SpacSec 2026

International Conference on Cyber Warfare, Security & Space Computing
St. Petersburg, 26-28 October, 2026

Final Program

Monday, 26 October 2026

09:00 - 10:00	Registration
9:30 - 10:00	Coffee break
10:00 - 10:30	Opening session (Sandeep Joshi, Igor Kotenko, Aleksandr Menschikov, Andrey Ronzhin) (ауд.306)
10:30 - 11:20	Plenary Session 1 - Dr. Sandeep Joshi, Manipal University Jaipur, India From Alert to Action: Reinforcement Learning for Autonomous Cyber Defence of Terrestrial and Space Systems. Session Chair – Igor Kotenko. (ауд.306)
11:30 - 12:20	Plenary Session 2 - Prof. Sergei A. Petrenko, Sirius University of Science and Technology, Russia Method for analyzing the cyber-resilience of self-healing blockchain platforms against quantum attacks. Session Chair – Igor Kotenko. (ауд.306)
12:30 - 13:30	Lunch
13:30 - 16:00	Parallel Sessions 1-3 Session 1: Information security of critical infrastructures and cyber-physical systems. Session Chairs - Andrey Chechulin, Igor Saenko. (ауд.306) 67 — Alexander A. Grusho, Michael Zabezhailo and Victor Piskovski. On some aspects of trust monitoring in autonomous control systems 60 — Mikhail Mitrofanov, Alexander Kurakin and Nikolay Kramskoy. Adaptive Distributed Denial-of-Service Defense Using Behavioral Analysis and Machine Learning 31 — Igor Kotenko, Igor Saenko, Evgenii Mityakov and Anton Loskutov. Evaluation of Cyber Threat Detection Results in Energy Systems Based on Threat Intelligence and Digital Twin

63 — Aleksei Meleshko, Vasily Desnitsky and Igor Kotenko.
Rule-based approach to detect modifications on layers of 3D products

3 — Ilya Livshitz.
Comparison of functional and information security requirements for Critical facilities

58 — Oleg Lauta, Denis Mahov and Nikita Vasilev.
Application of Zero Trust Architecture for Information Security of Large Language Models in Corporate Infrastructure

4 — Ilya Livshitz.
Ensuring operational audit of critical information infrastructure management systems

Session 2: Security of LLMs, multi-agent systems and generative AI.
Session Chairs - Andrei Petrovski, Maria Lapina. (ауд.311)

15 — Elizaveta Lykova and Anatolii Minzov.
Development of Information Security Policies Using Generative Artificial Intelligence (Large Language Models)

5 — Artem Kolbeev, Andrei Petrovski and Igor Kotenko.
Adversarial Benchmarking of Long-Term Memory Security in LLM-Based Multi-Agent Systems

23 — Alexey Nazyvaev and Anatoly Minzov.
Application of Large Language Models to Information Security Risk Assessment via Simulation Modelling

70 — Sergey Serko and Andrei Petrovski.
A Decentralized Semantic Attestation Method for Protecting Multi-Agent LLM Systems from Cascading Adversarial Injections

152 — Sherzodjon Yarmatov, Oleg Sanamyan, Vitalii Lapin, Maria Lapina and Gleb Semenov.
Methods for Detecting Prompt Injection Attacks in LLM Applications

61 — Mikhail Mitrofanov, Alexander Kurakin and Nikolay Kramskoy.
Deterministic Defense Methods Against Probabilistic Attacks: A Study of the Ineffectiveness of Traditional Approaches to Securing Large Language Models

8 — Oleg Sheluhin, Andrey Osin and Konstantin Khalizev.
Trajectory-based cluster neighborhood analysis for detecting rare anomalous events caused by AI agent behavior

Session 3: Data analysis, machine learning and decision support.
Session Chairs - Lev Utkin, Andrei Konstantinov. (ауд.305)

9 — Andrey Sukhanov and Sergey Kovalev.
Image Recognition in Role Learning Systems Based on Fuzzy Kolmogorov-Arnold Networks

52 — Andrei Konstantinov, Lev Utkin and Stanislav Kirpichenko.
Analytic Unary Density Trees for Inspectable Anomaly Scoring

53 — Lev Utkin, Andrei Konstantinov, Stanislav Kogan and Natalya Verbova.
Attention-Based Estimation of Individual Causal Benefit Probabilities under Dose Variation

22 — Andrey Kozachok, Anatoliy Bakaev, Aleksandr Kozachok, Shamil Magomedov and Artem Noev.
Context-Instrumental Data Distillation for Kubernetes Manifest Generation: Method and Experimental Evaluation

