32ND INTERNATIONAL CONFERENCE ON PROBLEMS OF COMPLEX SYSTEMS SECURITY CONTROL

In November 2024, the 32nd 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 dedicated to the memory of Vladimir V. Kul'ba, Dr. Sci. (Eng.), Prof., Honored Scientist of the Russian Federation, and the conference founder. It was held face-to-face, with over 100 participants.

The plenary session was opened by Academician *D.A. Novikov*, Director of ICS RAS. His welcoming speech was dedicated to the memory of Kul'ba, the permanent head of the Conference Program Committee.

I.V. Chernov, Chair of the plenary session, described the main stages of Kul'ba's scientific activities as well as the fields of his fundamental and applied research. As emphasized by the speaker, from 1962 to 2024, Kul'ba headed several research fields at ICS RAS. Under his leadership and with his direct participation, the following R&D results were obtained:

– analysis methods for complex management systems;

– theoretical foundations for using the principles of modularity and type designs in data processing systems design;

– methods and technologies for automating the design of software and information support for open-architecture and real-time systems;

–methodological foundations for improving the effectiveness of organizational control and management in emergencies;

– methods for solving theoretical and applied information security problems for control systems at the organizational and software-hardware levels;

– an information control methodology;

– theoretical and methodological foundations of scenario management.

The speaker paid special attention to the Conference on Problems of Complex Systems Security Control, Kul'ba's favorite brainchild. The conference history goes back to the early 1990s, when, in response to Kul'ba's proposal, the Institute of Control Sciences initiated the International Scientific Conference on Control Problems in Emergencies. The initiative was supported by the RAS Presidium and the State Committee for Civil Defense, Emergencies, and Elimination of Consequences of Natural Disasters under the President of the RSFSR (later, reorganized into the same-name ministry of the Russian Federation). In addition to ICS RAS, the organizers of the conference included the Scientific Council for the State Scientific and Technical Program "Security," the Keldysh Institute of Applied Mathematics RAS, the Institute of Design Automation RAS, the Kharkevich Institute for Information Transmission Problems RAS, and St. Petersburg State University. Starting from 1999 (the 7th conference), Russian State University for the Humanities became one of the conference organizers.

Initially, the main theme of the conference was fundamental and applied research into improving the effectiveness of emergency management. Later, the Organizing Committee of the conference decided to change its name to the current one, following the appearance of new fields in the subject areas under consideration and the related ones, a significant widening of the topics of conference submissions, and the wishes expressed by the majority of regular conference participants. Since 1998 the conference name and the composition of its sections have remained almost unchanged, and the last 32nd Conference is not an exception.

The conference was attended by 104 authors from 33 organizations, who presented 73 papers. The conference program included 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. Automatic systems and means of complex systems security support.

Many papers presented at the conference were devoted to the study and solutions of the problems of ensuring the key components of national security, namely, military-political, scientific, industrial-technological, social, economic, informational, and technogenic. The topicality of this range of problems, representing one of the most complex set of problems in the theory and methodology of organizational control and management and several related scientific disciplines, has significantly increased in recent years. It is connected with various objective geopolitical reasons and the continuing growth of international tension.

V.V. Shumov presented the paper “Analysis of Factors Affecting the Achievement of the Goals of the Special Military Operation.” He considered a conceptual formalized model for assessing the level of national security of a state using a power production function, reflecting the dichotomy of the human values of development and self-preservation. The author’s formalized representation of the security function is structurally the product of two components: the function of sovereignty (development), based on the Cobb–Douglas power function, and the preservation function. The first function covers a set of geographical, demographic, and socio-technological factors to assess the geopotential of the state; the second function reflects the ability of the state to resist destructive processes (including those inspired from the outside) and develop sustainably. The modeling results were described and analyzed to assess:

(a) Russia’s security level, place, and role in global processes against the background of the ongoing geopolitical inversion (change of the world leader);

(b) the security level of the European Union and Ukraine in the context of its regions (as of 2013, i.e., for the period preceding the Euromaidan, which provoked an acute political and economic crisis).

