

Preface: Fifth International Workshop on Cyber Hygiene

Sergiy Gnatyuk^{1,†}, Maksim Iavich^{2,†}, Roman Odarchenko^{1,†}, Marek Aleksander^{3,†} and Maksym Zaliskyi^{1,*,†}

¹National University "Kyiv Aviation Institute", Liubomyra Huzara Ave., 1, Kyiv, 03058, Ukraine

²Caucasus University, Paata Saakadze Str., 1, Tbilisi, 0102, Georgia

³Nowy Sacz School of Business - National Louis University, Grunwaldzka Str., 17, Nowy Sacz, 33-300, Poland

Abstract

This document is the preface of the Fifth International Workshop on Cyber Hygiene (WCH'26), June 25–26, 2026, held at the University of the National Education Commission, Krakow, Poland.

Keywords

computer science, cyber hygiene, cyber security, artificial intelligence, machine learning, Zero Trust, data processing, secure data transmission, quantum algorithms

1. Introduction

The Fifth International Workshop on Cyber Hygiene (WCH'26) took place on June 25–26, 2026, at the University of the National Education Commission (Krakow, Poland). This Workshop was part of Fifth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks 2026.

The WCH'26 brought together scientists, researchers, experts, and practitioners whose activities are related to the protection of modern information and communication systems, networks, and digital infrastructure. Significant attention during the event was paid not only to the technological aspects and features of cyber security, but also to the formation of an appropriate level of cyber hygiene as an important component of the general culture of safe work with digital resources.

Participants considered current approaches to information protection, data confidentiality, and ensuring the stability of critical information and communication systems. Special emphasis was placed on practices of responsible user behavior: recognizing potentially dangerous messages and links, safe use of accounts, protection of personal data, timely software updates, and compliance with basic digital security rules.

A separate thematic area of WCH'26 was devoted to the study of information confrontation, cyber conflicts, and modern forms of cyber warfare. Within the framework of this area, approaches to predicting potential conflict situations, their timely detection and prevention of escalation in the global information environment were considered. An important component of the discussions was the use of intelligent data processing technologies for analyzing information processes, detecting anomalies, and supporting decision-making in complex cyber environments.

The WCH'26 also served as a platform for presenting new scientific results and practical developments, in particular mathematical models, algorithms, methods, and technological solutions. The presented studies were aimed at increasing the reliability, stability, and adaptability of modern information infrastructure, as well as improving approaches to its functioning in case of increasing cyber risks.

WCH'26: Fifth International Workshop on Cyber Hygiene, June 25–26, 2026, Krakow, Poland

*Corresponding author.

†These authors contributed equally.

✉ s.gnatyuk@kai.edu.ua (S. Gnatyuk); miavich@cu.edu.ge (M. Iavich); roman.odarchenko@npp.kai.edu.ua (R. Odarchenko); aleksandermarek4@gmail.com (M. Aleksander); maksym.zaliskyi@npp.kai.edu.ua (M. Zaliskyi)

ORCID 0000-0003-4992-0564 (S. Gnatyuk); 0000-0002-3109-7971 (M. Iavich); 0000-0002-7130-1375 (R. Odarchenko); 0000-0003-2619-1063 (M. Aleksander); 0000-0002-1535-4384 (M. Zaliskyi)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

The WCH'26 was made possible thanks to the joint work and support of a wide range of specialists. The organizers express their sincere gratitude to the members of the program and organizational local committees, participants of the Technical Program Committees, as well as reviewers for their professional competence, responsibility, and significant contribution to the preparation and holding of the event. We hope that participation in WCH'26 has become a source of new scientific ideas, professional experience, and useful results for further research for all participants. We wish scientists, researchers, engineers, and practitioners success in the implementation of their scientific projects and professional tasks.

The main topics of these Workshop included:

- Management of Cyber Incidents, Warfare and Conflicts.
- Cyber Conflicts and Information Warfare.
- Critical Infrastructure and Cyber-Physical Systems.
- AI and Intelligent Cybersecurity.
- Secure Networks and Digital Communications.
- Reliability and Risk Management.
- Quantum Algorithms.
- Zero Trust.

The WCH'26 was in a hybrid format. Most of papers were presented at the University of the National Education Commission in Krakow, Poland. However, participants from places with a high from Ukraine are invited to participate in a virtual format. Participants from Poland, Ukraine, Georgia, Kazakhstan, and Czech Republic joined the conference.

