Джерела та література

1. Сталий розвиток. Центр екологічної сертифікації та маркування. Режим доступу : https://www.ecolabel.org.ua/stalij-rozvitok

2. Шуляк О. Цифровізація відбудови: як зробити процес максимально прозорим. ThePage. 2023. Режим доступу : https://thepage.ua/ua/experts/yak-zrobiti-proces-vidbudovi-ukrayini-maksimalno-prozorim

3. Даценко В. Пріоритезація проєктів відбудови: чому важливо правильно розподіляти ресурси на відновлення. Трансперенсі Інтернешнл Україна. 2023. Режим доступу : https://ti-ukraine.org/blogs/priorytezatsiya-proyektiv-vidbudovy-chomu-vazhlyvo-pravylno-rozpodilyaty-resursy-na-vidnovlennya/

**Публікація містить результати дослідження "Фундаментальні засади сталого та інклюзивного розвитку регіонального простору для повоєнного відновлення в умовах цифрової трансформації" (№ д.р. 0125U001620), що фінансується за рахунок державного бюджету України.*

УДК: 32

Лубкович Н., канд.істор.н., Лубкович А.
Галицький фаховий коледж імені В'ячеслава Чорновола, Україна

РОЛЬ ІТ-СЕКТОРУ В ЗАБЕЗПЕЧЕННІ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

Анотація. У статті досліджується роль ІТ-сектору України в забезпеченні обороноздатності країни в умовах російської агресії. Аналізуються ключові напрямки внеску ІТ-галузі, включаючи розробку військових технологій, кібербезпеку, волонтерську діяльність та економічну підтримку. Розглядаються перспективи розвитку військових технологій в Україні.

Ключові слова: ІТ-галузь, ІТ-сектор, обороноздатність, російська агресія, військові технології, кібербезпека, волонтерство.

Lubkovych N., PhD (History), Lubkovych A.
Vyacheslav Chornovil Halytskyi College, Ukraine

THE ROLE OF THE IT-SECTOR IN ENSURING UKRAINE'S DEFENSE CAPABILITY

Abstract. The article explores the role of Ukraine's IT sector in ensuring the country's defense capabilities under conditions of Russian aggression. It analyzes key areas of the IT industry's contribution, including military technology development, cybersecurity, volunteer activities, and economic support. The prospects for the development of military technologies in Ukraine are examined.

Keywords: IT industry, IT sector, defense capability, Russian aggression, military technologies, cybersecurity, volunteering.

Понад десять років триває військовий конфлікт, спровокований агресією російської федерації проти України. Цей конфлікт набув характеру екзистенційного виклику для української держави та став лакмусовим папірцем, що виявив ступінь прихильності держав світового співтовариства до демократичних цінностей.

Аналіз ситуації свідчить, що російсько-українська війна не обмежилася рамками двостороннього протистояння, вона актуалізувала питання збереження європейської та глобальної системи безпеки, що базується на принципах пріоритету демократії та міжнародного права.

Повномасштабна війна проти до зубів озброєного, технічно спорядженого, ідеологічно отруєного, антигуманно налаштованого російського ворога формує жорсткі вимоги до якості використання Силами оборони України технічних і технологічних досягнень [1, с.4]

В умовах війни ключову роль відіграє ІТ-сектор України. Він активно залучений до розробки військових технологій. Українські ІТ-фахівці створюють програмне забезпечення для систем зв'язку, розвідки та управління військами. Розробляють дрони, роботизовані системи та інші технологічні рішення для використання у військових операціях. Щонайменше 10 тисяч ІТ-фахівців вступили до лав ЗСУ, а понад 400 тисяч активістів, більшість з яких – айтівці, приєдналися до кіберспротиву [2].

Кібербезпека є критично важливим аспектом національної безпеки, особливо в умовах війни. ІТ-фахівці України відіграють ключову роль у захисті критичної інфраструктури від кібератак. Вони розробляють та впроваджують системи захисту інформаційних систем ЗСУ від кіберзагроз. Понад 400 тисяч фахівців долучилися до кіберспротиву, а 70% великих ІТ-компаній мають співробітників, що «вступили» до кібервійська (CERT-UA та IT ARMY – важливі складові кіберспорту українців).

ІТ-фахівці України також активно долучаються до волонтерської діяльності з підтримки конкретних підрозділів ЗСУ, Нацгвардії, Сил територіальної оборони та добровольчих формувань територіальних громад (ДФТГ), ГУР МО та СБУ. ІТ-індустрія за останні два роки спрямувала 8,8 мільярда гривень на потреби конкретних підрозділів та військових. Якщо на початку повномасштабного вторгнення ця допомога нагадувала оперативне «гасіння пожежі», то з часом вона стала чітко структурованою та фаховою. Співробітники ІТ-компаній швидко занурилися в нюанси закупівель і технічні характеристики необхідного захисникам озброєння. Окрім прямої грошової допомоги, ІТ-компанії купують техніку та обладнання для бойових підрозділів, виплачують зарплату своїм мобілізованим співробітникам, волонтерять тощо.

Крім того, згідно дослідження, 75% опитаних ІТ-компаній співпрацюють із різноманітними благодійними фондами, такими як UNITED24, «Повернись Живим», «Діти Героїв», KOLO та іншими. Варто зазначити, що половина великих ІТ-компаній мають власні благодійні фонди [3].

Також, ІТ-галузь сприяє економічній стабільності України під час війни. Суспільство має бачити повний спектр цього внеску – від донатів, проєктів, соціальних ініціатив чи технологічних розробок до створених робочих місць

Окремий напрямок діяльності ІТ-індустрії є – соціальні проєкти. Як мінімум 2,43 млрд грн за період повномасштабного вторгнення спрямувала ІТ індустрія на вирішення різноманітних гострих соціальних проблем: закупівля медикаментів, медичної техніки та обладнання, гуманітарна допомога та допомога ДСНС, відновлення постраждалих від війни територій, донація крові, допомога дітям, молоді, особам похилого віку, внутрішньо переміщеним особам та тваринам, евакуація, соціальна підтримка та освітні проєкти, проєкти у сфері розвитку громад, культурні проєкти і колаборації [4].

Російська агресія стимулює розвиток військових технологій в Україні. У майбутньому планується активне використання штучного інтелекту, машинного навчання та інших перспективних технологій у військових цілях.

Отже, в умовах повномасштабного вторгнення українська технологічна індустрія стала потужною силою загальноукраїнського спротиву російській агресії. Компанії та фахівці не тільки інвестують значні кошти та реалізують соціальні проєкти, але й застосовують свої знання та досвід для підтримки Сил оборони, мобілізованих працівників і ветеранів. Продовжуючи інвестувати у перемогу України, ІТ-галузь демонструє стійкість та готовність до змін, рухаючись до перемоги разом з усією країною.

Джерела та література

1. Застосування Сухопутних військ Збройних Сил України у конфліктах сучасності: Збірник тез доповідей Всеукраїнської науково-практичної конференції (Львів, 28-29 листопада 2024р.). – Львів: НАСВ, 2024. – 380 с. URL: chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://asv.mil.gov.ua/sites/default/files/2025-03/1-zbirnyk-tez

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: