Збірник наукових праць. Галузеве машинобудування, будівництво
Academic journal. Industrial Machine Building, Civil Engineering
http://journals.nupp.edu.ua/znp
https://doi.org/10.26906/znp. 2025.64.4034

UDC 658.382.3:355.01:004.8

Volodymyr Pogrebnyak *
Ivano-Frankivsk National Technical University of Oil and Gas
https://orcid.org/0000-0002-7735-3408

Oleksandr Kondrat
Ivano-Frankivsk National Technical University of Oil and Gas
https://orcid.org/0000-0003-4406-3890

Iryna Perkun
Ivano-Frankivsk National Technical University of Oil and Gas
https://orcid.org/0000-0002-6523-1606

Andrii Pogrebnyak
University of Customs and Finance
https://orcid.org/0000-0003-3214-6410

Transforming Occupational Safety and Civil Defense: Wartime Challenges and Solutions

Abstract. This article is dedicated to the urgent need for a fundamental reform of traditional occupational safety and civil defense systems under the conditions of a full-scale war. It examines new, previously unseen risks to the life and health of employees caused by military actions. These threats extend far beyond conventional occupational hazards, including direct missile strikes, the destruction of buildings, cyberattacks, and a severe impact on the mental health of personnel. It is proven that old approaches to occupational safety, which focused on preventing accidents in peacetime, are completely unable to cope with the dynamic, unpredictable, and aggressive nature of military threats. The paper substantiates the urgent need to integrate civil defense measures into the occupational safety management system, transforming two separate systems into a single, holistic, human-centric safety model at the level of each enterprise. Special attention is given to how digital technologies, particularly artificial intelligence (AI), can assist in this process. It demonstrates how AI can predict threats based on the analysis of large volumes of data, automate alert systems, optimize evacuation routes in real time, automatically assess damage, support decision-making in crisis situations, and provide psychological support to personnel. A conceptual model of such an integrated occupational safety and civil defense system, enhanced by AI tools, is proposed. This allows for a shift from a simple reaction to events towards proactive, preventive safety management. Finally, practical and scalable recommendations are formulated for enterprise managers to help them incrementally implement technological innovations into safety processes to increase the resilience and protection of personnel in wartime conditions, even with limited resources.

Keywords: occupational safety, civil defense, martial law, artificial intelligence, predictive analytics, integrated system, psychosocial risks.

*Corresponding author E-mail: VGPogrebnyak@gmail.com

Received: 17.04.2025 Accepted: 05.05.2025 Published: 26.06.2025

Introduction.

The full-scale invasion of Ukraine by the Russian Federation on February 24, 2022, and the introduction of martial law became a catalyst for fundamental changes in all spheres of public life, including labor relations. The state, employers, and employees alike faced unprecedented challenges: how to ensure one of the most basic human rights – the right to safe and healthy working conditions. The traditional paradigm of occupational safety, which for decades focused on minimizing workplace risks (mechanical, chemical, biological), proved ill-adapted to these new threats. Classical safety models were designed for predictable, localized, and predominantly unintentional events, whereas war introduced threats that are unpredictable, large-scale, and deliberately destructive: missile strikes, artillery shelling, drone attacks, and the destruction of buildings and critical infrastructure.

Historically, occupational safety (OS) systems in Ukraine were oriented primarily toward internal industrial risks, aiming to prevent workplace accidents and occupational diseases under peacetime conditions.

In parallel, the civil protection (CP) system evolved to address emergencies of natural or technogenic origin, mainly at the state and regional levels. These two systems operated independently, governed by different legislation, administrative structures, and risk-assessment approaches. However, the current military aggression has erased these formerly clear boundaries, demonstrating the critical need for their integration.

Today, the civil protection system—which in peacetime was largely under the responsibility of the Government and the State Emergency Service of Ukraine – has become essential for every enterprise. Issues such as shelters, alerting and evacuation procedures, and employee training on appropriate behavior during air-raid warnings have shifted from theoretical considerations to matters of vital importance that directly affect human life.

Thus, an urgent need has emerged for synergy between two previously autonomous spheres – occupational safety and civil protection. This necessity defines the relevance of the present study. At the same time, in the era of the Fourth Industrial Revolution, the potential of digital technologies in the field of safety cannot be overlooked. Artificial intelligence (AI) tools offer fundamentally new opportunities for developing proactive and adaptive safety management systems, enabling a transition from a reactive model – responding to incidents – to a predictive and preventive one [1].

