКА ТА СПОСТЕРЕЖЕННЯ

Системи на основі ШІ можуть аналізувати зображення з безпілотників для виявлення ворожих об'єктів або руху військ. У цьому контексті використовуються бібліотеки машинного навчання, такі як TensorFlow або PyTorch, які дозволяють створювати нейронні мережі для автоматичного розпізнавання об'єктів на зображеннях.

Для створення таких систем, насамперед, використовується великий набір зображень, які є навчальними та тестовими даними для моделі. Після збору даних здійснюється їх передобробка, яка включає нормалізацію зображень для забезпечення уніфікованого масштабу даних. Далі визначається архітектура нейронної мережі, яка може включати кілька шарів конволюційних та повноз'язаних. Модель навчається на тренувальних даних, після чого оцінюється на тестових зображеннях для перевірки її ефективності. Такий підхід дозволяє значно підвищити точність та швидкість виявлення об'єктів, що є критичним для військових операцій.

Такі системи можуть бути використані як для стратегічного, так і для тактичного розвідування. Наприклад, вони можуть виявляти масштабні рухи військ на великих територіях або ж визначати місцезнаходження конкретних цілей на полі бою. Завдяки цьому вони допомагають забезпечити перевагу в бойових діях та знизити ризик для власних військ.

ПРОГНОЗУВАННЯ ТА ПРИЙНЯТТЯ РІШЕНЬ

МН може використовуватися для прогнозування можливих сценаріїв розвитку конфліктів або оптимізації логістичних операцій. Використовуючи історичні дані про конфлікти, алгоритми МН можуть прогнозувати ймовірність виникнення нових конфліктів у різних регіонах. Для цього широко використовуються такі бібліотеки як scikit-learn, які надають широкий набір інструментів для обробки даних та навчання моделей.

Наприклад, для прогнозування конфліктів може бути використано алгоритм Random Forest або градієнтний бустинг. Спочатку збираються історичні дані про конфлікти, а також інші релевантні показники, такі як економічні, соціальні та політичні фактори. Далі ці дані використовуються для навчання моделей, які можуть аналізувати взаємозв'язки між різними факторами та передбачати ймовірність виникнення нових конфліктів.

Навчені моделі МН, які базуються на історичних даних, можуть бути застосовані для прогнозування майбутніх подій та визначення оптимальних стратегій дій. Це дозволяє військовим командуванням заздалегідь підготуватися до можливих сценаріїв та приймати обґрунтовані рішення щодо розгортання сил і ресурсів.

Використання МН у військових стратегіях відкриває нові можливості для прогнозування та управління ризиками, забезпечуючи військовим командуванням засоби для ефективного відстоювання національних інтересів та забезпечення безпеки країни.

КІБЕРБЕЗПЕКА

Кібербезпека є однією з найважливіших сфер військових операцій. Алгоритми МН можуть навчатися на нормальному мережевому трафіку і виявляти аномалії, які можуть свідчити про кібератаку. У цьому

контексті використовуються бібліотеки, такі як scikit-learn або PyOD, для створення моделей, здатних виявляти аномалії у мережевому трафіку.

Процес виявлення аномалій починається з збору даних про мережевий трафік, який включає нормальний та потенційно аномальний трафік. Далі здійснюється обробка даних для виділення основних характеристик мережевого трафіку, таких як обсяг даних, час передачі, джерело та пункт призначення. Потім модель навчання, така як Isolation Forest або Autoencoders, навчається на нормальному трафіку, щоб розпізнавати аномалії, які відхиляються від нормальних шаблонів. Це дозволяє автоматично виявляти та реагувати на кібератаки в реальному часі.

Ці технології можуть бути використані для розробки імунних систем безпеки, які автоматично аналізують, виявляють та блокують кіберзагрози до того, як вони завдають шкоди мережі чи інформаційним системам. Крім того, вони дозволяють виявляти нові види кіберзагроз та адаптувати заходи безпеки для їх виявлення та запобігання.

АВТОНОМНІ СИСТЕМИ

Автономні системи, такі як безпілотники та роботизовані транспортні засоби, використовують ШІ та МН для самостійного прийняття рішень на полі бою. Це дозволяє зменшити ризик для людей і підвищити ефективність операцій. Для оптимізації маршрутів автономних транспортних засобів використовуються бібліотеки, такі як NetworkX, та алгоритми пошуку шляху, такі як A*.

Наприклад, безпілотний транспортний засіб може використовувати алгоритми МН для аналізу карти місцевості та знаходження оптимального маршруту з урахуванням поточних умов на полі бою. Процес починається з визначення графу або карти місцевості, яка включає різні можливі маршрути та перешкоди. Далі використовується алгоритм пошуку шляху, такий як A*, який дозволяє знаходити найкоротший та найменш небезпечний маршрут від стартової до кінцевої точки. Такий підхід забезпечує високу оперативність та точність у виконанні завдань.