	62 — Vladimir Muliukha, Aleksey Vostrov, Dmitrii Motorin, Vadim Glazunov and Mikhail Kurochkin. Solving Applied Problems under Constraints Using Machine Learning Methods 17 — Ilya Mishchenko and Anton Misnik. Adaptive Neural Ensemble for X-Ray Preprocessing in Clinical Decision Support Systems 19 — Alexandra Chudinova. Workload Analysis: Uncertainty and Multi-criteria
16:00 - 16:30	**Coffee break**
16:30 - 18:00	**Round table - New trends in cybersecurity.** **Moderator - Sergey Petrenko. Speakers - Igor Saenko, Eugine Abramov, Alexey Vulfin, Ilya Popov, Aleksandr Menschikov. (ауд.306)**

Tuesday, 27 October 2026

09:00 - 10:00	**Registration**
10:00 - 10:30	**Coffee break**
10:30 - 11:20	**Plenary Session 3 - Prof. Boris Sokolov, St. Petersburg Federal Research Center of the Russian Academy of Sciences, Russia** **Methodology and Technologies for Proactive Management of Space Edge Computing.** **Session Chair – Igor Kotenko. (ауд.306)**
11:30 - 12:20	**Plenary Session 4 - Prof. Sergey V. Bezzateev, ITMO University, Russia** **Multilevel structured approach for digital watermarking: multimedia data protection survey and perspectives.** **Session Chair – Igor Kotenko. (ауд.306)**
12:30 - 13:30	**Lunch**
13:30 - 16:00	**Parallel Sessions 4-6** **Session 4: Detection of anomalies, intrusions and malware.** **Session Chairs - Oleg Sheluhin, Andrey Osin. (ауд.306)** 7 — Dmitriy Rakovskiy and Oleg Sheluhin. Cascade Model of Rare Multi-Label Anomalous Events in a Computer Network 11 — Maxim Gorda and Ksenia Zhernova.

Detecting Anomalies in Network Traffic Data and Its Graphical Representation Using Transformers

20 — Konstantin Chebunin.
System Call Chain Profiling of Containerized Applications for Security Regression Testing in CI/CD Pipelines

59 — Sergei Sokolov, Denis Mahov and Victor Kochin.
Comparative Analysis of Machine Learning Algorithms for Anomaly Detection in Time Series of User Activity in Corporate Systems

69 — Anton Shilov, Andrei Petrovski and Igor Kotenko.
A Reproducible Evaluation Framework for Immune-Augmented Intrusion Detection

148 — Dmitry Levshun and Diana Levshun.
Behavior-based Malware Detection in CAPEv2 Sandbox Using Deep Learning

145 — Tran Duc Le, Truong Duy Dinh, Igor Ushakov and Dinh Hai Nguyen.
Calibrating Evolutionary Game Payoffs from Malware Execution Traces: A Signature-Conditional Equilibrium Study on WinMET 2025

Session 5: Attack analysis, robustness and evaluation of AI models.
Session Chairs - Evgenia Novikova, Alexey Magazev. (ауд.311)

25 — Aleksei Shevchenko, Daniil Skaldin, Ilya Sokolov, Yuri Trofimov and Alexey Averkin.
Analysis of Attention Zone Shifts in a Medical Image Classifier Under FGSM Attack: A Comparative Study of Standard and Robust Models Using the Grad-CAM++ Method

41 — Evgenia Novikova and Aleksandr Sukhanov.
Approach to the evaluation of the AI model robustness to adversarial attacks

66 — Jenefa J, Mary Anita E A, Vinodha D, Maria Lapina and Vitalii Lapin.
An Enhanced Deep Ensemble Learning Approach for Accurate Phishing Website Detection

72 — Ansh Kaushik, Vimmi Malhotra and Divik Arora.
Beyond Accuracy: A Resource-Aware Comparative Evaluation of Machine Learning Models for Wearable Health Monitoring

6 - Alexey Magazev, Valeria Gorohova, Yana Seryogina and Pavel Lozhnikov.
A Markov-Based Framework for Security Metrics and Optimal Defense Using CAPEC Attack Patterns and CVSS

142 — Gleb Semenov, Maria Lapina, Amjad Gawanmeh, Vitalii Lapin and Oleg Sanamyan.
Robustness of Smart Grid Load Forecasting Models to Adversarial Attacks

16 — Nikita Kurganov.
Investigating the Robustness of a Classifier for Texts Generated by LLMs to Automatic Paraphrasing

Session 6: Cybersecurity, compliance and incident management.
Session Chairs - Eugine Abramov, Alexey Vulfin. (ауд.305

10 — Alena Stolnikova, Sergey Porshnev and Dmitry Khoroshkeev.
Ensuring Information Security of Systems with Integrated AI Technologies: A Comprehensive Approach to Security Auditing

12 — Maxim Gorda and Pavel Sharikov.
System Architecture for Legally Compliant Collection and Preprocessing of Digital Evidence in Incident Investigation

