33RD INTERNATIONAL CONFERENCE ON PROBLEMS OF COMPLEX SYSTEMS SECURITY CONTROL

In December 2025, the 33rd International Conference on Problems of Complex Systems Security Control took place at the Trapeznikov Institute of Control Sciences, the Russian Academy of Sciences (ICS RAS), Moscow.

The conference was attended by 86 authors from 28 organizations, who presented 63 papers. The conference was divided into the following sections:

1. General theoretical and methodological issues of security support;
2. Problems of economic and sociopolitical security support;
3. Problems of information security support;
4. Cybersecurity. Security aspects in social networks;
5. Ecological and technogenic security;
6. Modeling and decision-making for complex systems security control;
7. Automated systems and means of complex systems security support.

I.V. Chernov, the conference opener and chair of the plenary session, gave the floor to *D.I. Pravikov*, who dedicated his speech to the memory of *Sergey P. Rastorguev* (1958–2017), an outstanding Russian scientist, Dr. Sci. (Eng.), Prof., and author of over 100 research and scientific-popular publications of special and interdisciplinary nature. Rastorguev's fundamental and applied research interests were very broad to cover various fields of computer science, programming, cryptography, antivirus protection, avatarization (the transfer of the basics of biological life and consciousness to a computer system), philosophy and sociology, learning theory, and pedagogy. He is a founder of the Russian scientific school of information confrontation, the author of many scientific works on the theory and practice of information warfare, which have become classics of this fundamentally new scientific direction of the recent past. The term "information warfare" itself came to be understood in the Russian literature in Rastorguev's interpretation after the release of the same-name monograph in 1999.

The basis of his philosophical views was formed at a time when neural networks became a topical and rapidly developing field of science and engineering. As emphasized in the speech, Rastorguev's postulate about one of the fundamental properties of networks arose at that time: learning takes place through not only the creation but also the destruction of connections and the elimination of elements. This postulate, seemingly unobvious at first glance, underlies the description of the main properties of information weapons: during (self-)training, complex systems can (self-)restrict or suppress themselves.

According to the speaker, Rastorguev's scientific legacy and heritage are so profound and multifaceted that the research community has yet to comprehend and understand them. Operating intuitively understandable basic meanings ("life," "death," "information," "knowledge"), Rastorguev went far beyond the ordinary in his conclusions and philosophical constructs and aimed at a critical understanding of the surrounding reality. The scientific results obtained by S.P. Rastorguev remain extremely relevant today.

The program part of the conference was opened with a comprehensive review by *T.S. Akhromeeva*, *G.G. Malinetskii*, *and S.A. Toropygina*, entitled "New Approaches to the System Analysis of Large-Scale Projects." As stated in the first part of the review, in modern conditions, conventional interdisciplinary system analysis-based approaches to the problems of analysis, structuring, and management of the development of large-scale systems in various fields are undergoing a deep crisis, breaking down into a set of weakly interconnected methodological directions.

According to the authors, the main practice-suggested reason is that the conventional approaches fail to cope with the main contemporary problems of designing the development of large-scale systems, namely, analysis, prediction of their development dynamics, and risk management. Here, Akhromeeva–Malinetskii–Toropygina's recipe is to create new tools for pressing state development tasks based on the ex-

perience of applying methods and models of self-organization theory (synergetics) in the analysis of complex problems and the development of large-scale projects. This methodology can be effectively used to describe the properties and characteristics of competing large-scale projects, as well as the rivalry between countries, blocs, civilizations, and ethnic groups in the economy, military, or other areas of confrontation.

In particular, while considering the advantages of synergetics and analyzing the methodology for solving the above tasks, the authors noted that this approach eliminates the "curse of dimensionality" by identifying order parameters (primary variables and degrees of freedom) that gradually—over time—start determining the dynamics of other characteristics of the complex system under study. In other cases, where the key factors are so-called ultra-fast processes (compared to them, all others get "frozen"), there is an opportunity for simplification associated with the use of order parameters, which (in this case, on the contrary) describe fast variables.

The second part of the review was devoted to publications reflecting the use of various fragments of this approach to solve technological development tasks of the military-industrial complex of Russia's geopolitical opponents over a twenty-year horizon. The authors concluded that the high-level tension in international relations convincingly demonstrates the need to develop system analysis methods and technologies in order to manage the interaction (confrontation) of competing agents.