Literature Review

Issues of occupational safety have been extensively studied by Ukrainian scholars [21, 14, 16] as well as international researchers [26, 18, 6]. The field of civil protection has been explored in works [11, 14, 12] and also in [5, 11, 2]; however, these studies were conducted under peacetime conditions. An analysis of legislative changes and initial practical recommendations introduced during martial law [24] shows that the current response to emerging challenges is largely situational, while comprehensive scientific justification for establishing a unified, integrated system that combines the functions of occupational safety (OS) [22, 15, 16] and civil protection (CP) [23] at the macro level – specifically, at the enterprise level – is lacking.

In particular, there are no adapted methodologies for integrated risk assessment that simultaneously account for industrial, military, psychosocial, and cyber threats [4, 20]. There is also an insufficient number of practical guidelines for creating a psychologically resilient working environment under continuous stress.

At the same time, global research [9] demonstrates the rapid development of the “Safety 4.0” concept, which involves the active use of digital technologies such as the Internet of Things (IoT), big data analytics, virtual reality (VR), and augmented reality (AR). For example, in industrial settings, AI assists in predicting equipment failures, detecting anomalies, and automating routine safety inspections. However, these models typically do not account for the specifics of wartime threats. This gap, along with AI’s capacity to rapidly process large volumes of data, identify hidden patterns, and forecast events, makes it an indispensable tool for developing adaptive and proactive safety systems under dynamic wartime conditions. This substantiates the relevance of the present research.

The purpose of this article is to develop conceptual foundations and practical recommendations for integrating civil protection measures into the occupational safety management system at Ukrainian enterprises under martial law, taking into account the innovative potential of artificial intelligence technologies.

Results and Discussion

Risks to Occupational Safety During Wartime. To understand the scale of emerging challenges, it is necessary to consider official statistics. According to a joint assessment by the Government of Ukraine, the World Bank Group, the European Commission, and the United Nations (RDNA4), as of early 2025 Ukraine requires USD 524 billion for reconstruction [25]. Direct damage to infrastructure has reached USD 176 billion. The greatest losses have occurred in the housing sector (over 2.5 million damaged or destroyed homes), transport (USD 385 billion), and the energy sector (USD 14.6 billion). The Kyiv School of Economics (KSE) reports damage or destruction to more than 236,000 residential buildings as well as thousands of industrial enterprises and critical infrastructure facilities [7]. These constantly growing figures demonstrate the systemic nature of threats that extend far beyond conventional understandings of occupational hazards.

Workers are often exposed to danger not only due to direct destruction but also because of indirect factors: lack of access to shelters, disruptions in electricity and water supply, and associated cascading problems. Numerous cases of worker fatalities at industrial sites, in office buildings, or during outdoor tasks amid missile attacks clearly demonstrate that traditional OS systems – designed solely to address non-war-related accidents – are ineffective under current conditions.

Equally important is the profound impact on workers' mental health. According to the World Health Organization (WHO), nearly half of Ukraine’s population (46%) is experiencing mental health problems as a result of the war [3, 23, 19]. A Gradus Research study shows that 77% of Ukrainians have experienced stress, with its main causes being the war (72%) and financial difficulties (41%) [8]. This directly affects work capacity: 66% of managers and 56% of employees acknowledge that deteriorating mental health reduces productivity, increases inattentiveness, and leads to more errors in the workplace [17].

Psychosocial risks such as acute and chronic stress, burnout, constant anxiety, panic attacks, depression, and post-traumatic stress disorder (PTSD) create indirect but very serious threats to occupational safety. Chronic stress impairs cognitive functions (attention, memory, reaction speed), increases irritability, and can lead to workplace conflicts, absenteeism, and high staff turnover. All these factors directly affect workers’

ability to respond adequately to danger, perform complex tasks, and follow safety regulations, thereby increasing the likelihood of accidents and errors in critical situations. This underscores the importance of incorporating psychological support as an integral component of an integrated OS–CP system.

Given the emergence of these new risks, the traditional classification of hazardous and harmful workplace factors requires substantial expansion to include categories specific to wartime conditions. In addition to conventional risks, direct military-threat factors must now be considered, as detailed in Table 1.

To ensure effective management of these challenges within the Integrated Occupational Safety and Civil Protection System (IOS–CPS), a set of specialized response measures has been developed. These measures are summarized in Table 2.