The WCH'26 received 26 submissions in total. All papers were reviewed by two reviewers. Out of these, 20 papers were accepted for this volume, 17 as regular papers and 3 as short papers.

Paper [1] presents an AI agent coordination architecture for automated testing and analysis of cyber threats in distributed DevSecOps environments based on LLM and telemetry. Experimental evaluation in a Kubernetes environment demonstrated an increase in threat detection accuracy of up to 96.8%, reduced orchestration latency, and improved scalability compared to traditional approaches and single-agent systems.

Paper [2] is devoted to the development of a method for automated detection of modified images in large photo datasets based on histogram analysis and simultaneous study of different color spaces. The approach proposed in the study provides effective detection of traces of editing, photomontage, and synthetic content with low computational complexity, which makes it suitable for large-scale analysis of digital images.

Paper [3] considers the study of an asynchronous HTTP event processing pipeline in application-level security systems to reduce delays for legitimate users. The authors proposed a combination of an analytical model and discrete-event modeling to determine the optimal number of parallel processors and buffer size, taking into account peak load and response time requirements.

Paper [4] studies a method for comprehensive assessment of the state of software-controlled quantum networks using a multi-criteria approach to take into account the influence of a set of quantum channel parameters. The proposed method provides network state classification, localization of problem segments, and detection of service quality degradation, creating a basis for intelligent monitoring, routing, and resource management of quantum networks.

Paper [5] considers the features of developing a two-stage anomaly detection system to prevent DDoS attacks in large-scale networks using correlation analysis of network traffic, discrete wavelet transform, and machine learning methods. The proposed approach with K-means clustering allows to increase the speed and accuracy of detecting anomalous activity, reduce the number of false positives, and ensure timely response to threats.

Paper [6] deals with the development of a conceptual approach to the integration of Zero Trust architecture with the Security Operations Center (SOC) to increase the cyber resilience of enterprises. The proposed mathematical model for assessing the level of trust and the algorithm for automated SOC

response allow to reduce the time of processing cyber incidents, limit the spread of threats, and reduce the burden on security analysts.

Paper [7] concentrates on the development of an adaptive post-quantum digital signature scheme based on lattice structures. The proposed approach provides a unified foundation for post-quantum security for IoT, blockchain systems, and long-term data storage, allowing for a significant reduction in signature size and memory footprint while maintaining a 128-bit level of post-quantum stability.

Paper [8] is devoted to the study of a combined cryptographic and steganographic approach to multi-level protection of confidential information during its transmission over open communication channels. The proposed system combines mechanisms for protecting keys and hiding encrypted data in various file types; its software implementation in Python confirms the practical applicability of the approach.

Paper [9] presents deterministic frame attribution and homography-based geometric normalization of UAV vision datasets for explosive hazard detection. The proposed dual-loop architecture reduces perspective distortions and ensures the formation of spatially consistent AI datasets for training neural networks and autonomous monitoring.

Paper [10] provides a thematic literature review of current approaches to microservice architecture reconstruction based on static, dynamic, and combined data sources. The analysis showed that combining different sources of evidence increases the completeness of the reconstruction, while key unresolved issues remain technology stack dependency, incomplete implementation coverage, ambiguous component mapping, and the lack of a universal intermediate architecture representation.

Paper [11] considers the development of a method for protecting UAV command link channels, which combines resistance to radio electronic suppression and spoofing based on pseudo-random tuning of the carrier frequency. A mathematical model of the chaotic mode, the structure of the receiving-transmitting path, and an algorithm for synchronizing the chaotic frequency sequence with the command signal in the fast frequency tuning mode are proposed, and a comparison with classical systems is also made.

Paper [12] is devoted to the development of a multilevel attributed cyberspace model for cyber threat intelligence in information and communication systems. The proposed model supports the analysis of the spread of cyber threats, the integration of cyber intelligence data, and the audit of infrastructure state changes, which creates the basis for more effective response to the incident in complex environments.

Paper [13] considers the systematic review of quantum algorithms for solving linear algebra problems, taking into account their potential to provide computational advantages over classical methods. A multi-criteria evaluation of the considered algorithms is carried out, which allows comparing them by a set of characteristics and identifying the most promising approaches for practical application.

Paper [14] presents review of cybersecurity and recommended practices for energy sector. Particular attention is paid to the protection of industrial automation and control systems from targeted cyber threats and increasing the cyber resilience of Ukraine's energy systems in accordance with international standards.