A distinctive feature of the conference was many interesting and diverse papers devoted to solving a wide range of problems related to the secure and sustainable socio-economic development of Russia in the current (extremely difficult) conditions.

V.V. Tsyganov's paper "Secure Sustainable Development Mechanisms in a Multipolar World," considered the problems of the country's economic development in the context of intensifying contradictions and the negative impact of globalization processes. As noted therein, the Concept of Sustainable Development (put forward at the UN Conference on Environment and Development in Rio de Janeiro, 1992) pays central attention to the interests of not only the current but also future generations; however, this concept is now being exploited by the global capital center in its own interests as a tool to influence and manipulate environmental standards by applying environmental taxes to imports from developing countries. With such methods, globalists impose excessive environmental requirements on the production and goods of developing countries, which cannot be satisfied without expensive Western technologies. In this regard, it is necessary to modify sustainable development mechanisms in order to make their application secure for developing countries. This primarily concerns mechanisms for the secure and sustainable development of key economic agents in these countries, ensuring their independence, as well as the ability to adapt and self-organize in the face of regional or global changes.

The author presented a robust mechanism for solving this problem, including procedures for forming security indicators, algorithms for calculating the norms of the indicators to categorize them, as well as the convolutions of the resulting categories for an integrated assessment of sustainable development security to incentivize decision-makers. The practical application of the robust mechanism was illustrated by a detailed example of ensuring the secure and sustainable development of Russian rail transport under environmental protection requirements (the task of managing the overhaul of the diesel locomotive fleet within the maintenance program of JSC Russian Railways).

In the paper "Problems of the Development of the Russian Financial Market and Its Strategic Planning," *A.E. Abramov*, *M.I. Chernova*, *and F.S. Levin* comprehensively assessed the intermediate implementation results of the federal project "Development of the Financial Market" and analyzed the existing problems of financial regulation and strategic planning hindering its success. As stated in the paper, a necessary condition for the successful implementation of the Russian financial market development strategy based on domestic savings and investments is its integration into the strategic planning system for the development of the Russian economy as a whole. This necessitates greater engagement of the financial regulator in market development, which should largely be reduced to creating conditions for the growth of innovative business activity through the regulator's traditional functions.

According to Federal Law no. 172-FZ "On Strategic Planning in the Russian Federation," the Bank of Russia is a participant in the state long-term planning system. However, nowadays, a serious problem is that Federal Law no. 86-FZ "On the Central Bank of the Russian Federation (Bank of Russia)" describes the functions of the mega-regulator in a very fragmented manner, limiting them to the development and stability of the financial market. As a result, several pressing tasks of financial regulation and supervision (over-

coming "market failures," supporting competition, protecting the rights of investors and consumers of financial services, ensuring the stability of financial institutions, etc.) have almost no intersection with the objectives of the Bank of Russia as defined in the latter federal law.

The authors emphasized a series of challenges to be settled, notwithstanding the progress in recent years (significant in several areas) in integrating the financial market development policy into the strategic planning system, which was largely implemented by overcoming a definite gap between policy documents on financial market development and programs for the development of the Russian economy as a whole. Based on the comprehensive and detailed analysis results of the main target-setting and regulatory documents, as well as the key development indicators of the Russian financial market for the period up to 2030 (see the paper), Abramov et al. identified as the main problem the insufficiently justified quantitative targets reflecting the dynamics of financial market development, as well as the fragmentary nature of measures aimed at stimulating domestic long-term savings. To solve this problem in the long term, it is necessary to specify completely the key functions of the financial regulator at the legislative level, as well as to optimize the structure of strategic financial planning documents (in particular, to eliminate duplication and unify the system of predictive indicators for the development of the financial market for 2030, contained in the Strategy for the Development of the Financial Market of the Russian Federation until 2030 and the federal project "Development of the Financial Market").

The paper "Risks in a Financial Market and Their Assessment" by *A.D. Kozlov and N.L. Noga* presented an original methodology for assessing risks when conducting operations in a financial market. This methodology is based on the combined use of econometric and fuzzy logic methods; structurally, it consists of a sequence of interconnected stages as follows.

