



Workshop on

**Cybersecurity Providing
in Information
and Telecommunication Systems II**

CPITS-II'2025



ISSN 1613-0073

October 26, 2025
Kyiv, Ukraine

Workshop on Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II), ed. V. Sokolov, V. Ustimenko, T. Radivilova, M. Nazarkevych, Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine, Oct. 26, 2025.

The aim of the Cybersecurity Providing in Information and Telecommunication Systems (CPITS) workshop is to provide a forum for researchers to discuss current trends in cybersecurity and risk management, critical infrastructure security, wireless and sensor network privacy, IoT and IoMT security, routing techniques for cybersecurity, cybersecurity data science, artificial intelligence, machine learning in cybersecurity, deepfake attacks and cryptography. In CPITS, we encourage the submission of papers in the field of cybersecurity. Novel applications of these methods to real-world problems are welcome.

There were 63 papers submitted for peer review to this workshop. Out of these, 26 papers were accepted for this volume, 23 as regular papers and 3 as short papers.

Borys Grinchenko Kyiv Metropolitan University
18/2 Bulvarno-Kudriavska str.
04053 Kyiv, Ukraine

ISSN: 1613-0073

Creative Commons License Attribution 4.0 International (CC BY 4.0)
© 2025 Cybersecurity Providing in Information and Telecommunication Systems

Editors

Volodymyr Sokolov

PhD, Assoc. Prof., Borys Grinchenko Kyiv Metropolitan University, Ukraine

Vasyl Ustimenko

DSc, Prof., Royal Holloway, University of London, United Kingdom

Tamara Radivilova

DSc, Prof., Kharkiv National University of Radio Electronics, Ukraine

Mariya Nazarkevych

DSc, Prof., Lviv Polytechnic National University, Ukraine

Table of Content

Regular Papers

1	Spatial grasp technology and its application for management of distributed systems <i>Peter Sapaty, Anatolii Morozov, Vitalii Klymenko, Nikolay Ievlev</i>	1–19
2	Intelligence versus threats: The role of AI agents in ensuring cybersecurity of information and telecommunication systems <i>Nikolay Ievlev, Vitalii Klymenko, Anatolii Morozov, Vitalii Yashchenko, Hennadii Hulak</i>	20–34
3	Software module protecting web applications from several attacks types using formal logic <i>Nataliia Gulak, Sergii Ilyenko, Elena Dubchak, Andrii Maistrenko, Bohdan Zhurakovskiy</i>	35–45
4	Simulation of the availability and initialization speed of a layer 2 mesh network <i>Oleksii Dzhus, Mykhaylo Lobur</i>	46–57
5	Methodology for assessing computer security levels <i>Volodymyr Akhramovych, Vadym Akhramovych, Anna Ilyenko, Olha Kryvokulska, Viktoriia Zhebka</i>	58–71
6	Machine learning methods for detecting intrusions based on network traffic analysis <i>Yuliia Kostiuk, Pavlo Skladannyi, Volodymyr Sokolov, Svitlana Rzaieva, Karyna Khorolska</i>	72–94
7	Intelligent modeling of personalized learning in cybersecurity training <i>Pavlo Skladannyi, Yuliia Kostiuk, Oleksii Zhyltsov, Yuriy Savchenko, Yevhen Antypin</i>	95–119
8	Exponential data augmentation methods for improving YOLO performance in computer vision tasks <i>Yurii Myshkovskiy, Mariia Nazarkevych, Victoria Vysotska, Rostyslav Yurynets</i>	120–132
9	Phase categories as a tool for modeling uncertainty in higher education programs and program learning outcomes <i>Hryhorii Hnatiienko, Oleg Ilarionov, Hanna Krasovska, Larysa Myrutenko, Anzhelika Tkachuk</i>	133–148
10	AdaptiveBayes: Comprehensive empirical analysis and algorithmic enhancement framework <i>Sergii Kavun</i>	149–178
11	Building specific of zero trust architecture in hybrid infrastructures <i>Roman Syrotynskiy, Ivan Tyshyk, Alona Desiatko</i>	179–190

- 12 Layered model for protecting speech information against leakage through an opto-electronic channel 191–201
Nazarii Dzyanyi, Ivan Opirskyy, Mariia Shved, Olha Liubchuk
- 13 Universal security platform for intelligent cyber-physical technology of carbon dioxide monitoring in the regional ecosystem 202–216
Valerii Dudykevych, Halyna Mykytyn, Sviatoslav Borduliak, Yaroslav Fur
- 14 Pragmatic DDoS detection on AWS cloud with lightweight machine learning 217–227
Vitalii Molnar, Dmytro Sabodashko
- 15 A security system with automated person identification based on computer vision technologies 228–245
Bohdan Zhurakovskiy, Viktor Shutenko, Anatoliy Makarenko, Oleksandr Pliushch, Rostyslav Zakharov
- 16 A method of generating data for further training artificial intelligence models aimed at solving cybersecurity problems 246–256
Ivan Chernihivskiy, Larysa Kriuchkova
- 17 Security difficulties and barriers in building decentralized blockchain bridges, solution methods 257–274
Andrii Bondarchuk, Viktoriia Onyshchenko, Andrii Hashko, Andrii Strazhnikov, Nataliia Korshun
- 18 Privacy-preserving security operations: Bridging the conformance gap between SOC efficiency and GDPR compliance 274–283
Maksim Iavich, Giorgi Iashvili
- 19 Security methods in .NET technology 284–294
Serhii Buchyk, Serhii Toliupa, Oleksandr Buchyk, Anastasiia Shabanova
- 20 Research on a new hybrid random number sequence generator 295–305
Serhii Yanushevskiy, Heorhii Prokhorov, Oleksandr Hres, Yurii Yaremchuk, Volodymyr Lytvynenko
- 21 Model of an intelligent decision support system to ensure cyber resilience of military information systems 306–315
Olena Nehodenko, Svitlana Shevchenko, Vitalii Nehodenko, Yuliia Zhdanova
- 22 Technological process management for cloud-based critical infrastructure under emerging threats and challenges 316–328
Tetiana Smirnova, Oleksandr Dobrynychuk
- 23 Formation of a conceptual model for cyber-physical monitoring of critical infrastructure environmental objects 329–340
Vadym Chytulian, Andrii Kolodiuk, Ivan Oleinikov, Viktoriia Zhebka, Valeriia Balatska

Short Papers

- | | | |
|---|---|---------|
| 1 | Ontology-based model for security management in IoT systems
<i>Oleksiy Kovalenko, Natalia Karevina</i> | 341–347 |
| 2 | Scalability analysis of neural network architectures for voice biometric authentication
<i>Khrystyna Ruda, Dmytro Sabodashko, Ihor Kos, Ivan Opirskyy, Alina Akhmedova</i> | 348–356 |
| 3 | On the stream ciphers based on the hidden algebraic graphs
<i>Vasyl Ustimenko, Oleksandr Pustovit, Tymofii Svyrydenko</i> | 357–364 |