Paper [15] concentrates on the experimental validation of the method for enhancing the security of critical information systems. The proposed approach allows for a comprehensive assessment of the state of security, identification of vulnerable components, and selection of optimal organizational and technical measures with limited resources, which has been confirmed by experimental application in critical transport systems.

Paper [16] is devoted to the development of the attention-based CNN-LSTM architecture for smart-phone human activity recognition in intelligent mobile monitoring systems. Experimental evaluation showed an accuracy of 99.76% , and the use of the attention mechanism reduced the number of misclassified samples by 28% compared to the base CNN model.

Paper [17] concentrates on the development of approaches to monitoring and classifying the technical condition of radio equipment in conditions of changepoints. A combination of statistical methods, IoT, artificial intelligence, and data repositories is proposed to reduce uncertainty about the condition of equipment and increase the efficiency of its operation and maintenance.

Paper [18] considers the development of RFID-based access control system with automated employee attendance tracking. Experimental results confirmed the effectiveness of the proposed solution in

increasing the accuracy of attendance accounting, reliability of access control and automation of administrative processes.

Paper [19] presents the analysis of a cyber hygiene readiness model for network digital twins in telecommunication infrastructure. The proposed model encompasses eight dimensions of cyber hygiene and four maturity levels, consistent with known recommendations, providing a structured approach to assessing network digital twins readiness for safe operational use.

Paper [20] concentrates on real-time Bluetooth Low Energy vulnerability detection using TinyML on edge devices. The proposed neural network model demonstrated 99.68% accuracy during testing and 97.98% in the field validation, with a size of only 4.62 KB and an inference latency of 0.9 ms, providing a significant increase in computational efficiency compared to existing solutions.

All our team invites you to visit the CMiGIN'26 workshop website <https://cyberconf.kai.edu.ua/CH/CH5/> where you can find all the relevant information about this event.

The materials of previous WCH workshops were published in CEUR Workshop Proceedings:

- Volume 4024, URL: <https://ceur-ws.org/Vol-4024/>
- Volume 3925, URL: <https://ceur-ws.org/Vol-3925/>
- Volume 2654, URL: <https://ceur-ws.org/Vol-2654/>

2. Acknowledgments

The WCH'26 would not been possible without the support of the University of the National Education Commission, Poland (www.uken.krakow.pl/en/), National University "Kyiv Aviation Institute", Ukraine (www.nau.edu.ua), Tomas Bata University in Zlin, Czech Republic (www.utb.cz/en/), and CEUR Workshop Proceedings team (ceur-ws.org). Organizers and all participants of the Fifth International Workshop on Cyber Hygiene express a lot of thanks.

Program Committee

- Roman Jasek, Tomas Bata University in Zlin, Czech Republic
- Bronislav Chramcov, Tomas Bata University in Zlin, Czech Republic
- Jugoslav Achkoski, Military Academy, North Macedonia
- Audrius Lopata, Kaunas University of Technology, Lithuania
- Rui Luis Aguiar, University of Aveiro, Portugal
- Rat Berdibayev, Almaty University of Power Engineering and Telecommunications, Kazakhstan
- Haruna Chiroma, University of Hafr Al Batin, Saudi Arabia
- Thierry Oscar Edoh, University of Bonn, Technical University of Munich, Germany
- Emil Faure, Cherkasy State Technological University, Ukraine
- Solomia Fedushko, Lviv Polytechnic National University, Ukraine
- Natalia Shakhovska, Lviv Polytechnic National University, Ukraine
- Tetiana Okhrimenko, Scientific Cyber Security Association of Ukraine, Ukraine
- Valentín Cardeñoso Payo, University of Valladolid, Spain
- Jamil Al-Azzeh, Al Balqa Applied University, Jordan
- Vishnu Narayan Mishra, Indira Gandhi National Tribal University, India
- Zhengbing Hu, University of Bonn, Central China Normal University, China