The first stage is to examine a financial market and determine a set of parameters characterizing both systematic and unsystematic risks. The resulting set is divided into groups of financial, internal, and external economic parameters, as well as other parameters (if necessary). In the next stage, expert procedures are used to select from the initial set the subsets of parameters with the greatest impact on the risks of financial losses, and a fuzzy knowledge base is formed accordingly. These parameters are written as linguistic variables normalized in the range from 0 to 1. Then, a table of production rules is formed, where each row is assigned a specific risk level. In the third stage, a linear multiple regression model is constructed based on this table, and standardized equation coefficients are determined for their ranking. The fourth (final) stage is to identify the variables with the greatest impact on the risks of financial losses and to check their interdependence. The quality of the resulting model is assessed by computing the multiple determination coefficients. The statistical significance of the regression coefficients and the regression equation as a whole is verified using Fisher's F-test and Student's t-test. In conclusion, the authors provided an example illustrating the practical possibilities of using the methodology by investors to predict financial losses under uncertainty and risk.

Note a large group of conference participants who considered a wide range of methodological and applied problems of managing the socio-economic development of Russia, its regions, and economic agents: *N.I. Komkov*, *V.V. Sutyagin*, *and N.N. Volodina* ("Possible Coordination of the Effectiveness of Economic and Social Development Management"); *V.A. Irikov and D.R. Gonchar* ("The Breakthrough Socio-Economic Development of the Country in 2025–2030: New Directions, Features, Opportunities, and Examples of Multiple Growth"); *Z.K. Avdeeva and S.V. Kovriga* ("The Strategic Planning Graph in the Russian Federation's National Security System"); *V.V. Shumov* ("Conflict Modeling Using Methods of Military Cybernetics and Security Studies"); *V.V. Nicheporchuk* ("Intelligent Services for Territorial Security Management"); *A.V. Rozhnov* ("Justifying the Development of an Information and Analytical System When Implementing Hybrid Analysis Technology Models for the Environment in Predictive Modeling"); *V.I. Medennikov* ("Digital Tools Providing a More Environmentally Friendly and Safer Path for Humanity Development"); *O.B. Bairamov* ("Combined Application of Penalty Models and Environmental Insurance for Managing the Risks of Water Basin Degradation"); *T.Kh. Usmanova and O.V. Dem'anova* ("Formation of the Socio-Economic Security of the North–South International Transport Corridor"); *L.E. Mistrov* ("A Method for Distributing Heterogeneous Resources to Ensure Conflict Resilience in the Interaction of Organizational and Technical Systems"); *D.R. Gonchar* ("Population Preservation as a New Target Indicator for the More Successful Socio-Economic Development of the Country in 2025–2030"); *V.O. Sirotyuk and L.V. Bogatyreva* ("Compre-

hensive Security of the Subjects of an Intellectual Property Management System"); and *N.N. Lanter* ("Features of Arctic Concepts of Foreign Countries in 2025–2030").

A series of interesting papers were devoted to theoretical and practical problems of developing a scenario analysis methodology and simulation modeling technologies for managing the development of complex socio-economic systems at the governmental, industrial, regional, and object levels. Among them, let us mention the following: "The Vulnerability of a Complex System: A Hierarchy of Concepts" (*D.A. Kononov and I.V. Chernov*); "The Sustainable and Secure Development of Complex Systems, Southern Russia, Cognitive Modeling" (*G.V. Gorelova*); "Analysis of Verification Methods and Technologies for Scenario Management Models" (*V.L. Shul'ts*, *I.V. Chernov*, and *A.B. Shelkov*); "Support for the Management of Complex Socio-Economic Systems Using Situational Scenario Analysis Methods" (*M.Yu. Dmitrieva*, *I.D. Butusov*, and *Yu.A. Gogoladze*); "The Use of Scenario Analysis in DSSs for Regional Security: A Brief Review" (*N.V. Komanich*); "A Scenario Model for Studying Threats to the Secure Development of Urban Infrastructure" (*M.Yu. Dmitrieva* and *L.V. Bogatyreva*); and "Prospects for Using Scenario Analysis to Ensure AI Information Security" (*E.D. Ermolaeva*).