The main goal of the modeling studies was to assess the possible consequences of a significant complication of the military and political situation in the world, associated with the growingly aggressive actions of Russia’s geopolitical adversaries aimed at weakening, inflicting a strategic defeat, and ultimately dismembering Russia. According to the analysis results, the response potential to parry existential threats to the Russian state and society exceeds the capabilities of Western countries, and the actions of their ruling elites do not meet the vital interests of their people. Hence, there are objective favorable conditions for achieving the security and sovereignty goals of the Russian Federation.

The paper “On a New Approach to the Design of Complex Organizational and Technical Systems” (*S.V. Chvarkov*, *S.N. Podchufarov*, and *R.M. Kufrik*) was devoted to the problems of increasing the effectiveness of modern weapon systems design. The following essential problems were emphasized in the first part of the paper:

1. the level of initial goal problem formulations (military and operational requirements for the development of complex products and systems), which often diverge from modern realities;

2. the incomplete compliance of the given requirements with the needs of practice, primarily concerning the development of information and control systems (an integral part of modern complexes and weapon systems that largely determines the effectiveness of their combat application).

According to the authors’ point of view, the reason is the insufficient level of correctness for the descriptions of particular subject areas (including related ones), due to, on the one hand, the high dynamism of information technology development and, on the other hand, the unsolved problems of passing from a non-formalized (linguistic) description to a formalized (mathematical) representation of control problems solved by complex organizational and technical systems.

The paper provided a detailed analysis of several organizational and technological drawbacks of the current practice of complex systems development, which include:

– definite disproportions in the distribution of funds for the development and modernization of mathematical, software, and hardware support for design processes;

– irrational desire to design expensive or unique, rather than unified, control complexes;

– insufficient attention to the development of prediction models, which serve to identify the evolution of weapon systems and analyze the character of armed struggle considering the asymmetry of using armed forces and nonmilitary means, etc.

Based on the analysis results (including foreign experience), Chvarkov et al. proposed an approach to solving the problems under study, which combines the problems of national security and defense with those of the economic, scientific, technical, industrial, and technological development of the state, considering the available real possibilities and limitations and the level of similar R&D results of probable adversaries.

In the paper "Opportunities for Active Adaptation of the Russian Economy to New Challenges," *N.I. Komkov, V.V. Sutyagin, and N.N. Volodina* considered a set of economic potential development problems as the most important component of the national security. As noted therein, the need to counteract the military-political and sanction pressure of Russia's geopolitical adversaries as well as attempts to isolate its national economy required rapid adaptation of public administration to the emerging threats. Thanks to this adaptation, contrary to the expectations of ill-wishers, the Russian economy is steadily growing, like the public support level for the country's top leadership. Nowadays, a set of new problems of ensuring economic growth in the current unfavorable conditions comes to the forefront.

The paper was focused on the design and analysis of an infological model of a full reproduction cycle based on the achievements of scientific and technological progress under the regular change of high technologies formed through innovations. Komkov et al. emphasized that science is the key link of this model: the effective realization of its potential largely determines the basic directions and rates of innovation development of a modern economy.

According to the authors' retrospective analysis, the low share of high-tech products in the Russian economy since the early 2000s was largely due to the dominance and availability of innovative technologies imported from EU countries and the USA. This factor actually blocked the development of domestic science and reduced the interest of industrial companies in the prospects of their development, which eventually led to a decline in the volume and level of prediction studies on the problems of scientific and technological development. Komkov et al. assessed the possibilities of economic growth in modern conditions and identified key factors directly affecting the processes under consideration. Among them, the most important ones are:

– the state of the innovation sphere and its conjugation with the economy;

– the manageability and coordination of economic development processes and the innovation sphere;

– the ability to adapt the economy to the effective assimilation of progressive innovative solutions and technologies;

– the availability of necessary and sufficient funding, as well as the vigor and purposeful actions of executive authorities to coordinate the interests of economic agents and develop the potential of the innovation sphere and the entire economy. According to the authors, the mechanism of state indicative planning should become a tool for solving innovative development problems. For companies and enterprises, this mechanism forms planned tasks consistent with a stable tax system, regular funding, and the coordination of the Central Bank's activity with financial structures issuing monetary resources and bonds.