	40 — Maxim Shamanaev and Alexey Filippov. Semantic Matching of Cybersecurity Requirements and Internal Policy Documents for Automated Compliance Assessment 54 — Alexey Vulfin, Andrey Lutskovich and Anastasia Kirillova. Cyber threat intelligence data analysis system based on knowledge graphs 55 — Pavel Sundeev. Technology for the synthesis of constructive information protection 57 — Eugine Abramov and Margarita Knyazeva. Formalization of the semantic gap in projecting cyber threat models onto computational forensics tasks 68 — Galina Rybina and Andrey Grigoryev. An Approach to Ensuring Information Security of an Intelligent Control System for the Functioning of Tutoring Integrated Expert Systems: Integration of Simulation Modeling, Temporal Inference and Cognitive Engineering Methods
16:00 - 16:30	**Coffee break**
16:30 - 18:00	**Round table - AI and cybersecurity.** **Moderators - Andrey Chechulin, Michael Zabezhailo. Speakers - Evgenia Novikova, Darina Okuneva, Abdulkhamid Buchaev. (ауд.306)**
19:00 - 22:00	**Dinner**

Wednesday, 28 October 2026

09:00 - 10:00	**Registration**
10:00 - 10:30	**Coffee break**
10:30 - 12:30	**Parallel Sessions 7-9** **Session 7: Safety of space and unmanned systems.** **Session Chairs - Boris Sokolov, Ilya Popov, Olga Krivorotko. (ауд.306)** 36 — Anton Baranov, Valerii Zakharov and Boris Sokolov. Model-based and algorithmic support for proactive control of distributed measurements and calculations performed by a multi-satellite constellation 51 — Alexandr Spesivtsev, Yuri Tilichko and Vasily Spesivtsev. Assessing the Degree of Autonomy of Unmanned Aerial Vehicles: Methodological Aspects and Fuzzy-Possibility Modeling 85 — Olga Krivorotko, Nikolay Zyatkov, Ilya Markov, Anastasiia Murzina, Yakov Scherbina and Konstantin Pronin. Large-scale agents cooperative attack-defense control in high-dimensional environments based on deep reinforcement learning

	14 — Timofey Melnikov, Evdokiia Galkina and Ilya Popov. Subjective Logic-based Trust and Reputation model for FANETs 30 — Pavel Chertovskikh, Andrey Boiko and Ilya Popov. Numerical Optimization Method for Satellite Constellation Control in Area Surveying Problems Using a GPU-Accelerated Simulator 93 — Mohd Adnan and Aasim Zafar. Benchmarking Operational-Leak Risk in Open-Weight LLMs for Space and Counterspace Attacks **Session 8: Cryptography, quantum, blockchain and formal methods.** **Session Chairs - Sergey Bezzateev, Anatoly Korobeynikov. (ауд.311)** 13 — Anatoly Korobeynikov. Analysis of the application of the Lenstra-Lenstra-Lovasz algorithm in lattice cryptosystems 49 — Anton Pljonkin, Sandeep Joshi, Pradeep Kumar Singh and Gennady Veselov. Review of Synchronization Algorithms in Quantum Key Distribution Systems 56 — Evgeniya Ishchukova. Differential and Linear Cryptoanalysis Of The Kuznyechik's Three Rounds 73 — Anastasija Krasnenkova. Formal Verification of a Typical Smart Contract for the Innochain Blockchain 91 — Andrei Golovanov, Anastacia Kiryanova and Sergey Bezzateev. Application of a Fail-Stop Signature Mechanism in Satellite Group Authentication 33 — Igor Saenko, Vladislav Sheviakov, Vladimir Sadovnikov and Andrey Chechulin. Improving the efficiency of response to information security incidents based on a hybrid mesh network architecture and blockchain technology **Session 9: Biometric security and authentication.** **Session Chairs - Vasily Desnitsky, Viktoriia Korzhuk. (ауд.305** 46 — Mohamed Azab and Viktoriia Korzhuk. Robust ECG Biometric Authentication Using a Hybrid Deep Learning Model with Adaptive Beat Aggregation 18 — Daria Goncharenko, Oleg Kravchenko, Pavel Mizinov and Dobroslav Egorov. Artifact Synthesis for Robustness Assessment of Palm-Dorsal Vein Biometric Systems 48 — Mohamed Azab and Viktoriia Korzhuk. ECGAuthNet: A Segment-Adaptive CNN Architecture for Variable-Length ECG Biometric Authentication 24 — Pavel Mizinov, Dobroslav Egorov, Oleg Kravchenko and Natalia Konnova. PAI on the skin's surface: A New Attack Vector for Dorsal Vein Biometrics 50 — Mohamed Azab and Viktoriia Korzhuk. Multimodal Biometric Authentication using Paired ECG and PPG Signals via a Multiple Beat Aggregation Algorithm
12:30 - 13:00	**Closing session (ауд.306)**

13:00 - 14:00	Lunch
15:00 - 18:00	Excursion

Plenary - 50 min (talk - 40 min, questions - 10 min)
Session paper - 20 min (talk - 15 min, questions - 5 min)
Round table - 1 hour 30 min