DOI: http://doi.org/10.25728/cs.2023.1.6

30TH INTERNATIONAL CONFERENCE ON PROBLEMS OF COMPLEX SYSTEMS SECURITY CONTROL

In December 2022, the 30th International Conference on Problems of Complex Systems Security Control took place at Trapeznikov Institute of Control Sciences, Russian Academy of Sciences (RAS), Moscow. The conference was organized by the Ministry of Science and Higher Education of the Russian Federation, Trapeznikov Institute of Control Sciences RAS, Keldysh Institute of Applied Mathematics RAS, the RAS Scientific Council on the Theory of Controlled Processes and Automation, and the Ministry of the Russian Federation for Civil Defense, Emergencies and Elimination of Consequences of Natural Disasters.

Note that 30 years have passed since the first conference on the topic. Initially, this annual scientific event was conceived as a conference on the problems of control and management in emergencies due to the high relevance of such problems in the 1990s. According to the conference organizers, the main task was to develop theoretical and methodological foundations for improving the efficiency of public administration systems in emergencies as well as design and implement rapidly deployed information systems for the timely and uninterrupted operation of specialized structural departments and services.

The topics of the conference papers began to expand significantly with the course of time, following the appearance of new pressing problems related to the sustainable and secure development of Russia.

Several new lines of research arouse in this field and the adjacent ones, including the following: planning, organization, and automation of technogenic security management processes; information support methods and technologies for decision-making in emergencies; general theoretical and methodological problems in the integrated security of complex organizational systems; problems of social, economic, political, regional, environmental, and public security management; management of geopolitical information confrontation; scenario analysis methods for the development of socio-economic systems under uncertainty and risk; simulation and scenario modelling technologies; information security and cybersecurity (protection methods and technologies for telecommunications and networks, computer-aided systems, software, and data against remote attacks, damage or unauthorized access), etc.

As a result, in 1998 the conference was given its current name and the composition of conference sections was significantly expanded. With few exceptions, the sections have remained unchanged in recent years.

Over the past 30 years, the annual conference has become a platform for discussing research results and exchanging experience on a wide range of fundamental and applied problems in the field of security control in the face of new challenges and threats of different nature. The situation in Russia and the world has been determining the main lines and topics of research, reflected in the conference papers.

A distinctive feature of the conference was the growing interest of the participants in a wide range of theoretical and applied problems to improve the effectiveness of security control of individuals, society, and the state in modern realities.

The conference was attended by 99 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.

According to an established tradition, the conference was opened with a detailed paper, “Military conflicts and industrial policy in the context of risk man-

agement theory," by *G.G. Malinetskii* and *V.V. Kul'ba*. It was devoted to a wide range of problems faced by Russia nowadays. As stated by the authors, the sphere of geopolitical confrontation between Russia and Western countries has significantly expanded in recent years. There is an active struggle not only on the battlefield with conventional weapons but also in cyberspace and information space, in the realm of meanings and values, and in biological space (a great danger to humanity). The paper emphasized that victory in the military-political (more broadly, civilizational) conflict between Russia and Western countries requires the consolidation of Russian society; moreover, each citizen must realize that the current, formally undeclared, war with NATO countries is everyone's business. The future of Russia is largely determined today.

Based on the analysis results, the authors gave detailed proposals on countering external threats and the main directions of Russia's development in the current extremely difficult conditions. In particular, the industrial, scientific, and technical policy of the country should agree with the new challenges, and structural changes should be made in the public administration system to concentrate resources and efforts on the most important (key) areas of Russia's development in the face of confrontation with NATO countries and harsh economic sanctions.

Undoubtedly, several conclusions and proposals of the paper are debatable, and some require further deep interdisciplinary studies. At the same time, an active discussion on many relevant and urgent problems touched by the authors would be useful for the domestic scientific community.