A rather wide group of conference papers were devoted to the results of research into various methodological and applied problems of increasing the effectiveness of national security control processes, namely: "Security Control of Complex Systems in the New Reality" (*G.G. Malinetskii*, *T.S. Akhromeeva*, and *S.A. Toropygina*); "A Complex of Strategic Security Models for the Russia's Perimeter" (*V.V. Tsyganov*); "Urgent Critical Threats to the Information-Psychological Security of Social Objects" (*E.A. Derbin*); "The Method of Pseudo-Retrospective Manipulation of Consciousness as an Information Warfare Tool" (*A.N. Fomichev*); "An Information Security Model in the Case of Two Disinformation Sources" (*N.G. Kereselidze*); "Synergetic Foundations of System Approach to Complex Systems Security" (*G.G. Malinetskii* and *V.S. Smolin*); "Justification of Hybrid Models for Analyzing the Operating Environment in Descriptive Examples of Assessing the Effectiveness of Complex Systems" (*A.V. Rozhnov*); "Military Security as a Factor of Socioeconomic and Innovative Development of Public Systems" (*O.I. Krivosheev*); "Justification of the Urban Risks Map Project as Applied to the Current Military-Strategic Conditions in the Russian Federation" (*D.E. Fesenko*); "Mathematical Modeling of Economic Security within a Unified Digital Platform of Production Management" (*V.I. Medennikov*); "Means of Laser Space Communication Systems" (*V.V. Leshchenko* and *I.N. Panteleimonov*); "Network Cooperation Prospects in the Innovation System of the Russian Federation in New Conditions" (*N.N. Lanter*); "The Potential of a Long-Term Savings Program as a Tool for Improving the Pension Welfare of Citizens" (*A.E. Abramov*, *A.A. Sorokolad*, and *M.I. Chernova*); "Ecological Sovereignty under the Sustainable Development of Regional Mesosystems" (*R.E. Torgashev*); finally, "On the Sustainability of Investment and Loan Insurance in Microfinance" (*O.B. Bairamov*).

Methodological and applied issues of using scenario and cognitive modeling technologies as an information support tool for preparing and implementing management decisions under uncertainty and risk were the subject of several interesting papers. Among them, note the following: “Directions to Apply the Scenario Approach to the Safety Control of Organizational Systems” (*I.V. Chernov*); “Development of a Forecasting Support System Based on the Integration of Cognitive Analysis, Information Source Monitoring, and Time Series Analysis Methods” (*Z.K. Avdeeva*, *O.A. Volgina*, *E.D. Ermolaev,* and *A.A. Chereshko*); “Study of the Characteristics of Complex Systems Security Control” (*D.A. Kononov*); “Scenario Technologies for Reducing Uncertainty in Security Control” (*V.L. Shultz*, *I.V. Chernov,* and *A.B. Shelkov*); “Analyzing the Sustainability of Territorial Development: Simulation Modeling” (*G.V. Gorelova*); “The Structure, Principles, and Problems of Group Hierarchical Control of Regional Security” (*N.V. Komanich*); “Applicability of Scenario Analysis Methods in the Information Security of the Russian Federation” (*E.D. Ermolaev* and *S.V. Feoktistov*); finally, “The Influence of the Public Control System on the Protest Potential of Society” (*V.R. Feizov*).

Many conference papers dealt with the problems of information security and cybersecurity: their relevance is constantly growing in the era of rapid development of digital technologies.

R.V. Meshcheryakov, *O.O. Evsyutin*, *A.O. Iskhakova*, and *A.V. Dushkin* presented the paper “Ensuring the Information Security of Semistructured Data When Solving Information Protection Problems.” They considered the problems of improving protection mechanisms for data without a fixed format and a clear structure. As noted in the study, the heterogeneity of semistructured data, the complexity of their processing and ensuring their security, and their significant volumes require new methods for assessing information security. (By various estimates, the share of semistructured data in the total volume of corporate information reaches 80–90%.) The authors focused on the analysis of promising trends in the development of information security systems. On the one hand, such systems should provide a sufficient level of infrastructure protection and security of semistructured data considering the specifics of their acquisition, updating, processing, and analysis; on the other, they should meet definite requirements regarding the speed of processing and communication with data sources and end users.