Table 1 – New risks of wartime. Categories and manifestations

Risk Category	Risk Manifestation	Key Response Measures Within the Integrated OS–CP System
Direct Military Threats	Fatalities or injuries caused by missile strikes, shrapnel, drones; impact of blast waves	Establishment and maintenance of shelters; ensuring quick access to shelters; regular evacuation drills; instructions on behavior during attacks; provision of personal protective equipment
Infrastructure Damage	Collapse of structures; damage to electricity, gas, heating, and water supply networks	Technical audit of buildings; development and implementation of emergency shutdown plans; provision of backup power and water supply systems; monitoring of structural conditions
Chemical and Radiological Risks	Release of hazardous substances due to attacks on industrial facilities, storage sites, or nuclear power plants	Provision of personal protective equipment (respiratory protection, protective suits); evacuation plans for affected areas; monitoring of radiation and contamination levels; training on emergency response procedures
Psychosocial Factors	Acute and chronic stress, PTSD, anxiety, panic attacks, reduced concentration and work performance	Implementation of psychological support programs; stress-resilience training; access to individual counselling; building a supportive corporate culture; training managers in crisis communication
Risks Associated With Enterprise Relocation	Work in unsuitable premises; violation of safety requirements during installation/dismantling; mismatch of equipment to new conditions	Comprehensive safety audit at the new site; establishment of temporary or permanent shelters; adjustment of technological processes; repeated mandatory safety briefings; certification or inspection of relocated equipment

Table 2 – New wartime risks. The response measures within the Integrated Occupational Safety and Civil Protection System (IOS–CPS)

Risk Category	Key Response Measures within the IOS–CPS
Direct military threats	Availability and accessibility of well-equipped shelters; regular evacuation drills and scenario-based training; provision of first-aid kits and flashlights; clear instructions on behavior during air-raid alerts.
Infrastructure destruction	Regular inspection of building conditions; development of emergency shutdown plans for utilities; provision of backup power and water sources; creation of strategic reserves of fuel, water, medical supplies, and essential tools.
Chemical and radiological hazards	Provision of personal protective equipment (gas masks, respirators, chemical protective suits, potassium iodide); development of detailed evacuation plans for contaminated areas; training in decontamination procedures and first aid for chemical or radiological exposure.
Psychosocial factors	Implementation of comprehensive psychological support programs: access to professional counseling, support groups, stress-resilience and self-regulation training; creation of a psychologically safe and supportive work environment.
Relocation-related risks	Full safety audit at the new location before commencing operations; proper arrangement of shelters and workplaces in accordance with OSH and civil protection standards; repeated safety briefings; adaptation and integration programs for personnel.
Cyberthreats	Implementation of comprehensive cybersecurity systems; regular software updates; personnel training in cyber hygiene; development of incident response plans; regular data backups and disaster-recovery strategies.

Main Components of the Integrated Occupational Safety and Civil Protection System (IOS-CPS). For the Integrated Occupational Safety and Civil Protection System to function effectively under wartime conditions, several key components must be implemented.

First, the foundation of such a system must be an updated **safety policy.** This document should not be just another formal regulation but a unified, comprehensive approach that integrates all aspects of occupational safety and civil protection. It must clearly define responsibilities, detailed procedures, and safety standards under martial law. Importantly, this document should not be a static “paper formality” but a living, adaptive mechanism that is regularly reviewed and updated to reflect a changing environment.

A crucial element is also comprehensive risk management. This goes beyond simply adding wartime risks to an existing list. It requires systematic assessment that considers interactions with existing occupational, cyber, and psychosocial hazards. The process includes the development of specific methodologies for identifying, thoroughly analyzing, evaluating, and continuously monitoring risks, based on ongoing surveillance and proactive forecasting of potential threats.

A particularly important step toward ensuring comprehensive safety is employee training and awareness-raising [26, 2]. This includes expanded training programs that cover not only standard occupational safety rules but also basics of first aid, including tactical medicine, rules of conduct during air-raid alerts, psychological self-help and peer-support techniques, and cybersecurity fundamentals. To enhance preparedness, it is essential to conduct regular exercises, simulations, and scenario-based crisis response drills. At the same time, shelter availability and readiness must be ensured (with all necessary supplies: communication tools, water, first-aid kits), along with sufficient alerting equipment (including backup communication channels), backup power sources, water and medical supplies, and required personal protective equipment for various types of threats.

In addition, having a clear, flexible, and continuously updated emergency response plan is critical. This action algorithm must account for the dynamics of wartime events, potential loss of communication or power, and other specific wartime challenges, enabling rapid and effective response to any threats.

Finally, active cooperation with the State Emergency Service of Ukraine (SESU), local military administrations, and other emergency services is essential for system effectiveness. Sharing information on threats, closely coordinating actions, and conducting joint drills significantly improve emergency response efficiency, minimize casualties and economic losses, and help form a unified and resilient safety system at all levels—from national to enterprise scale.

Artificial Intelligence in the Safety System. Artificial intelligence is becoming a powerful tool capable of significantly enhancing the effectiveness of an integrated safety system by enabling prediction, rapid response, and adaptability—capabilities beyond human capacity alone. This is achieved through automation, forecasting, and decision-support functionalities.