The paper "Tools of influence and aggression of the global capital center under growth limits" by *V.V. Tsyganov* considered manipulation mechanisms for the consciousness of citizens of Western countries (including Russia's neighbors) based on the neuropsychological model of an individual. In this model, an individual is treated as an active element of the socio-economic system. Manipulation mechanisms for the desires and fears of citizens were analyzed as a basic tool of information-psychological influence. According to the author, when realizing their desires to accumulate financial means, the individuals in the consumer society actually form local capital centers. (In the global financial openness conditions, the matter concerns a global capital center (GCC), currently located in the USA.) However, since the global growth limits in the 21st century restrict consumption (even in the GCC-hosting country), the capital center is forced to reduce the severity of mass discontent. To this end, tools are used to expand these growth limits by using external sources of cheap resources of the so-called periphery countries of the global financial system, particularly by taking over their markets. At the same time, to counteract the manifestations of discontent of individual consumers and retain power, the GCC uses fear management mechanisms: forming the image of an external enemy and supporting the manifestations of nationalism (national exclusiveness), including its most aggressive form (nazism, also called national socialism).

Note that the practical operation of such mechanisms is well illustrated, in particular, by the "pull" of manufacturing companies from the EU to the USA and the "grain deal" used mainly to import food to EU countries instead of needy countries (expanding the growth limits), the rise of nationalist and far-right movements in Western Europe, and the information policy of Western countries (fear management) blaming all their problems on Russia.

The paper "Management of Law Transformation Processes under Digitalization Based on a Scenario Approach" by *V.L. Shultz*, RAS Corresponding Member, and his colleagues was devoted to improving the efficiency of legal norms regulating digital relations and assessing their impact on the processes of socio-economic development of the state and society. As noted therein, large-scale digitalization of almost all aspects of human life inevitably leads to several fundamental changes due to the emergence of new problems and threats to the security of individuals, society, and the state rather than the growth of circulating information. The problems of improving the effectiveness of legal norms regulating inter-subjective relations in the digital environment become particularly relevant during an open information war with the countries of the collective West.

According to the authors, assessing the effectiveness of legislative acts is an extremely difficult and complex problem due to the following objective reasons: high-level uncertainty and the "informational fuzziness" of such objects; significant inertia of the socio-economic system response to the decisions made to improve the processes of legislative regulation; limited practical experience in addressing many legal problems associated with the development of high technology, and others. All these conditions increase the role of creating effective and, at the same time, fairly universal methods and mechanisms of anticipatory scenario assessment (expertise) of the effectiveness of legal acts developed. The approach proposed by the authors involves simulation models to analyze a wide class of processes and phenomena in the political-legal, socio-political, socio-economic, and innova-

tive-technological spheres as well as in the environment. To assess the effectiveness of legal regulation, the idea is to use criteria reflecting the degree of achieving the goals set in the course of lawmaking, particularly by comparing them with the real results.

The problems of ensuring technological sovereignty and economic growth under large-scale external sanction pressure and the withdrawal of foreign businesses from Russia were addressed in the paper "Analysis and assessment of the criticality level of industrial and corporate failures in the sanctioned economy of Russia" by *N.I. Komkov* and *N.N. Lanter*. According to the authors, after the withdrawal of foreign companies from 70 countries representing competencies in 55 different industries, there was an imbalance in the production sector of the national economy. As a result, the industry markets were transformed. In fact, a significant layer of technological competencies and logistical know-how dropped out of Russia's economy, which changed the quality of produced goods and services and also damaged the national intellectual capital due to the increased outflow of professionals abroad. Nevertheless, as noted in the paper, the potential of import substitution as a tool for "debottlenecking" remains significant; many technological links dropped out can be successfully replaced in a short time by Russian or available foreign analogs, particularly through an active search for new trade and technological partners.

In the current situation, the authors argued, achieving Russia's technological sovereignty in the long term should become the main goal of all levels of the state development management system. It requires the mobilization of resources within the program-target approach to ensure economic growth in the face of current and future challenges. To solve this problem, the authors developed a methodological tool to enhance Russia's competitiveness potential based on the information-logical model of import substitution within the full life cycle of the technological chain of innovation reproduction.