Крім того, системи штучного інтелекту можуть допомагати в оптимізації енергоспоживання та використання ресурсів, аналізуючи динаміку витрат у реальному часі, щоб підтримувати оптимальний рівень функціонування системи. Це дозволяє зберігати енергію та ресурси, що особливо важливо у військових операціях з обмеженими ресурсами.

Таким чином, використання ШІ та МН в автономних системах відкриває нові перспективи для підвищення ефективності та безпеки військових операцій. Ці технології дозволяють системам самостійно приймати рішення та адаптуватися до змінних умов на місцевості, що робить їх незамінними знаряддями для військових дій.

ПРОТИДІЯ ДЕЗІНФОРМАЦІЇ ТА ПРОПАГАНДИ

Протидія дезінформації та пропаганді відіграє ключову роль у військових операціях, де ворожі сили намагаються впливати на суспільство та військових противників шляхом поширення фальшивих інформаційних повідомлень та маніпуляцій. Для виявлення та боротьби з такими загрозами використовуються інструменти аналізу тексту та візуалізації даних. Наприклад, бібліотека Natural Language Toolkit (NLTK) може бути використана для аналізу тексту та виявлення аномалій у способі поширення інформації, що може свідчити про дезінформацію або пропаганду. Додатково, бібліотеки для обробки природної мови, такі як SpaCy або TextBlob, дозволяють виявляти ключові слова, емоційне забарвлення тексту та інші ознаки, які можуть вказувати на маніпуляції в інформаційному просторі. Такі інструменти допомагають розвідникам та аналітикам вчасно виявляти та реагувати на спроби ворожих сил впливати на суспільство та військових противників шляхом маніпуляції інформацією.

АВТОМАТИЧНЕ РОЗПІЗНАВАННЯ МОВИ

Автоматичне розпізнавання мови в перехоплених комунікаціях відіграє важливу роль у зборі розвіданих та виявленні загроз безпеці. За допомогою бібліотек для обробки мови, таких як SpeechRecognition та Google Cloud Speech-to-Text, можна автоматизувати процес розпізнавання та транскрипції аудіо- або відеофайлів з виявленням ключової інформації.

Наприклад, системи автоматичного розпізнавання мови можуть використовуватися для моніторингу телефонних розмов або радіоелектронних перехоплень, забезпечуючи перевагу у виявленні загроз та ризиків. Такі системи можуть автоматично переводити мовлення на різні мови, аналізувати ключові теми та визначати тон або настрій співрозмовника. Це допомагає аналітикам та розвідникам швидко отримувати цінну інформацію з перехоплених комунікацій, що може використовуватися для прийняття стратегічних рішень та запобігання потенційним загрозам.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Штучний інтелект та машинне навчання мають великий потенціал для трансформації військових операцій, підвищуючи їх ефективність та безпеку. Використання цих технологій у розвідці, прогнозуванні, кібербезпеці та автономних системах вже демонструє значні переваги. Однак існують виклики, пов'язані з надійністю систем, безпекою даних та етичними питаннями. Подальші дослідження мають бути спрямовані на вирішення цих проблем, а також на розширення застосування ШІ та МН у військовій сфері.

Література

1. Демідов Б. О., Кучеренко Ю. Ф., Матюшенко О. Г. Основні напрямки застосування технологій, що містять елементи та методи штучного інтелекту, в оборонній сфері. Наука і техніка Повітряних Сил Збройних Сил України. 2018. № 4(33). С. 7-15.
2. Домарієв В. В. Система ситуаційного управління : Теорія, методологія, рекомендації. Київ : Знання України, 2017. 347 с.
3. Борисенко О.А., Бережна О.В., Новгородцев А.І., Сердюк В.В., Яковлев М.М. Система передачі та відображення інформації із захистом числових даних. Системи обробки інформації. 2019. № 2(157). С. 103-108. <https://doi.org/10.30748/soi.2019.157.14>.
4. Гриб Д. А., Демідов Б. О., Борисенко М. В., Кузнєцова М. Ю. Інформатизація управління структурною динамікою складних багатоструктурних систем військового призначення при динамічній зміні обстановки в районі ведення бойових дій. Збірник наукових праць.
5. Hui Liu, Investigation on Works and Military Applications of Artificial Intelligence. URL: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9143084>
6. Сергій Балашук, Штучний інтелект та бойове прогнозування: нові можливості для ЗСУ. URL: <https://softline.org.ua/news/shtuchnyi-intelekt-ta-boiove-prohnozuvannia-novi-mozhlyvosti-dlia-zsu>
7. Ігор Пилипів, "Війну виграють технології". Як штучний інтелект допоможе перемогти у війні з РФ? URL: <https://www.epravda.com.ua/publications/2023/12/4/707197/>
8. Ніколаєвський О.Ю., Скляренко О.В., Сидорчук А. Analysis and comparison of face detection Apis // Телекомунікаційні та інформаційні технології. - 2019.- № 4 (65) –С.121-133
9. Колодінська Яніна. Використання штучного інтелекту для управління процесами створення та розвитку ІТ-проектів //Штучний інтелект у науці та освіті (AISE 2024). Artificial intelligence in science and education: збірник матеріалів міжнародної наукової конференції (Київ, 1-2 березня 2024 р.) [Електронний ресурс] / [упоряд: А. Яцишин, В. Матусевич, В. Коваленко]. – Київ : УкрІНТЕІ, 2024. – С. 101-102.
10. Троян К.М., Скляренко О.В. Практичні кейси та перспективи розвитку технологій штучного інтелекту //Цифрова трансформація в економіці, менеджменті і бізнесі. Проблеми науки, практики та освіти: Зб. матеріалів XXVIII Міжн. наук.- практ. конф., Київ, 24.11.2022 р.; К.: Вид-во Європейського університету, 2023 – С. 66-68.
11. Скляренко О.В., Ніколаєвський О.Ю., Біометричні системи безпеки: розпізнавання облич // Актуальні питання забезпечення кібербезпеки та захисту інформації. Матеріали VII міжнародної науково-практичної конференції 24–27 лютого 2021 р.- Київ-2021.- Видавництво Європейського університету. – С. 85-87.