Key Directions of AI Implementation. AI can analyze massive amounts of data (Big Data), including open SESU data, air-threat information from the Armed Forces of Ukraine, weather information, IoT sensor data from facilities, transport-movement data, and accumulated shelling data. Using machine-learning algorithms (e.g., neural networks), AI can predict potential missile strikes, artillery shelling, or drone attacks. The models can determine likely trajectories and impact zones for a specific enterprise, considering its geographic location. This enables strengthening protective measures in advance or even performing preventive evacuation.

Based on these data—previous trajectories and current weather conditions—AI may predict with 85% probability that the threat is within a dangerous radius of the enterprise. The system automatically sends enhanced threat notifications to all employees at the facility.

AI can automate alerts based on specific conditions. It may consider the exact location of each employee (using GPS or internal positioning), type of threat (e.g., chemical alert vs. air-raid alert), and individual needs (e.g., support required for people with disabilities). Such systems can integrate with mobile apps, corporate chats, and internal communication networks, reducing "alarm fatigue" by sending only important and personalized notifications.

During a nationwide air-raid alert, the AI system identifies that the threat is concentrated in a neighboring district. It sends "enhanced alert" messages only to employees working near the high-risk zone, while others receive general information. This helps avoid panic and maintain workflow where conditions remain safe.

In crisis situations, traditional pre-planned evacuation routes may fail due to damage, blockages, or crowding. AI systems, using IoT sensor data (such as smoke detectors, occupancy sensors, structural-condition sensors) and video analytics from surveillance cameras, can analyze shelter conditions (occupancy, damage), road obstructions, blockages, and crowd density in real time. This enables providing optimal, dynamically updated evacuation routes to the safest accessible shelters, displayed on interactive maps in employees' mobile apps.

During an air-raid alert following a missile strike in a nearby area, the AI system receives information about partial destruction of one evacuation exit and smoke accumulation in the corridor. It instantly recalculates optimal and safe evacuation paths for each area of the building, updating digital displays and mobile apps with shortest safe routes.

AI-enabled computer vision applied to drones or stationary cameras allows rapid detection of structural damage, fires, hazardous-substance leaks, or collapses following an enemy attack. This greatly accelerates situation assessment, identification of danger zones, and dispatch of emergency responders to where they are most needed.

After an explosion at the enterprise, reconnaissance drones automatically deploy. The AI system processes incoming video data, identifies fire zones, structural destruction, potential hazardous-material leaks, and generates a detailed damage map, forwarding it to emergency responders and management.

AI can process data from all subsystems (monitoring, analytics, alerting) and provide integrated analytics, forecasts, and recommendations to management, enabling rapid and effective decision-making during crisis situations. This may include prioritizing rescue operations, optimal distribution of

available resources, coordination of personnel actions, and effective communication with emergency services.

In conditions of limited resources requiring rapid decisions, an AI-based decision-support system analyzes information on the number of injured persons across the facility, availability of medical staff and transport. The system proposes an optimal order of casualty evacuation based on injury severity and route safety.

During wartime, mental health is critically important. AI-based chatbots developed using cognitive-behavioral therapy (CBT) principles and natural-language processing (NLP) technologies can provide anonymous psychological support. They can offer stress-reduction exercises, self-regulation techniques, and direct employees to qualified psychologists if severe problems are detected. This ensures 24/7 access to assistance and reduces stigma associated with seeking mental-health support.

If an employee feels severe anxiety after a shelling episode, they can anonymously contact the corporate AI assistant. The chatbot provides breathing exercises, grounding techniques, and—after evaluating stress level—recommends contacting the staff psychologist, providing contact details.

When implementing AI systems in safety management, it is important to consider ethical challenges: ensuring employee data privacy (especially during psychological monitoring), transparency of decision-making algorithms (to avoid bias), and accountability for potential AI errors in critical situations. Moreover, AI systems require large volumes of high-quality data for effective operation, they are vulnerable to cyberattacks, and their recommendations must always be verified and validated by humans, since humans remain the key element in the process of making final decisions. It is also important to remember the energy dependence of such systems, which becomes a significant issue during frequent power outages.

Practical Recommendations for Implementing the Integrated Occupational Safety and Civil Protection System (IOSCPS) with AI Elements.

Implementing an integrated occupational safety and civil protection system with AI elements requires a systematic approach that takes into account the specifics of each enterprise and the current regional situation. Here are key practical recommendations for enterprise managers:

Conduct a detailed risk assessment of all hazards (ordinary industrial, wartime, psychosocial, cyber) and evaluate the current state of OSH and civil protection systems at the enterprise. This includes assessing the facility's vulnerability to various threats, analyzing existing response plans, surveying employees regarding their readiness and mental state, and thoroughly inspecting the availability, condition, and accessibility of shelters, evacuation routes, and alert systems.

Develop a phased AI implementation plan. Start with pilot projects (for example, implementing smart alerts or a shelter monitoring system at a single facility) to evaluate effectiveness, adaptability, and scalability. Identify the necessary resources (funding, personnel, technology) and establish realistic timelines for each phase.