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

- [1] E. Faure, I. Rozlomii, A. Kovalova, B. Savchuk, S. Naumenko, Architecture of AI-agent orchestration for automated testing and cyber threat analysis in DevSecOps environments, in: CEUR Workshop Proceedings, 2026, pp. 7–20.
- [2] A. Dudnik, D. Zhuravlov, A. Fesenko, V. Mykolaichuk, V. Cernej, V. Datsko, M. Ivasiv, A method for detecting manipulated images in large-scale photo datasets based on histogram analytics and multi-color space analysis, in: CEUR Workshop Proceedings, 2026, pp. 21–35.
- [3] A. Chizhov, A. Fesenko, A. Gajewska, V. Chizhov, Analytical-simulation modeling of a finite queue for asynchronous HTTP request analysis, in: CEUR Workshop Proceedings, 2026, pp. 36–47.
- [4] M. Aleksander, Y. Kulakov, A. Devociogullari, O. Zhurakovska, O. Havrylenko, D. Sytnyk, A method for software-defined quantum network state assessment and detection of anomalous or degraded communication channels, in: CEUR Workshop Proceedings, 2026, pp. 48–66.
- [5] B. Kotyk, D. Bakhtiarov, O. Lavrynenko, A. Leleko, D. Kocherga, Y. Tertus, DDoS attack detection in large-scale networks using wavelet transform and machine learning, in: CEUR Workshop Proceedings, 2026, pp. 67–78.
- [6] Z. Poberezhna, Conceptual approach to the interaction of zero trust and SOC in cybersecurity system of enterprises, in: CEUR Workshop Proceedings, 2026, pp. 79–88.
- [7] M. Iavich, Quantum-adaptive lattice signatures for next-generation secure communications, in: CEUR Workshop Proceedings, 2026, pp. 89–101.
- [8] D. Odnoochko, A. Ilyenko, S. Ilyenko, O. Smirnov, H. Hulak, Marker-based crypto-steganographic system for secure data transmission over open channels, in: CEUR Workshop Proceedings, 2026, pp. 102–117.
- [9] A. Dudnik, S. Vyhovskyy, O. Batrak, O. Toroshanko, V. Mykolaichuk, D. Reznik, P. Tkachuk, Deterministic frame attribution and homography-based geometric normalization of UAV vision datasets for explosive hazard detection using dual-loop architecture, in: CEUR Workshop Proceedings, 2026, pp. 118–130.
- [10] O. Grinenko, A. Gizun, A. Morhun, A. Bekh, Methods for reconstructing microservice architectures: A thematic literature review, in: CEUR Workshop Proceedings, 2026, pp. 131–146.
- [11] S. Zhyla, K. Muzychenko, V. Yerokhin, A method for protecting UAV command link transmission using pseudo-random frequency hopping based on a parametric oscillator, in: CEUR Workshop Proceedings, 2026, pp. 147–157.
- [12] A. Pinchuk, R. Odarchenko, O. Polihenko, A. Imanbayev, R. Berdibayev, A multilevel attributed cyberspace model for cyber threat intelligence in ICT systems, in: CEUR Workshop Proceedings, 2026, pp. 158–168.
- [13] A. Ibraimova, T. Shmahlii, G. Litawa, T. Okhrimenko, Systematic review on quantum algorithms for solving tasks of linear algebra and statistics, in: CEUR Workshop Proceedings, 2026, pp. 169–199.
- [14] H. Noga, V. Lukashenko, P. Varacha, O. Dobrynychuk, Review of cybersecurity and recommended practices for energy sector, in: CEUR Workshop Proceedings, 2026, pp. 200–215.
- [15] V. Sydorenko, A. Polozhentsev, K. Kluczevska-Chmielarz, S. Sydorenko, O. Zhyharevych, Experimental validation of the method for enhancing the security of critical information systems, in: CEUR Workshop Proceedings, 2026, pp. 216–230.
- [16] M. Turdalyuly, N. Baisholan, S. Gnatyuk, A. Zholdassova, A. Yerimbetova, Attention-based CNN-LSTM architecture for smartphone IMU-based human activity recognition in intelligent mobile monitoring systems, in: CEUR Workshop Proceedings, 2026, pp. 231–246.
- [17] O. Solomentsev, M. Zaliskiy, Y. Petrova, A. Osipchuk, A. Plugoviy, S. Halenko, Data processing in operation systems of CNS equipment, in: CEUR Workshop Proceedings, 2026, pp. 247–259.
- [18] L. Berkman, S. Otrokh, M. Prokopchuk, V. Danylchenko, RFID-based access control system with automated employee attendance tracking, in: CEUR Workshop Proceedings, 2026, pp. 260–268.
- [19] L. Petrosian, V. Gnatyuk, R. Jasek, A cyber hygiene readiness model for network digital twins in telecommunication infrastructure, in: CEUR Workshop Proceedings, 2026, pp. 269–277.

- [20] E. Abdullaiev, V. Sokolov, P. Skladannyi, Y. Kostiuk, V. Strelnikov, Real-time Bluetooth Low Energy vulnerability detection using TinyML on edge devices, in: CEUR Workshop Proceedings, 2026, pp. 278–286.