



Workshop on

**Cybersecurity Providing
in Information
and Telecommunication Systems**

CPITS'2026



ISSN 1613-0073

February 28, 2026
Kyiv, Ukraine

Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS), ed. V. Sokolov, V. Ustimenko, T. Radivilova, M. Nazarkevych, Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine, Feb. 28, 2026.

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 71 papers submitted for peer review to this workshop. Out of these, 24 papers were accepted for this volume, 20 as regular papers and 4 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)
© 2026 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

Mariia Nazarkevych

DSc, Prof., Lviv Polytechnic National University, Ukraine

Table of Content

Regular Papers

1	On quadratic equations of q -regular tree and their applications to symmetric cryptography <i>Vasyl Ustimenko, Oleksandr Pustovit, Tymofii Svyrydenko</i>	1–10
2	Architecture design of ML-based spoofing detection solution <i>Serhii Bulba, Danylo Yefimov, Larysa Kriuchkova, Roman Kyrychok, Sergiy Obushnyi</i>	11–20
3	Verification of video content authenticity and integrity using artificial intelligence <i>Pavlo Skladannyi, Yuliia Kostiuk, Dmytro Hnatchenko, Igor Goncharenko, Artem Platonenko</i>	21–45
4	An integrated AI-supported model for developing digital competence in lifelong learning <i>Svitlana Popereshnyak, Oleg Kulynich</i>	46–64
5	Risk-aware proactive hardening of IoT and cyber-physical networks <i>Tetiana Babenko, Kateryna Kolesnikova, Larysa Myrutenko, Oleksandr Kruchinin</i>	65–79
6	S3 and S4: Novel hybrid activation functions for deep neural networks <i>Sergii Kavun</i>	80–97
7	Computational data-processing methods for sustainable enterprise development under energy- and resource-saving constraints <i>Zarina Poberezhna, Maksym Zaliskyi, Khadija Slimani, Dmytro Shvets, Nataliia Demchenko</i>	98–108
8	Developing students' cognitive resistance to information manipulation through critical thinking: Practical aspects <i>Liudmyla Ilich, Olena Akilina, Svitlana Shevchenko, Yuliia Zhdanova</i>	109–121
9	Well-posedness of boundary-value problems in information security of cyber-physical systems for the bioeconomy <i>Dmytro Levkin, Ruslana Levkina, Yana Kotko, Artur Levkin, Andriy Dudnik</i>	122–135
10	A fuzzy-logic and machine-learning multicriteria model for cybersecurity risk management <i>Yuliia Kostiuk, Pavlo Skladannyi, Dmytro Hnatchenko, Nadiia Dovzhenko, Halyna Kuchakovska</i>	136–162
11	Autonomous intelligent navigation in unknown environments <i>Bohdan Zhurakovskiy, Sergii Otrokh, Anatoliy Makarenko, Oleksandr Pliushch, Serhij Mamchenko</i>	163–186

12	An ISO/IEC 25010-based quality assessment model for distributed ledger technology platforms <i>Serhii Zhebka, Viktoriia Zhebka, Kateryna Nesterenko, Ganna Grynkevych, Oleksii Cherevyk</i>	187–199
13	A method for detecting unauthorized interference in network communications using intelligent traffic analysis <i>Vladyslav Bilous, Dmytro Bodnenko, Oleksandra Lokaziuk, Valerii Kozachok, Zoreslava Brzhevska</i>	200–215
14	A method for implementing security-as-code in relational databases <i>Yaroslava Momryk, Yuriy Yashchuk, Roman Tuchapskyy, Ivan Opirskyy</i>	216–230
15	Artificial intelligence in higher education: Balancing innovation against ethical risk <i>Tamara Mykheieva, Nataliia Zaiets, Oleksii Holubnychyi, Olena Datsun, Mariia Patrul</i>	231–240
16	Connection context verification as a basis for network access control in zero-trust architectures <i>Roman Syrotynskyy, Ivan Tyshyk, Bohdan Zhurakovskiy</i>	241–255
17	Protecting machine-learning datasets with digital watermarking based on modified QR decomposition <i>Oles Hospodarskyy, Natalia Kukharska, Orest Polotai, Oleh Harasymchuk, Ivan Tyshyk</i>	256–277
18	Evaluating speaker verification robustness to neural voice cloning attacks <i>Nazarii Dzhaliuk, Khrystyna Ruda, Dmytro Sabodashko, Volodymyr Khoma</i>	278–289
19	Development of intelligent intrusion detection systems based on intelligent data analysis methods <i>Serhii Toliupa, Serhii Buchyk, Yurii Shcheblanin, Anastasiia Shabanova, Andrii Kulko</i>	290–305
20	Classical machine learning baselines for synthetic speech detection across modern voice cloning systems <i>Khrystyna Ruda, Dmytro Sabodashko, Volodymyr Povoroznyk, Yuriy Khoma</i>	306–317

Short Papers

1	Integrating the compartmentalization method into information protection against OSINT reconnaissance <i>Valeriia Ivkova, Ivan Opirskyy</i>	318–325
2	Language and conflict: verbal aggression and strategies for mitigation and resolution in online discourse <i>Alla Golovnia, Liana Budanova, Yuliia Petrova</i>	326–334

- 3 Accounting for the information threat level in the route-segment cost metric for UAVs in emergency situations 335–343
 Viktor Shevchenko, Yevhen Derevianko, Olena Derhylova, Volodymyr Shevchenko, Yulii Kondratenko
- 4 A software-defined-radio replay attack on Bluetooth Low Energy devices 344–352
 Oleksandr Romaniuk, Volodymyr Sokolov, Andrii Anosov, Hennadii Hulak, Nataliia Korshun