Review and consolidate safety policies, OSH and civil protection regulations, and instructions. Incorporate new risks, clear procedures for responding to wartime threats, AI tool usage algorithms, and a description of personnel responsibilities at all levels. Documentation should be accessible, clear, and regularly updated.

Develop and implement comprehensive training programs covering both physical safety (first aid, use of protective equipment, actions during air alarms, evacuation) and psychological resilience and digital literacy. Regular drills, crisis simulations, and the involvement of external experts (psychologists, tactical medicine specialists, cybersecurity professionals) are crucial.

Engage highly qualified specialists for the development, implementation, integration, and maintenance of complex AI systems. Collaboration with specialized IT companies, research institutions, and cybersecurity experts will enable the use of best practices and provide technical support while adapting solutions to the enterprise's specific needs.

Explore opportunities for grants, donor, and technical assistance from international organizations to finance digital transformation projects in safety. Investigate cost compensation programs or preferential loans for enterprises investing in safety improvements during wartime. Investments in safety should be seen not as mere expenses, but as strategic contributions to preserving human capital, ensuring business continuity, and increasing enterprise resilience under war conditions, which, in the long term, reduces financial and reputational risks.

Actively cooperate with government bodies, NGOs, and associations to adapt legislation to new realities. This includes regulating the use of AI in occupational safety and civil protection, defining responsibilities, and establishing standards.

Conclusions

1. The war in Ukraine has acted as a catalyst for a fundamental reassessment of approaches to human safety in the workplace. Analysis has shown that the separate existence of occupational safety and civil protection systems is ineffective in the face of modern military threats. Therefore, it is necessary to deeply integrate them into a unified, human-centered system that accounts for both the physical and psychological safety of personnel.

2. The scientific novelty of this work lies in the justification and development of a conceptual model of an Integrated Occupational Safety and Civil Protection System (IOSCPS) enhanced with artificial intelligence tools. This enables a new, digitally oriented approach to safety management, based on the principles of prediction, adaptability, and automation. AI integration allows not only the collection of data but also its

transformation into valuable forecasts and automated actions. This creates a system that autonomously adapts to dynamic and unpredictable wartime threats, representing a significant advance compared to traditional reactive measures.

3. The practical value of this work is that the proposed recommendations serve as a foundation for developing specific safety standards for various industries during wartime and provide managers with a clear "roadmap" for the phased implementation of AI technologies. These recommendations are flexible and can be adapted for enterprises of different sizes and sectors, enabling enhanced personnel protection and ensuring the continuity of production processes even under resource constraints.

Future research prospects include the development of specific mathematical models and software algorithms for predictive threat analysis (considering the characteristics of different types of weapons and their impacts), studying human–AI interaction in crisis situations (for example, optimizing interfaces for rapid decision-making by AI system operators), analyzing the economic efficiency of investments in AI safety systems in terms of preserving human capital and reducing indirect wartime losses, and developing ethical and legal standards for AI use in the context of occupational safety and civil protection during armed conflicts.

References

1. Ahmad, A., & Kumar, S. (2023). Artificial intelligence in disaster management: A systematic literature review. *International Journal of Disaster Risk Reduction, 95,* 103569. https://doi.org/10.1016/j.ijdrr.2023.103569
2. Alexander, D. E. (2003). Towards the development of a standard in emergency management training and education. *Disaster Prevention and Management, 12*(2), 113–123. https://doi.org/10.1108/09653560310474223
3. An, J., Kang, E., Choi, Y. J., Lim, H., Lee, H., & Park, E. (2025). Association of exposure to missile and bomb attacks with mental health symptoms among Ukrainian adults during the 2022 Russian invasion. *JAMA Network Open, 8*(6), e2830228. https://doi.org/10.1001/jamanetworkopen.2025.30228
4. British Standards Institution. (2008). *Occupational health and safety management systems: Guidelines for the implementation of OHSAS 18001:2007 (BS OHSAS 18001:2008).*
5. Coppola, D. P. (2015). *Introduction to international disaster management* (3rd ed.). Butterworth-Heinemann.
6. Fernández-Muñiz, B., Montes-Peón, J. M., & Vázquez-Ordás, C. J. (2007). Safety management system: Development and validation of a multidimensional scale. *Journal of Loss Prevention in the Process Industries, 20*(1), 52–68. https://doi.org/10.1016/j.jlp.2006.10.002
7. GMK Center. (2025). Прямі збитки інфраструктури України від війни сягнули $170 млрд – KSE. https://gmk.center/ua/news/pryami-zbitki-infrastrukturi-ukraini-vid-vijni-syagnuli-170-mlrd-kse/
8. Gradus Research. (2024). Психічне здоров'я та ставлення українців до психологічної допомоги. https://gradus.app/uk/open-reports/mental-health-and-attitudes-ukrainians-towards-psychological-assistance-during-war/
9. Hale, A., & Guldenmund, F. (2022). Safety 4.0: The role of new digital technologies in occupational safety. *Safety Science, 150,* 105697. https://doi.org/10.1016/j.ssci.2021.105697
10. Kapucu, N., & Liou, K. T. (Eds.). (2014). *Disaster and emergency management systems.* Routledge.
11. Королькова, О. (2024). Як організувати цивільний захист на підприємстві. *Охорона праці*, (5), 123–133. https://ohoronapraci.kiev.ua/article/news/ak-organizuvati-civilnij-zahist-na-pidpriemstvi-persi-kroki
12. Курепін, В. М. (2017). *Охорона праці в галузі та цивільний захист: навчальний посібник.* МНАУ. https://dspace.mnau.edu.ua/jspui/bitstream/123456789/2405/1/Okhorona_pratsi_v_%20haluzi_ta%20tsyvil%27nyy_zakhyst.pdf