References

1. Demidov B. O., Kucherenko Yu. F., Matiushchenko O. H. Osnovni napriamky zastosuvannia tekhnolohii, shcho mistiat elementy ta metody shtuchnoho intelektu, v oboronni sferi. Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy. 2018. № 4(33). S. 7-15.
2. Domariiev V. V. Systema situatsiinoho upravlinnia : Teoriia, metodolohiia, rekomendatsii. Kyiv : Znannia Ukrainy, 2017. 347 s.
3. Borysenko O.A., Berezhna O.V., Novhorodtsev A.I., Serdiuk V.V., Yakovlev M.M. Systema peredachi ta vidobrazhennia informatsii iz zakhystom chyslovykh danykh. Systemy obrobky informatsii. 2019. № 2(157). S. 103-108. <https://doi.org/10.30748/soi.2019.157.14>.
4. Hryb D. A., Demidov B. O., Borysenko M. V., Kuznietsova M. Yu. Informatyzatsiia upravlinnia strukturoiu dynamikoiu skladnykh bahato strukturykh system viiskovoho pryznachennia pry dynamichnii zmini obstanovky v raioni vedennia boiovykh dii. Zbirnyk naukovykh prats.
5. Hui Liu, Investigation on Works and Military Applications of Artificial Intelligence. URL: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9143084>
6. Serhii Balashuk, Shtuchnyi intelekt ta boiove prohnozuvannia: novi mozhlyvosti dlia ZSU. URL: <https://softline.org.ua/news/shtuchnyi-intelekt-ta-boiove-prohnozuvannia-novi-mozhlyvosti-dlia-zsu>
7. Ihor Pylypiv, "Viinu vyhraiat tekhnolohii". Yak shtuchnyi intelekt dopomozhe peremohty u viini z RF? URL: <https://www.epravda.com.ua/publications/2023/12/4/707197/>
8. Nikolaievskiy O.Iu., Skliarenko O.V., Sydorochuk A. Analysis and comparison of face detection Apis // Telekomunikatsiini ta informatsiini tekhnolohii. - 2019.- № 4 (65) –S.121-133
9. Kolodinska Yanina. Vykorystannia shtuchnoho intelektu dlia upravlinnia protsesamy stvorennia ta rozvytku IT-proiektiv //Shtuchnyi intelekt u nauksi ta osviti (AISE 2024). Artificial intelligence in science and education: zbirnyk materialiv mizhnarodnoi naukovoї konferentsii (Kyiv, 1-2 bereznia 2024 r.) [Elektronnyi resurs] / [uporiad: A. Yatsyshyn, V. Matusevych, V. Kovalenko]. – Kyiv : UkrINTEI, 2024. – S. 101-102.
10. Troian K.M., Skliarenko O.V. Praktychni keisy ta perspektyvy rozvytku tekhnolohii shtuchnoho intelektu //Tsyfrova transformatsiia v ekonomitsi, menedzhmenti i biznesi. Problemy nauky, praktyky ta osvity: Zb. materialiv KhKhVIII Mizhn. nauk.- prakt. konf., Kyiv, 24.11.2022 r.; K.: Vyd-vo Yevropeiskoho universytetu, 2023 – S. 66-68.
11. Skliarenko O.V., Nikolaievskiy O.Iu., Biometrychni systemy bezpeky: rozpiznavannia oblych // Aktualni pytannia zabezpechennia kiberbezpeky ta zakhystu informatsii. Materialy VII mizhnarodnoi naukovo-praktychnoi konferentsii 24–27 liutoho 2021 r.- Kyiv-2021.- Vydavnytstvo Yevropeiskoho universytetu. – S. 85-87.