PROGRAM
Round Table “AI and Cybersecurity”

Date: Tuesday, 27 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 current trends in the use of artificial intelligence in information security, the new opportunities and threats associated with the development of intelligent technologies, and issues of their practical implementation and workforce training. Representatives of academia, industry and education will discuss how artificial intelligence is changing the confrontation between attackers and defenders, which technologies have already proven effective, how safe it is to use autonomous intelligent systems, and how the requirements for information security professionals will change in the coming years. Particular attention will be paid to cooperation between research organizations, universities and industry, promising research directions, and the challenges of putting research results into practice.

MODERATORS

Andrey A. Chechulin – Candidate of Technical Sciences, Associate Professor, Leading Researcher, Head of the International Digital Forensics Center, St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS).

Research interests: information security, digital forensics, computer attack detection, cyber incident investigation, security of cyber-physical systems, and applications of artificial intelligence in information security.

Michael I. Zabezhailo – Doctor of Physical and Mathematical Sciences, Professor, Federal Research Center “Informatics and Control” of the Russian Academy of Sciences (FRC IC RAS).

Research interests: artificial intelligence, data mining, machine learning, formalization of reasoning, inductive inference and decision support.

SPEAKERS

Evgenia S. Novikova – Candidate of Technical Sciences, Associate Professor, Head of the Department of Information Systems, Saint Petersburg Electrotechnical University “LETI” named after V.I. Ulyanov (Lenin).

Research interests: information security, detection of anomalies and computer attacks, machine learning, security data analysis and visualization, and protection of cyber-physical systems.

Darina V. Okuneva – Candidate of Technical Sciences, Associate Professor, Head of the Cybersecurity Analytics Center at Gazinformservice.

Professional focus: information security, development and application of cyber defense technologies, cyber threat analysis, development of the competencies of information security professionals, and adoption of domestic cybersecurity solutions.

Abdulkhamid Ya. Buchaev – Senior AI Security Expert, Alfa-Bank; ITMO University.

His professional work focuses on MLSecOps (Machine Learning Security Operations), a relevant and rapidly developing field concerned with securing the life cycle of machine learning and artificial intelligence models.

SCHEDULE

16:30–16:45

Opening talk by Andrey Chechulin: “AI in Cybersecurity: A Tool for Defense, a Means of Attack, and an Object of Research”.

16:45–17:10

Block 1. Technologies and threats.

17:10–17:30

Block 2. Practice and implementation.

17:30–17:50

Block 3. Professionals and the future.

17:50–18:00

Audience questions and wrap-up.

DISCUSSION QUESTIONS

BLOCK 1. TECHNOLOGIES AND THREATS

16:45–17:10

1. Who is adopting AI faster today: attackers or defenders?

What changes in cyberattacks and defenses has AI already brought about? Are attackers gaining an advantage from the availability of generative models and automation?

2. Which AI technologies are genuinely changing cybersecurity, and which are still just marketing?

Large language models, autonomous intelligent agents, machine learning for attack detection, intelligent SOC automation. Where are there already measurable results, and where do expectations outpace actual capabilities?

3. Who should protect AI systems themselves, and how?

Attacks on models, data poisoning, prompt injection, manipulation of intelligent agents. Are traditional information security approaches sufficient, or are fundamentally new protection methods needed?

BLOCK 2. PRACTICE AND IMPLEMENTATION

17:10–17:30

4. Can AI be trusted to respond to cyberattacks on its own?

Where is the line between a recommendation, an automated action and a human decision? Which tasks can be fully automated, and who should be responsible for the errors of intelligent systems?

5. Why do promising AI research results not always make it into real-world deployment?

What is missing for the transition from a research prototype to an industrial solution? Which business problems remain unsolved, and which directions should research focus on?

BLOCK 3. PROFESSIONALS AND THE FUTURE

17:30–17:50

6. How is AI changing the requirements for information security professionals?

Which professional tasks will be automated, which competencies will be most in demand, and will we need as many cybersecurity professionals in the future?

7. Is the education system keeping pace in preparing professionals for new threats and technologies?

Do educational programs need to be revised, what should future information security professionals be taught, and how can industry and research organizations be involved in their training?

8. What will cybersecurity look like in five years?

Will autonomous intelligent agents become the main participants in the confrontation between attackers and defenders? Which of today’s problems will disappear, and what new threats will emerge?

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 three thematic blocks. The moderators guide the discussion, address questions to the speakers based on their professional experience and ensure that different points of view can be shared.

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

Duration: 90 minutes.

Language: Russian.