1. Ahmad, A., & Kumar, S. (2023). Artificial intelligence in disaster management: A systematic literature review. *International Journal of Disaster Risk Reduction, 95,* 103569. https://doi.org/10.1016/j.ijdrr.2023.103569
2. Alexander, D. E. (2003). Towards the development of a standard in emergency management training and education. *Disaster Prevention and Management, 12*(2), 113–123. https://doi.org/10.1108/09653560310474223
3. An, J., Kang, E., Choi, Y. J., Lim, H., Lee, H., & Park, E. (2025). Association of exposure to missile and bomb attacks with mental health symptoms among Ukrainian adults during the 2022 Russian invasion. *JAMA Network Open, 8*(6), e2830228. https://doi.org/10.1001/jamanetworkopen.2025.30228
4. British Standards Institution. (2008). *Occupational health and safety management systems: Guidelines for the implementation of OHSAS 18001:2007 (BS OHSAS 18001:2008).*
5. Coppola, D. P. (2015). *Introduction to international disaster management* (3rd ed.). Butterworth-Heinemann.
6. Fernández-Muñiz, B., Montes-Peón, J. M., & Vázquez-Ordás, C. J. (2007). Safety management system: Development and validation of a multidimensional scale. *Journal of Loss Prevention in the Process Industries, 20*(1), 52–68. https://doi.org/10.1016/j.jlp.2006.10.002

7. GMK Center. (2025). Direct damage to Ukraine's infrastructure from the war reached $170 billion – KSE. https://gmk.center/ua/news/pryami-zbitki-infrastrukturi-ukraini-vid-vijni-syagnuli-170-mlrd-kse/
8. Gradus Research. (2024). Mental health and Ukrainians' attitudes towards psychological assistance. https://gradus.app/uk/open-reports/mental-health-and-attitudes-ukrainians-towards-psychological-assistance-during-war/

9. Hale, A., & Guldenmund, F. (2022). Safety 4.0: The role of new digital technologies in occupational safety. *Safety Science, 150,* 105697. https://doi.org/10.1016/j.ssci.2021.105697
10. Kapucu, N., & Liou, K. T. (Eds.). (2014). *Disaster and emergency management systems.* Routledge.

11. Korolkova, O. (2024). How to organize civil defense at an enterprise. *Ohorona Pratsi, (5),* 123–133. https://ohoronapraci.kiev.ua/article/news/ak-organizuvati-civilnij-zahist-na-pidpriemstvi-persi-kroki
12. Kurepin, V. M. (2017). *Labor protection in the industry and civil defense: A textbook.* MNAU. https://dspace.mnau.edu.ua/jspui/bitstream/123456789/2405/1/Okhorona_pratsi_v_%20haluzi_ta%20tsyvil%27nyy_zakhyst.pdf