The paper "Justifying Comprehensive Assessment Indicators for the Security of Critical Information Infrastructure of Oil and Gas Companies" by *D.I. Pravikov and V.A. Burkin* was devoted to developing security assurance methods for the production, information, and technology infrastructure of companies extracting hydrocarbon minerals. As noted therein, oil and gas complex facilities are complex socio-technical systems in which automated process control subsystems, information resources, personnel, and regulatory documents form a single interdependent structure. Managing their security requires passing from regulatory supervision to a quantitatively verifiable and comprehensive (integrated) security assessment to compare facilities, prioritize organizational and technical measures, and justify managerial decisions based on measurable indicators.

The authors presented an original methodology for calculating a comprehensive security indicator for the critical information infrastructure of oil and gas companies (a weighted sum of ten standardized partial metrics). These metrics reflect a wide range of security indicators: critical segments of the information structure are covered by centralized collection and correlation of security events, and nodes are covered by the minimum necessary set of protective measures; the timeliness of eliminating critical vulnerabilities of protected facilities is assessed, and the unscheduled downtimes of industrial systems and the rate of recovery after an incident are estimated; the level of personnel's readiness for actions in abnormal and critical situations is assessed, etc. Appropriate metrics are selected considering industry specifics, and each metric has a direct connection to the actions stipulated by the relevant regulatory, normative, and other organizational documents and requirements. As a consequence, the indicators are comparable, the results can be audited, and operational risk management in the loop of industrial and information security becomes more efficient. Generally speaking, the approach proposed is a practice-oriented tool for managing the security of critical information infrastructure, linking target security levels to particular actions and resources; moreover, it ensures the reproducibility of assessments and the transparency of decisions.

Traditionally, many conference papers deal with various information security management problems. In this thematic group, note the following: "An Information Security Model Considering Sanctions" (*N.G. Kereselidze*); "Improving Video Data Security by Using a Noise-Resistant Video Steganography Method Based on Deep Neural Networks" (*S.A. Shustov and R.V. Meshcheryakov*); "Approaches and Tools for Collecting Information from Open Sources to Monitor and Identify Information Security Threats" (*L.N. Loginova and A.D. Drozdov*); "REST Services Based on the C# Language to Provide Information Protection in Windows–Linux Environments" (*R.E. Asratyan*, *S.S. Vladimirova*, *E.A. Kurako*, and *V.L. Orlov*); "An Online Reputation Monitoring Algorithm Based on Search Queries" (*D.S. Ignatov*); "Architectural Features and Specifics of Ensuring Information Security in High-Load Information Systems" (*A.D. Domashkin and L.N. Loginova*); "Risk Management for Computer Networks with the Tree Topology" (*A.A. Shiroky*); "Modeling Security Threats to Critical Information Infrastructure Facilities in the Republic of Angola" (*I.F. Mikhalevich and A.M. Fransisco Nelson*); "Using the Principles of Lean Management to Ensure the Information Security of an Industrial Enterprise" (*V.V. Vedishchev and R.V. Batishchev*); "Using Regular Expressions to Manage the Information Security of Intelligent Transport Systems" (*I.F. Mikhalevich and*

D.I. Pchelintsev); "Formalization of Information Security Risk in Intelligent Water Transport Systems as a Fuzzy Linguistic Assessment Based on Decision Theory" (*L.A. Baranov*, *N.D. Ivanova*, and *I.F. Mikhalevich*); and "Modeling a Smart Home Security System" (*Yu.A. Klimenko*, *A.P. Preobrazhenskii*, *and I.A. Tikhonov*).

