Література

1. Збірник матеріалів Міжнародної науково-практичної конференції «Інформаційна безпека: сучасний стан, проблеми та перспективи» Кам'янець-Подільський національний університет імені Івана Огієнка, 2023. 113 с. URL: https://politkaf.kpnu.-edu.ua/wp-content/uploads/2023/04/zbirnyk-material-konfer.-inf_bezp_2023.pdf ;
2. Варенко В.М. Інформаційно-аналітична діяльність: Навч. посіб. / В. М. Варенко. – К.: Університет «Україна», 2014. – 417 с. URL: https://kjourn.pnu.edu.ua/wp-content/uploads/sites/54/2018/04/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%BE-%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D1%82%D0%B8%D1%87%D0%BD%D0%B0-%D0%B4%D1%96%D1%8F%D0%BB%D1%8C%D0%BD%D1%96%D1%81%D1%82%D1%8C.pdf ;
3. Проблеми інформаційного забезпечення та розвитку парламентського контролю в контексті Європейської та Євроатлантичної інтеграції України : матеріали наук.-практ. конф. (Київ, 25 квіт. 2024 р.) / упоряд.: В. М. Фурашев, С. О. Дорогих, О. В. Лебединська, О. Г. Радзієвська. – Київ; Одеса : Фенікс, 2024. – 150 с. URL: https://ippi.org.ua/sites/default/files/konferenciya_25.04.2024.pdf ;
4. Вагонова О. Г., Горпинич О. В., Чорнобаєв В. В. Організація діяльності органів державної влади : навч. посіб. ; М-во освіти і науки України, НТУ «Дніпровська політехніка». Дніпро : НТУ «ДП», 2019. 77 с.;
5. Демкова М., Фігель М. Інформація, як основа інформаційного суспільства: поняття та правове регулювання. URL: https://www.oa.edu.ua› loadnew›5.doc;
6. Ліпкан В. А., Сопілко І. М., Кір'ян В. О. Правові засади розвитку інформаційного суспільства в Україні : монографія / за заг. ред. В. А. Ліпкана. Київ : ФОП О. С. Ліпкан, 2015. 664 с.;
7. Загуменна В. В., Кузьменко О. І. Інформаційно-аналітична діяльність як наукова та навчальна дисципліна: еволюція, тенденції розвитку. Бібліотекознавство. Документознавство. Інформологія. 2022. № 4. С. 102-107.

Haborets Olha Andriivna

Associate Professor of the Department of Operational and Search Activities and Information Security, Donetsk State University of Internal Affairs, PhD, Associate Professor

DEFENSE ANALYTICS: LEVERAGING ARTIFICIAL INTELLIGENCE FOR STRATEGIC INSIGHTS AND OPERATIONAL EXCELLENCE

Artificial intelligence (AI) has emerged as a revolutionary tool in the defense sector, fundamentally transforming the way analytical support is provided for operations and decision-making. In an era characterized by complex and evolving threats, such as cyberattacks, hybrid warfare, and asymmetric conflicts, AI plays a critical role in enabling defense organizations to maintain operational superiority. The ability to process and analyze vast amounts of data in real time, anticipate potential threats, and provide actionable intelligence makes AI indispensable for modern defense strategies.

One of the most prominent applications of AI in defense analytics is in the field of big data analysis and intelligence gathering. Defense operations generate immense volumes of data from a multitude of sources, including satellite imagery, sensors, open-source intelligence (OSINT), and social media platforms. AI algorithms excel in processing this data, identifying patterns, and drawing correlations that are often imperceptible to human analysts. For example, AI-driven natural language processing (NLP) systems can parse intelligence reports, extracting critical information and detecting early warning signs of emerging threats. These capabilities enable defense agencies to act proactively, addressing potential risks before they escalate.

Predictive analytics is another area where AI has made a significant impact. Machine learning (ML) models analyze historical data to identify trends and predict potential security risks. In the context of cybersecurity, AI algorithms can detect anomalies and vulnerabilities in networks, anticipating attacks such as phishing, malware intrusions, or distributed denial-of-service (DDoS) assaults. By providing a predictive framework, AI enhances the ability of defense organizations to mitigate risks and implement preemptive measures. For example, predictive models can forecast enemy troop movements or cyberattack strategies, allowing for more effective resource allocation and response planning.

AI also enhances situational awareness by integrating data from multiple sources and presenting it in a coherent and actionable format. This capability is particularly critical in complex and dynamic operational environments. For instance, AI-enabled image recognition systems can analyze satellite or drone imagery to detect enemy installations, identify equipment, or monitor unusual activities. By synthesizing geospatial data, battlefield sensor inputs, and real-time surveillance, AI provides commanders with a comprehensive understanding of the operational landscape. This enhanced situational awareness is pivotal for informed decision-making, minimizing risks, and maximizing mission success.