13. Kurapov, A., Reznik, A., Bazarova, E., Isralowitz, R., & Cherkasova, E. (2023). Mental health of people living in Ukraine after Russia's invasion: The role of social support, religiosity, and place of residence. *Frontiers in Psychology, 14,* 1226184. https://doi.org/10.3389/fpsyg.2023.1226184
14. Левченко, О. Г., Бахрушин, В. Є., & Соколов, М. М. (2019). *Охорона праці та цивільний захист: підручник*. КПІ ім. І. Сікорського. https://ela.kpi.ua/bitstream/123456789/26895/1/OP_ta_TsZ_pidruchnyk.pdf
15. OHSAS Project Group. (2007). *Occupational health and safety management systems: Requirements (OHSAS 18001:2007).*
16. Радецький, І. І., Горобинський, С. В., Костанян, В. Р., та ін. (2012). Удосконалення системи управління безпеки виробництва підприємств нафтогазового комплексу. *Нафтова і газова промисловість*, (6), 16–20.
17. Robota.ua. (2025). Робота під тиском війни: важливі інсайти з дослідження психічного здоров'я працівників в Україні. Budni. https://budni.robota.ua/hr/robota-pid-tiskom-viyni-vazhlivi-insayti-z-doslidzhennya-psihichnogo-zdorov_ya-pratsivnikiv-v-u
18. Robson, L. S., Clarke, J. A., Cullen, K., Bielecky, A., Severin, C., Bigelow, P. L., Irvin, E., Culyer, A., & Mahood, Q. (2007). The effectiveness of occupational health and safety management system interventions: A systematic review. *Safety Science, 45*(3), 329–353. https://doi.org/10.1016/j.ssci.2006.07.003
19. Seleznova, V., Pertsovska, V., Semigina, T., & Roberts, B. (2023). Mental health system reform in Ukraine in times of war: Challenges and opportunities. *International Journal of Mental Health Systems, 17*(1), 47. https://doi.org/10.1186/s13033-023-00598-3
20. Державний стандарт України. (1993). *Безпечність промислових підприємств. Терміни та визначення (ДСТУ 2156-93).*
21. Ткачук, К. Н., & Васійчук, В. О. (2021). Управління ризиками в системі охорони праці на підприємстві. *Вісник Хмельницького національного університету*, (4), 115–121.
22. Верховна Рада України. (1992). *Про охорону праці* (Закон України №2694-XII). https://zakon.rada.gov.ua/laws/show/2694-12
23. Верховна Рада України. (2012). *Кодекс цивільного захисту України* (Закон України №5403-VI). https://zakon.rada.gov.ua/laws/show/5403-17
24. Верховна Рада України. (2022). *Про організацію трудових відносин в умовах воєнного стану* (Закон України № 2136-IX). https://zakon.rada.gov.ua/laws/show/2136-20
25. European Union, United Nations, Government of Ukraine, & World Bank. (2025). Ukraine – Fourth Rapid Damage and Needs Assessment (RDNA4): February 2022 – December 2024. World Bank Group. https://documents.worldbank.org/curated/en/099022025114040022
26. Zwetsloot, G. I. J. M., Kines, P., Ruotsala, R., Drupsteen, L., Merivirta, M.-L., & Bezemer, R. A. (2017). The importance of commitment, communication, culture and learning for the implementation of OHS management systems. *Safety Science, 96,* 197–212. https://doi.org/10.1016/j.ssci.2017.03.017

13. Kurapov, A., Reznik, A., Bazarova, E., Isralowitz, R., & Cherkasova, E. (2023). Mental health of people living in Ukraine after Russia's invasion: The role of social support, religiosity, and place of residence. *Frontiers in Psychology, 14,* 1226184. https://doi.org/10.3389/fpsyg.2023.1226184
14. Levchenko, O. H., Bakhrushyn, V. Ye., & Sokolov, M. M. (2019). *Labor protection and civil defense: A textbook.* KPI named after I. Sikorskyi. https://ela.kpi.ua/bitstream/123456789/26895/1/OP_ta_TsZ_pidruchnyk.pdf
15. OHSAS Project Group. (2007). *Occupational health and safety management systems: Requirements (OHSAS 18001:2007).*
16. Radetskyi, I. I., Horobynskyi, S. V., Kostanian, V. R., et al. (2012). Improving the safety management system of oil and gas complex enterprises. *Naftova i Hazova Promyslovist, (6),* 16–20.
17. Robota.ua. (2025). Working under the pressure of war: Important insights from a study of employees' mental health in Ukraine. *Budni.* https://budni.robota.ua/hr/robota-pid-tiskom-viyni-vazhlivi-insayti-z-doslidzhennya-psihichnogo-zdorov_ya-pratsivnikiv-v-u
18. Robson, L. S., Clarke, J. A., Cullen, K., Bielecky, A., Severin, C., Bigelow, P. L., Irvin, E., Culyer, A., & Mahood, Q. (2007). The effectiveness of occupational health and safety management system interventions: A systematic review. *Safety Science, 45*(3), 329–353. https://doi.org/10.1016/j.ssci.2006.07.003
19. Seleznova, V., Pertsovska, V., Semigina, T., & Roberts, B. (2023). Mental health system reform in Ukraine in times of war: Challenges and opportunities. *International Journal of Mental Health Systems, 17*(1), 47. https://doi.org/10.1186/s13033-023-00598-3
20. State Standard of Ukraine. (1993). *Safety of industrial enterprises. Terms and definitions (DSTU 2156-93).*
21. Tkachuk, K. N., & Vasiichuk, V. O. (2021). Risk management in the occupational safety system at the enterprise. *Visnyk Khmelnytskyi National University, (4),* 115–121.
22. Ukrainian Parliament. (1992). *On labor protection (Law of Ukraine No. 2694-XII).* https://zakon.rada.gov.ua/laws/show/2694-12
23. Ukrainian Parliament. (2012). *Civil Protection Code of Ukraine (Law of Ukraine No. 5403-VI).* https://zakon.rada.gov.ua/laws/show/5403-17
24. Ukrainian Parliament. (2022). *On the organization of labor relations under martial law (Law of Ukraine No. 2136-IX).* https://zakon.rada.gov.ua/laws/show/2136-20