The paper “A Method for Assessing the Information Security Risks of Complex Systems” (*N.F. Volodina*, *A.D. Kozlov*, and *N.L. Noga*) was devoted to the problems of preventing hacker cyberattacks on Russian distributed information systems and resources. The authors emphasized the growing topicality and complexity of ensuring information security due to global digitalization and incessant attacks on Russian information resources by the geopolitical adversaries. At present, the target of hacker attacks is shifting towards destabilizing the socio-political situation in the country and inflicting direct economic damage by organizing personal data leaks and disrupting (and even destroying) critical information infrastructure facilities.

In the paper, a methodology for assessing information security risks based on the mathematical apparatus of fuzzy logic and regression analysis was presented. This methodology allows determining a set of parameters affecting, to the maximum degree, the possible realization of various threats through the identified vulnerabilities in the nodes and other structural components of complex distributed information systems. In practice, the methodology can be applied to predict risk levels under uncertainty and an ambiguous risk dependence on various factors, including subjective ones. This approach increases the effectiveness of measures elaborated and implemented to prevent or reduce damage from malicious attacks on information systems in the most dangerous areas as well as minimizes the cost of measures to protect information resources.

In the paper “Development of an Analyzer Model for Phishing Attacks,” *V.M. Alekseev* and *S.N. Chichkov* considered the problem of increasing the effectiveness of information protection in corporate networks. To solve the problem, they proposed a two-level structure of an information protection system for a corporate fully connected network with different intelligent analyzers to recognize and block computer attacks. At the first (external) level, analyzers control and examine information flows at the corporate network input, detecting and preventing service denial attacks of various types, phishing attacks, attacks on applications, and other attempts to penetrate the network from the outside. At the second level, analyzers monitor activity within the corporate network, viewing traffic between the automated workstations of users and administrators, system servers, and connected mobile devices, as well as network and peripheral equipment, detecting infected devices, preventing the spread of malware, etc.

The authors developed and implemented the analyzers using the methods of statistical analysis, time series, probability theory and statistics, machine learning, optimization of network monitoring parameters and resource allocation, as well as hashing algorithms and graph algorithms to model network interactions. Also, the features of the main methods and approaches to the development of a phishing attack analyzer based on their mathematical interpretation, as well as signature and heuristic analysis technologies, were described in detail.

A large group of conference participants presented solutions of various information security and data protection problems for automated systems: *V.V. Vedischev* and *R.V. Batischev* ("An Optimization Problem Statement for Choosing the Measures and Means of Information Protection for State Information Systems"); *R.E. Asratyan*, *S.S. Vladimirova*, *E.A. Kurako*, and *V.L. Orlov* ("Features of Ensuring Technological Independence in the Development of Systems with Service-Browser Architecture"); *A.D. Domashkin* and *L.N. Loginova* ("A Comparative Analysis of Machine Learning Algorithms for Anomaly Detection in Information Systems"); *M.V. Vedmedeva* and *V.G. Mironova* ("Information Systems Evolution: from Simple Solutions to Complex Infrastructures"); *L.E. Mistrov* ("Foundations of Justifying an Information Security Criterion for Organizational and Technical Systems"); *A.A. Shiroky* ("An Express Risk Assessment Method for a Computer Network with the Star Topology"); *I.A. Andronov* and *V.G. Sidorenko* ("Advantages of Artificial Intelligence Application When Working with Documents in terms of Information Security"); *A.A. Sidorenko* and *Yu.R. Tedeev* ("Increasing the Information Security of Control Channels by Applying Corrective Codes"); *A.Yu. Iskhakov* and *M.V. Mamchenko* ("A User Authentication Algorithm Based on Behavioral Analytics and Machine Learning for Web Resources"); *A.G. Uimin* ("A Continuous-Discrete Biometric Identification System Based on Analysis of the Computer Mouse Data Flow"); *A.A. Salomatin* ("A User Authentication Algorithm Based on Static Characteristics of Computer Hardware"); *A.G. Cheban* and *E.A. Anisimova* ("The Principles of Organization and Design of Secure Videoconference Systems"); *L.N. Loginova* and *A.D. Drozdov* ("Analysis of Information Security Threats When Using Telegram Bots in Business"); *V.P. Kuminov* and *V.G. Sidorenko* ("Analyzing the Cryptographic Resistance of Pseudorandom Number Generators Using Machine Learning"); *D.I. Pravikov* and *V.A. Murashkin* ("Approaches to the Quantitative Assessment of Information Security at an Enterprise of the Fuel and Energy Complex"); *V.O. Sirotyuk* ("Increasing the Security of Digital Intellectual Property Management Systems"); finally, *S.K. Somov* ("Methods for Reducing the Computational Complexity of Optimal Data Array Allocation Algorithms in Distributed Data Processing Systems").