A number of interesting application-oriented papers were devoted to the security of industrial and transport systems and facilities: "Cybernetics of the Security of Energy Systems with a Nuclear Reactors" (*V.V. Leshchenko*); "Assessment of the Effectiveness of Industrial Safety Management System Audits" (*E.V. Klovach*, *I.A. Kruchinina*, and *V.A. Tkachenko*); "Security and Reliability of Complex Technical Systems" (*S.K. Somov*); "An Approach to Assessing Changes in the Critical Characteristics of Robotic Systems over Time" (*M.V. Mamchenko*); "Reliability of Conductive Elements of Power Equipment with Pulse Modulation" (*O.B. Skvortsov and V.I. Stashenko*); "Mathematical Modeling of the Security of Ground Protective Structures under an External Seismic Wave Impact" (*V.K. Musaev*); "A Simulation Model of Operational Fire Response Phases at Fuel and Energy Complex Facilities with Robust Optimization of Time, Risk, and Resources" (*R.Sh. Khabibulin*); "General Theoretical and Methodological Issues of Security Assurance in the Development of a Flight Controller for UAVs: Control in the Process of Setting Up Experiments" (*D.A. Vol'f and R.R. Galin*); "Forming the Structure of a Flight Safety Management System for Unmanned Aerial Systems Based on Interoperability" (*D.M. Mel'nik*); "Security Assessment for the "Unmanned Aerial Complex–Personnel–Environment" System Based on Scenario Analysis" (*A.G. Davydovskii*); "A Mathematical Model of the Influence of Space Flight Factors on the Quality of Astronaut Performance and the Formation of Ergonomic Risk" (*E.A. Timme*); "Safety of Transport Infrastructure and Vehicle Control Systems" (*L.A. Baranov*, *S.E. Ikonnikov*, and *A.E. Ermakova*); "A Threat Model for a Wheeled Platform Control System with a Multi-Agent Multi-Level Neural Network Implementation" (*O.A. Tel'minov*); "Organizational Features of the Transportation Process on the Moscow–St. Petersburg High-Speed Railway under Construction" (*A.I. Isakova and A.S. Meshcheryakova*); "Development of a Microservice for Analyzing and Predicting the Wear of Railway Contact Network Elements" (*A.S. Ikonnikov*); and "Application of Artificial Intelligence Technologies to Ensure the Information Security of Medical Systems and Devices" (*V.A. Zorin*).

The conference proceedings are published electronically[1] and are also available at the official website: https://iccss2025.ipu.ru/conf_proceedings.

The 34th International Conference on Problems of Complex Systems Security Control is scheduled for November–December 2026 at ICS RAS. The date and time of the conference will be announced in the information letter of the Organizing Committee, which will be published on the official website (https://iccss2026.ipu.ru/) as well as distributed to potential participants, interested parties, and specialized organizations. Also, please contact the Organizing Committee via phone + 7 495 198-17-20 (ext. 1407) or e-mail iccss@ipu.ru. The Technical Secretary of the conference is *Al'fiya Farissovna Ibragimova*.

Academic Secretary of the Organizing Committee
A.B. Shelkov
Event coordinator of the Organizing Committee
L.V. Bogatyreva

Author information

Shelkov, Alexey Borisovich. Cand. Sci. (Eng.), Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia
✉ abshelkov@gmail.com
ORCID iD: https://orcid.org/0000-0003-1408-5212

Bogatyreva, Larisa Vladimirovna. Cand. Sci. (Hist.), Trapeznikov Institute of Control Sciences, Russian Academy of Sciences, Moscow, Russia
✉ lbogat@mail.ru
ORCID iD: https://orcid.org/0000-0003-2744-0404

Cite this paper

Shelkov, A.B. and Bogatyreva, L.V., 33rd International Conference on Problems of Complex Systems Security Control. *Control Sciences* **1**, 79–83 (2026).

Original Russian Text © Shelkov, A.B., Bogatyreva, L.V., 2026, published in *Problemy Upravleniya*, 2026, no. 1, pp. 90–96.

This paper is available under the Creative Commons Attribution 4.0 Worldwide License.

Translated into English by *Alexander Yu. Mazurov,*
Cand. Sci. (Phys.–Math.),
Trapeznikov Institute of Control Sciences,
Russian Academy of Sciences, Moscow, Russia
✉ alexander.mazurov08@gmail.com

[1] *Materialy 33-ei Mezhdunarodnoi konferentsii "Problemy upravleniya bezopasnost'yu slozhnykh sistem"* (Proceedings of the 33rd International Conference on Problems of Complex Systems Security Control), December 17, 2025, Moscow, Kalashnikov, A.O. and Chernov, I.V., Eds., Moscow: Trapeznikov Institute of Control Sciences RAS, 2025. (In Russian.)