PROGRAM
Round Table "New Trends in Cybersecurity"

Date: Monday, 26 October 2026
Time: 16:30–18:00 (90 minutes)
Venue: ITMO University, 14A Pesochnaya Embankment, Saint Petersburg, Russia.

ABOUT THE ROUND TABLE

The round table is devoted to new trends in cybersecurity. The development of key cross-cutting information technologies, including quantum technologies and artificial intelligence, is changing the cybersecurity landscape: from the emergence of new classes of threats to the use of promising quantum-resistant solutions based on these technologies. Leading scientists and representatives of corporate R&D divisions will discuss which fundamental and exploratory research in cybersecurity needs to be carried out today to ensure the country's technological sovereignty amid growing cyber threats, stricter information security requirements for critical information infrastructure (CII) facilities of the Russian Federation, and the increasing inadequacy of existing cybersecurity technologies. The discussion focuses on shaping a long-term research agenda and identifying priority areas for the development of cybersecurity.

MODERATOR

Sergei A. Petrenko – Doctor of Technical Sciences, Professor, Group Leader at the Scientific Center for Information Technologies and Artificial Intelligence, Sirius University of Science and Technology, Sirius Federal Territory, Russia.

Research interests: information security and cyber resilience of CII facilities of the Russian Federation, quantum and post-quantum cybersecurity, early detection, prevention and mitigation of computer attacks, proactive security of cyber-physical systems, development of immune-inspired information security systems, AI technologies, and self-healing technologies for CII facilities of the Russian Federation.

SPEAKERS

Igor B. Saenko (SPC RAS) – Doctor of Technical Sciences, Professor, Leading Researcher at the Laboratory of Computer Security Problems, St. Petersburg Federal Research Center of the Russian Academy of Sciences. His main works address theoretical and practical problems in the use of information and telecommunication technologies, including information security in computer networks, artificial intelligence, databases, and decision support in the design and planning of information systems. He is the author of more than 400 scientific publications, including 10 textbooks, study guides and monographs.

Eugine S. Abramov (SFedU) – Candidate of Technical Sciences, Associate Professor, Head of the O.B. Makarevich Department of Information Technology Security (BIT ICTIS SFedU). Research interests: information security, detection of anomalies and computer attacks, machine learning, security data analysis and visualization, and protection of cyber-physical systems.

Alexey M. Vulfin (UUST) – Doctor of Technical Sciences, Professor, Professor at the Department of Computer Engineering and Information Security, Ufa University of Science and Technology. Research interests: information security; models and methods for comprehensive security risk assessment of critical information infrastructure facilities based on data mining; anomaly and computer attack detection technologies; architecture and technologies of

information security monitoring centers; artificial intelligence technologies; computer forensics; microprocessors and microprocessor systems.

Ilya Yu. Popov (ITMO) – Candidate of Technical Sciences, Associate Professor at ITMO University. Research interests: information security methods and systems, information security, swarm systems and unmanned technologies. Head of the drone racing section of the university team “Kronverkskie Barsy” and Vice President of the Leningrad Region Drone Racing Federation. He leads a number of ITMO projects on the development and testing of unmanned transport systems (jointly with JSC NIIAS).

Aleksandr A. Menshchikov (ITMO) – Candidate of Technical Sciences, Associate Professor, Dean at ITMO University, Director of the Cyber Range training and practice center. Research interests: formal verification of neural network computer vision systems and management of domain shift in synthetic data for cooperative perception of unmanned vehicles; development of algorithms for automatic chain-of-thought reasoning in large language models; development of systems for detection, prevention and mitigation of computer attacks on CII facilities of the Russian Federation; mathematical models of countering computer attacks in training cyber ranges based on Attack-Defense CTF principles; technologies for ensuring information integrity in V2X cooperative perception systems for multi-agent autonomous vehicles.

SCHEDULE

16:30–16:45

Opening remarks by Sergei Petrenko: “New Cybersecurity Challenges and Threats”.

16:45–17:00

Block 1. Current cybersecurity trends.

17:00–17:15

Block 2. Quantum and post-quantum cybersecurity.

17:15–17:30

Block 3. Applications of AI technologies in cybersecurity

17:30–17:45

Block 4. Development of information security monitoring and operations management technologies (SOC, MSSP, CERT, CIRT, etc.)

17:45–18:00

Audience questions and wrap-up.

DISCUSSION QUESTIONS

BLOCK 1. Current cybersecurity trends.

16:45–17:00

1. Which of the following, in your opinion, is most relevant for developing perimeter protection of CII facilities of the Russian Federation?

