2. IT-індустрія на захисті України: донати, інновації та підтримка армії URL: https://fact-news.com.ua/it-industriya-na-zahisti-ukraini-donati-innovatsii-ta-pidtrimka-armii

3. Ukrsibbank підтримав дослідження «Де IT на війні», яке представила Асоціація IT Ukraine та Mind URL: https://minfin.com.ua/ua/2024/09/26/136391488/

4. Де IT на війні: Асоціація IT Ukraine та Mind представили унікальне дослідження про внесок IT-індустрії у боротьбу проти російської агресії URL: https://itukraine.org.ua/de-it-na-vijni-asotsiatsiya-it-ukraine-ta-mind-predstavili-unikalne-doslidzhennya-pro-vnesok-it-industriyi-u-borotbu-proti-rosijskoyi-agresiyi/

УДК: 004.8:355.4:623.618

Станько А., доктор філософії; Дідич І., доктор філософії; Микитишин А.; Зозуляк Б.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ АНАЛІЗУ РОЗВІДУВАЛЬНИХ ДАНИХ, РОЗПІЗНАВАННЯ ЦІЛЕЙ І ПРОГНОЗУВАННЯ РОЗВИТКУ КОНФЛІКТІВ

Анотація. У тезі розглянуто застосування технологій штучного інтелекту для аналізу розвідувальних даних, автоматизованого розпізнавання цілей і прогнозування сценаріїв розвитку військових конфліктів. Окреслено основні напрями використання ШІ: обробка зображень, аналіз текстової інформації, ф'южн-аналіз та побудова прогностичних моделей. Проаналізовано переваги, виклики та ризики впровадження таких рішень у військовій сфері, зокрема в контексті сучасних гібридних загроз. Наведено перспективи розвитку ШІ в оборонному секторі України.

Ключові слова: штучний інтелект, розвідувальні дані, розпізнавання цілей, прогнозування конфліктів, військова аналітика.

Stanko A., PhD; Didych I., PhD; Mykytyshyn A., Zozuliak B.
Ternopil Ivan Puluj National Technical University, Ukraine

USE OF ARTIFICIAL INTELLIGENCE TO ANALYSE INTELLIGENCE DATA, RECOGNISE TARGETS AND PREDICT THE DEVELOPMENT OF CONFLICTS

Abstract. The paper discusses the use of artificial intelligence technologies for intelligence analysis, automated target recognition, and forecasting scenarios of military conflicts. The main areas of AI use are outlined: image processing, textual information analysis, fusion analysis, and building predictive models. The advantages, challenges and risks of implementing such solutions in the military sphere, in particular in the context of modern hybrid threats, are analyzed. Prospects for the development of AI in the defense sector of Ukraine are presented.

Keywords: artificial intelligence, intelligence data, target recognition, conflict forecasting, military analytics.

Сучасні воєнні конфлікти характеризуються високою динамікою, гібридними загрозами та великим обсягом даних, які потребують швидкої та точної обробки. Традиційні методи аналізу розвідувальної інформації (data intelligence) часто є недостатньо ефективними через людський фактор, обмеженість ресурсів і часового фактору [1]. Впровадження технологій штучного інтелекту (ШІ) у сферу військової аналітики дозволяє автоматизувати обробку великих масивів даних (Big Data), підвищити точність розпізнавання об'єктів, виявляти приховані закономірності та формувати прогностичні моделі розвитку конфліктів [2].

Технології ШІ інтегруються у процеси збору та обробки інформації з різних джерел: супутникових знімків, безпілотних літальних апаратів (БПЛА), радіоперехоплень, відкритих джерел (OSINT), сенсорних систем та кіберпростору [3].

Основні напрямки застосування включають:

– Обробку зображень і відео: системи комп'ютерного зору (Computer Vision) здатні розпізнавати військову техніку, об’єкти інфраструктури, пересування військ у реальному часі [4].

– Натурально-мовний аналіз (NLP): аналіз текстових повідомлень, соцмереж, перехоплень для виявлення загроз, координації дій противника або інформаційних операцій [5].

– Ф'южн-аналіз: об’єднання різнотипних даних для створення цілісної картини оперативної обстановки [6].

– Застосування ШІ дозволяє автоматизувати процес ідентифікації стратегічно важливих цілей. Алгоритми машинного навчання (ML) навчаються на великих наборах даних, щоб з високою точністю:

– Визначати типи об’єктів (наприклад, розрізнення військової техніки від цивільних об’єктів) [4].

– Виявляти аномалії, які можуть свідчити про підготовку до наступальних дій.

– Оцінювати ймовірність розвитку певних сценаріїв на основі історичних даних і поточної ситуації [7].

Такі системи стають основою для систем підтримки прийняття рішень (DSS), що дозволяє військовому командуванню оперативно реагувати на зміни в зоні конфлікту.

Інструменти ШІ здатні моделювати сценарії розвитку подій з урахуванням багатьох змінних: політичних рішень, логістики, економічних факторів, настроїв населення та військових дій [8]. Використання нейромережевих моделей та агентного моделювання (agent-based modeling) дозволяє: Оцінювати ризики ескалації конфлікту; Передбачати можливі маршрути наступу або відступу військ; Визначати найбільш вразливі точки у власній обороні чи в системі супротивника [9].

Прогностичні системи також враховують інформаційно-психологічні операції (ІПсО), що суттєво впливають на хід сучасних гібридних конфліктів.