Automation is another area where AI significantly contributes to the efficiency of defense analytics. Routine tasks, such as categorizing data, generating reports, and indexing documents, can be automated using AI, allowing human analysts to focus on higher-level strategic analysis. Virtual assistants and chatbots powered by AI further enhance productivity by assisting with data retrieval, answering routine queries, and streamlining communication processes. This shift towards automation not only reduces the workload of personnel but also accelerates the decision-making process, which is often critical in time-sensitive defense operations.

Cybersecurity, a cornerstone of modern defense strategies, greatly benefits from AI-driven innovations. Advanced intrusion detection systems (IDS) powered by AI monitor network traffic, identifying and neutralizing threats in real time. AI algorithms are capable of recognizing suspicious patterns, such as unauthorized access attempts or abnormal data transfers, and can automatically deploy countermeasures to prevent data breaches. Furthermore, AI enhances the ability to secure sensitive information by employing techniques like encryption, anomaly detection, and user behavior analysis. This is particularly important in safeguarding classified information and ensuring the integrity of defense communication systems.

Despite its numerous advantages, the integration of AI into the defense sector is not without challenges. One of the primary hurdles is ensuring the availability of high-quality and diverse datasets for training AI models. Incomplete, biased, or corrupted data can lead to inaccurate results, undermining the reliability of AI systems. Additionally, ethical and legal concerns arise with the deployment of AI, particularly in autonomous systems capable of

lethal actions. The use of AI in defense must align with international laws and ethical guidelines to ensure accountability and prevent misuse.

Technical and organizational barriers also pose significant challenges. Integrating AI into existing defense infrastructure requires substantial investment in hardware, software, and personnel training. Resistance to change and a lack of AI literacy among staff can further hinder adoption. Moreover, the risk of adversarial AI, where opponents exploit vulnerabilities in AI systems, necessitates the development of robust countermeasures. Techniques such as adversarial training, continuous model updates, and advanced security protocols are essential to safeguard AI systems from manipulation.

Looking to the future, the role of AI in defense analytics is expected to expand exponentially. Emerging technologies, such as quantum computing, promise to enhance AI capabilities by enabling faster data processing and more complex analysis. The development of collaborative AI-human systems will further optimize decision-making by combining the strengths of machine precision with human intuition and ethical judgment. Additionally, advancements in autonomous systems, including drones, robotics, and unmanned vehicles, will revolutionize reconnaissance, logistics, and combat operations.

In conclusion, artificial intelligence represents a paradigm shift in the analytical support systems of the defense sector. By enabling real-time intelligence, predictive analytics, enhanced situational awareness, and automated processes, AI empowers defense organizations to address emerging threats with unprecedented efficiency and precision. However, to fully realize the potential of AI, it is crucial to overcome challenges related to data quality, ethical considerations, and adversarial risks. Continuous investment in AI research, infrastructure, and personnel training will be essential for ensuring that AI remains a reliable and secure asset in the defense sector. With strategic integration, AI has the potential to redefine the future of national and global security.

References

1. Prosvirina T.V., Haborets O.A., Lunhol O.M. Analysis of the organization of information and analytical support of police activities. Scientific innovations and advanced technologies. Issue № 1(15) 2023. Pp. 319 – 327.
2. Габорець О., Шаєц Є. Впровадження штучного інтелекту у системи моніторингу та прогнозування громадської безпеки. Збірник тез доповідей ІІ Міжнар. наук.-практич. конфер. «Інновації та перспективні шляхи розвитку інформаційних технологій» (06 груд. 2023 р., м. Черкаси) [Електронний ресурс] / упоряд. : Т. О. Прокопенко, Я. В. Тарасенко ; М-во освіти і науки України, Черкас. держ. технол. ун-т. – Черкаси : ЧДТУ, 2023. С. 105-106.

Галайко Наталія Володимирівна

старший викладач кафедри інформаційних систем та технологій ННІУПБ Львівського державного університету внутрішніх справ

РОЛЬ CRM-ТЕХНОЛОГІЙ У ПІДВИЩЕННІ ЕФЕКТИВНОСТІ БІЗНЕСУ

Сучасні умови ведення бізнесу, що характеризуються високою конкуренцією, швидким розвитком технологій та змінюваними вимогами ринку, свідчать про те, що успіх можуть досягти лише ті компанії, які здатні ефективно інтегрувати сучасні