Web server technology fingerprinting and protection recommendations? A real-time application “health” widget? Development of information security profiles? Fast creation of exceptions directly from the attack log? Automation via Ansible (IaC)? Extended protection for JSON and XML? Your own answers?

2. Which cybersecurity technology trends are genuinely useful in practice, and which still remain merely promising information security technologies?

- **Implementation of the “Secure by Design” principle,** which implies designing and building automated systems in a secure configuration from the earliest stages of their life cycle (requirements analysis, technical design).
- **Identity and access control (Identity Security): shifting the focus** of protection from the system perimeter to specific accounts, strengthening multi-factor authentication (MFA) and controlling digital footprints.
- **Adapting to the MaaS (Malware-as-a-Service) and Attacker AI-as-a-Service (malicious AI by subscription) models, as attackers have adopted** “services”: phishing, ransomware and infostealers offered by subscription on “black” marketplaces.
- **Focus on supply chain security, taking into account the risks** of compromise through vulnerabilities in third-party software and weaknesses of contractors or partner organizations and their services.
- **A shift from “responding to security challenges” to “ensuring cyber resilience”:** recognizing that 100% protection does not exist and security risks always remain; managing information security risks; developing security metrics and measures.

BLOCK 2. Quantum and post-quantum cybersecurity.

17:00–17:15

3. The global transition to post-quantum cryptography is no longer merely a research prospect: it has become an engineering and organizational migration task whose timeline and cost are directly determined by the parameters of the underlying cryptographic primitives. Existing standardized families (lattice-based, hash-based and MQ schemes) show a trade-off between security level and the overhead of transmission, storage and verification, which subjects their use in high-load distributed systems to architectural constraints.

Which methods for constructing post-quantum digital signature algorithms are currently most in demand, and why? How can the strength of cryptographic primitives be assessed? How can the architecture of software tools for building post-quantum digital signatures be implemented in practice?

4. The transitional stage of migrating critical information infrastructure facilities to post-quantum cryptography requires support for hybrid signature schemes (for example, KNAA-2 digital signature + GOST R 34.10-2018).

How can sufficient procedures be defined for signature aggregation, fallback routing and estimating the overhead of storing dual cryptographic material in the transaction ledger? How can the hybrid-mode protocol be formalized, and how can its impact on throughput and on the state size of intermediate nodes be assessed?

BLOCK 3. Development of AI technologies in cybersecurity

17:15–17:30

In 2026, AI agents and multi-agent systems in general are developing and being adopted at a rapid pace. The main engineering challenge has shifted from creating AI agents to deploying them. As a result, so-called open infrastructures for rapid deployment of the Agent Stack have come into demand. The Agent2Agent (A2A) protocol has enabled agents built on different frameworks to interact with each other more productively. Technologies like these have taken agentic AI to a new level.

The following questions also remain relevant.

5. How can the required accuracy of general-purpose large language models (LLMs) trained on massive datasets be achieved for specific domains and engineering tasks in information security? What is the role of domain-specific language models (DSLMs) here? How should such models be trained on highly specialized datasets?

6. What opportunities do AI technologies open up for the broad practical use of software engineering tools, including low-code and no-code platforms?

BLOCK 4. Development of information security monitoring and operations management technologies: SOC, MSSP, CERT/CIRT.

17:30–17:45

7. What technological innovations in information security monitoring and management are expected over the next three years?

- **SIEM + Next-Gen SIEM (collection and correlation of security events):** development of user and entity behavior analytics (**UEBA**) to detect previously unknown anomalies.
- **EDR / XDR (detailed detection, mitigation and response):** development of endpoint cybersecurity capabilities, use of cloud environments and advanced network traffic analysis (NTA)? How will this affect the development of the unified cyber kill chain and the improvement of the well-known information security threat modeling methodologies of MITRE and FSTEC of Russia in general?
- **SOAR / IRP (orchestration and automation):** development of automated scenarios (**Playbooks**) for timely detection and isolation of compromised hosts, etc.?
- **ASM (Attack Surface Management):** development of external attack surface management technologies: how will this affect the development of SOC 2 and next-generation SOCs (external monitoring capabilities, tracking forgotten IT assets, open ports, shadow cloud services (Shadow IT) and the Darknet, etc.)?

FORMAT

The round table is held as an open moderated discussion.

After the opening talk, the speakers will discuss the questions in turn, grouped into four thematic blocks. The moderator guides the discussion, addresses questions to the speakers based on their professional experience and ensures that different points of view can be shared.

The final part includes audience questions and a wrap-up.

Duration: 90 minutes.

Language: Russian.