Попри значні переваги, використання ШІ у військовій сфері супроводжується низкою викликів: якість даних: для ефективного навчання алгоритмів необхідні великі обсяги достовірної та репрезентативної інформації [3]; Кібербезпека: системи ШІ стають потенційною ціллю для кібератак і маніпуляцій (атаки на навчальні дані, підміна об’єктів) [10]; Етичні аспекти: автономні системи розпізнавання цілей можуть викликати дискусії щодо відповідальності за прийняті рішення, особливо в контексті летальних автономних систем (LAWS) [11]; Ймовірність хибних позитивних або негативних результатів, що в умовах війни може призвести до критичних помилок.

В умовах збройної агресії проти України активне використання ШІ у сфері оборони є важливим інструментом для посилення розвідувальних можливостей. Українські ІТ-фахівці вже залучають ШІ для аналізу супутникових знімків, автоматизації обробки даних БПЛА та моніторингу кіберзагроз [7]. Подальший розвиток таких систем потребує інвестицій у наукові дослідження, створення захищених дата-центрів, а також співпраці з міжнародними партнерами у сфері оборонних технологій.

Штучний інтелект відкриває нові горизонти у військовій аналітиці: від швидкої обробки розвідувальних даних до прогнозування розвитку конфліктів. Його застосування підвищує ефективність прийняття рішень, знижує навантаження на аналітичні служби та забезпечує проактивний підхід до управління військовими операціями. Водночас необхідно враховувати ризики, пов’язані з кіберзагрозами, якістю даних і етичними аспектами застосування автономних систем.

Джерела та література

1. Коваль В.О. Інформаційно-аналітичні системи у військовій справі // *Оборонні технології*. – 2021. – №3. – С. 15–22.

2. Smith J. Artificial Intelligence in Military Decision-Making // *Journal of Defense Studies*. – 2020. – Vol. 12(4). – P. 101–115.

3. Петренко І.М. Big Data у військовій розвідці // *Системи управління та навігації*. – 2022. – №2. – С. 45–50.

4. Lee K., Park S. Computer Vision for Target Recognition // *IEEE Access*. – 2019. – Vol. 7. – P. 150123–150135.

5. Johnson A. NLP Applications in Intelligence Analysis // *AI & Security Review*. – 2021. – Vol. 9(1). – P. 33–47.

6. Brown M. Data Fusion Techniques in Military Intelligence // *Defense Technology*. – 2020. – Vol. 16(2). – P. 200–210.

7. Сидоренко Р.П. Використання ШІ для аналізу даних БПЛА в Україні // *Збірник наукових праць НАОУ*. – 2023. – №1. – С. 60–66.

8. Chen Y. Conflict Prediction Models Using AI // *International Journal of Conflict Studies*. – 2021. – Vol. 5(3). – P. 78–92.

9. Miller D. Agent-Based Modeling in Warfare Scenarios // *Computational Military Science*. – 2022. – Vol. 8(2). – P. 120–135.

10. Гуменюк Л.В. Кіберзагрози для систем ШІ у військовій сфері // *Інформаційна безпека України*. – 2022. – №4. – С. 25–31.

11. Anderson K. Ethics of Autonomous Weapons // *Journal of Military Ethics*. – 2020. – Vol. 19(1). – P. 1–17.

УДК: 621.311.2:004.91

Станько А., доктор філософії; Микитишин А., канд. техн. наук, доц.; Блавіцький А.
Тернопільський національний технічний університет імені Івана Пулюя, Україна

СМАРТ-МЕРЕЖІ ТА БЛОКЧЕЙН-РІШЕННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ СТАБІЛЬНОГО ЕНЕРГОПОСТАЧАННЯ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ

Анотація. У роботі проаналізовано впровадження смарт-мереж (smart grid) та блокчейн-рішень для стабільного енергопостачання в умовах надзвичайних ситуацій. Особливу увагу приділено воєнним конфліктам та техногенним катастрофам, коли централізовані системи енергозабезпечення виявляються вразливими. Смарт-мережі дають змогу оперативно балансувати споживання та генерацію, а блокчейн-технології забезпечують прозорий та децентралізований облік енергії і фінансових транзакцій. Розглянуто приклади використання мікромереж, технології Peer-to-Peer для купівлі-продажу електроенергії, а також вплив законодавчих, економічних та кібербезпекових чинників на запровадження цих рішень в Україні. Зроблено висновок про доцільність комплексної стратегії розвитку децентралізованої енергетики для підвищення надійності та безпеки енергетичної інфраструктури.

Ключові слова: смарт-мережі, блокчейн, енергопостачання, надзвичайні ситуації, енергетична безпека.

Stanko A., PhD; Mykytyshyn A., PhD (Tech.), Assoc. Prof.; Blavitskyi A.
Ternopil Ivan Puluj National Technical University, Ukraine

SMART GRIDS AND BLOCKCHAIN SOLUTIONS TO ENSURE STABLE ENERGY SUPPLY IN EMERGENCY SITUATIONS

Abstract. The paper analyzes the implementation of smart grids and blockchain solutions for stable energy supply in emergency situations. Particular attention is paid to military conflicts and man-made disasters, when centralized energy supply systems are vulnerable. Smart grids allow for a quick balance of consumption and generation, and blockchain technologies provide transparent and decentralized accounting of energy and financial transactions. Examples of the use of microgrids, Peer-to-Peer technology for the purchase and sale of electricity, as well as the impact of legislative,