Also, many conference papers were traditionally devoted to the problems of preventing and eliminating the consequences of natural and man-made emergencies as well as ensuring the safety and reliability of transport systems.

In the first thematic group, note the following papers: "Statistical Observation Forms for Hydrological Situation in Settlements During Floods Caused by Heavy Precipitation" (*V.A. Akimov*, *D.V. Buryak*, and *E.O. Ivanova*); "On Managing the Individual Risk of Death and Health Damage in Emergencies Caused by Catastrophic Floods" (*I.Yu. Oltyan*); "Statistical Observation Forms for Fire-Prevention Situation in Forest Areas" (*V.A. Akimov*, *E.O. Ivanova*, and *M.A. Pulikov*); "Feedback During the Audit of Industrial Safety Control Systems" (*V.A. Tkachenko*); "An Attack on Robotic Systems as a Method of Information-Technical Impact" (*V.A. Zorin*); "Numerical Modeling of a Concentrated Vertical Explosive Impact on a Slab with a Solid Foundation" (*V.K. Musaev*); finally, "Vibroacoustic Diagnosis Methods for Equipment" (*O.B. Skvortsov* and *V.I. Stashenko*).

Several conference participants considered the problems of ensuring the safety of transport systems and objects: *E.A. Kuklev* and *D.M. Mel'nik* ("Intellectual Decision Support in Flight Safety Control of Civil Aircraft Providers Based in Scenario Modeling of Rare Events"); "Ensuring the Safety of Train Traffic under the Coordinate Interval Regulation Method" (*V.G. Novikov*); "A Decision Support System in Technical Re-equipment Problems of the Railway Industry" (*S.V. Makshakov*); "A Distributed Sensor Model with Multi-Fiber Multiplexing to Monitor the Location of Rolling Stock" (*V.M. Alekseev* and *D.N. Khusenov*); "Increasing the Safety of Subway Traffic under Compensated Disturbances" (*L.A. Baranov* and *Yungqiang Zhang*); "Application of Augmented Petri Nets to Model the Automated Scheduling of Subway Trains" (*A.I. Safronov*); "Application of PNETLab to Model Intelligent Water Transport Systems" (*N. D. Ivanova* and *I.F. Mikhalevich*); finally, "The Concept of Developing a Trusted Operation Environment for Autonomous Shipping Objects" (*L.A. Baranov*, *I.F. Mikhalevich*, and *S.S. Sokolov*).

The conference proceedings are published electronically[1] and are also available at the official website: https://iccss2024.ipu.ru/prcdngs.

The 33rd International Conference on Problems of Complex Systems Security Control is planned to be held in November–December 2025 at ICS RAS. The conference schedule will be announced in the information letter of the Organizing Committee, which will be published on the official website (https://iccss2025.ipu.ru/) as well as distributed to po-

[1] *Materialy 32-oi Mezhdunarodnoi konferentsii "Problemy upravleniya bezopasnost'yu slozhnykh sistem"* (Proceedings of the 32nd International Conference on Problems of Complex Systems Security Control), November 13, 2024, Moscow, Kalashnikov, A.O. and Chernov, I.V., Eds., Moscow: Trapeznikov Institute of Control Sciences RAS, 2024. (In Russian.)

tential 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

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

Cite this paper

Shelkov, A.B., 32nd International Conference on Problems of Complex Systems Security Control. *Control Sciences* **1**, 45–50 (2025).

Original Russian Text © Shelkov, A.B., 2025, published in *Problemy Upravleniya*, 2025, no. 1, pp. 53–59.

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