25. European Union, United Nations, Government of Ukraine, & World Bank. (2025). Ukraine – Fourth Rapid Damage and Needs Assessment (RDNA4): February 2022 – December 2024. World Bank Group. https://documents.worldbank.org/curated/en/099022025114040022
26. Zwetsloot, G. I. J. M., Kines, P., Ruotsala, R., Drupsteen, L., Merivirta, M.-L., & Bezemer, R. A. (2017). The importance of commitment, communication, culture and learning for the implementation of OHS management systems. *Safety Science, 96,* 197–212. https://doi.org/10.1016/j.ssci.2017.03.017

Погребняк В.Г. *
Івано-Франківський національний технічний університет нафти і газу
https://orcid.org/0000-0002-7735-3408

Кондрат О.Р.
Івано-Франківський національний технічний університет нафти і газу
https://orcid.org/0000-0003-4406-3890

Перкун І.В,
Івано-Франківський національний технічний університет нафти і газу
https://orcid.org/0000-0002-6523-1606

Погребняк А.В.
Університет митної справи та фінансів
https://orcid.org/0000-0003-3214-6410

Трансформація підходів до безпеки праці та цивільного захисту: виклики та рішення в період воєнного стану

Аннотація. Стаття присвячена нагальній потребі фундаментального реформування традиційних систем безпеки праці та цивільного захисту в умовах повномасштабної війни. Розглянуті нові, раніше небачені ризики для життя та здоров'я працівників, спричинені воєнними діями. Ці загрози виходять далеко за рамки звичних виробничих небезпек, включаючи прямі ракетні удари, руйнування будівель, кібератаки та серйозний вплив на психіку людей. Доведено, що старі підходи до безпеки праці, які зосереджувалися на запобіганні нещасним випадкам у мирний час, абсолютно не справляються з динамічними, непередбачуваними та агресивними воєнними загрозами. Обґрунтовано, чому необхідно терміново інтегрувати заходи цивільного захисту в систему управління безпекою праці, перетворивши дві окремі системи на єдину, цілісну модель безпеки, орієнтовану на людину, на рівні кожного підприємства. Особливу увагу приділено тому, як цифрові технології, зокрема штучний інтелект, можуть допомогти в цьому. Показано, як штучний інтелект може прогнозувати загрози на основі аналізу великих обсягів даних, автоматизувати системи оповіщення, оптимізувати шляхи евакуації в режимі реального часу, автоматично оцінювати пошкодження та допомагати приймати рішення в кризових ситуаціях, а також надавати психологічну підтримку персоналу. Запропоновано концептуальну модель такої інтегрованої системи безпеки працуі та цивільного захисту, посиленої інструментами штучного інтелекту. Це дозволяє перейти від простої реакції на події до проактивного, превентивного управління безпекою. На завершення сформульовано практичні та масштабовані рекомендації для керівників підприємств, які допоможуть їм поетапно впроваджувати технологічні інновації у процеси безпеки, щоб підвищити стійкість і захищеність персоналу в умовах війни, навіть маючи обмежені ресурси.

Ключові слова: безпека праці, цивільний захист, воєнний стан, штучний інтелект, предиктивна аналітика, інтегрована система, психосоціальні ризики.

*Адреса для листування E-mail: VGPogrebnyak@gmail.com

Надіслано до редакції:	17.04.2025	Прийнято до друку після рецензування:	05.05.2025	Опубліковано (оприлюднено):	26.06.2025

Suggested Citation:	
APA style	Pogrebnyak, V., Kondrat, O., Perkun, I., & Pogrebnyak, A. (2025). Transforming Occupational Safety and Civil Defense: Wartime Challenges and Solutions. *Academic Journal Industrial Machine Building Civil Engineering*, *1* (64), 14–21. https://doi.org/10.26906/znp.2025.64.4034
DSTU style	Transforming Occupational Safety and Civil Defense: Wartime Challenges and Solutions / V. Pogrebnyak et al. *Academic journal. Industrial Machine Building, Civil Engineering*. 2025. Vol. 64, iss. 1. P. 14–21. URL: https://doi.org/10.26906/znp.2025.64.4034.