In general, a wide range of operational and long-term tasks to ensure the secure and sustainable development of the country in an extremely difficult geopolitical and economic situation were considered in many papers on various topics, including the following papers: "Science and education as objects of control of complex systems" by *G.G. Malinetskii*, *T.S. Akhromeeva*, *S.A. Toropygina*, and *V.V. Kul'ba*; "On Russia's civilization security" by *R.Yu. Leshchenko*; "Information confrontation scenario modeling with an asymmetric influence on small groups" by *M.E. Stepantsov*; "Scenario modeling of innovation development of Russia's Arctic zone under external threats" by *N.V. Komanich* and *I.V. Chernov*; "Qualitative approaches to import substitution strategies modeling at the sectoral and inter-sectoral levels" by *M.V. Krotova*; "Detection of changes in socio-economic situations based on heterogeneous information" by *Z.K. Avdeeva* and *S.V. Kovriga*; "The concept of energy pseudo-security as genesis of the global economic crisis" by *A.N. Fomichev*; "Organization of an employee training system to counteract social engineering mechanisms" by *A.A. Ryzhenko*; "Management strategy and tactics for national economy security" by *V.V. Kafidov*; "The uncertainty problem in the study of law enforcement" by *D.A. Kononov*, *A.A. Timoshenko*, and *L.V. Bogatyreva*; "On development trends of microfinance in Russia" by *O.B. Bairamova*.

The paper "Modeling of air accidents based on analysis of a fuzzy set of data and events of aircraft operators" by *D.M. Mel'nik* was devoted to the problems of flight safety, aggravated under the sanctions announced by Western countries against Russian civil aviation. The flight safety method proposed in the paper involves the risk-oriented approach. According to the author, in contrast to traditional methods based on the averaged estimates of numerous indicators, this method determines the acceptable level of risk for a complex production system of air transport operators. The approach under consideration rests on fuzzy set theory; in a complex integrated production system of air transport operators, it yields reliable flight safety estimates as well as provides opportunities to model and study forecasted scenarios of possible air accidents and disasters to develop preventive measures. The scenarios are developed by analyzing two basic groups of indicators related to the quality of production processes and aircraft flight safety, respectively. These tasks are solved using the results of systematic complex monitoring activities of the production system (the information base), including audit procedures, inspections and qualification checks, the evaluation of production and safety indicators, flight information analysis, investigation of aviation events, etc.

Traditionally, the conference participants are interested in the problems of technogenic security and emergency response management, as evidenced by many papers on various related topics: "The problem of cybersecurity of critical facilities in an untrusted environment" by *V.G. Promyslov* and *K.V. Semenkov*; "On the safety of radio-probing of the ionosphere by powerful wave beams" by *V.A. Eremenko* and *N.I. Manaenkova*; "About the objectivization of expert assessments for the probabilities of rare events" by

M.Yu. Prus, *M.S. Zhubanov*, *I.A. Lobanov*, and *Yu.V. Prus*; "Mathematical modeling of impact (transient process) on a ten-storied building with basement" by *V.K. Musaev*; "Towards higher safety of designing natural-technical systems" by *D.I. Katsko* and *A.I. Katsko*; "On one approach to increase the industrial-technological safety of managing complex industrial objects" by *V.O. Chinakal*; "An approach to ensure the fulfillment of functions and tasks in a complex technical system" by *O.M. Lepeshkin*, *M.A. Ostroumov*, *O.A. Ostroumov*, and *V.V. Kulakov*; "On technosphere safety management" by *K.V. Chernov*; "Forecasting of an optimal service area using geoinformation modeling" by *S.Yu. Karpov*; "High-frequency vibration: diagnosis and fatigue" by *O.B. Skvortsov* and *V.I. Stashenko*; "Emergency response management support considering the opinion of experts of crisis management centers" by *R.Sh. Khabibulin* and *Sh.K. Kadiev*; "Mathematical models and methods of transport systems safety management" by *V.G. Sidorenko*; "Analysis as a tool to improve the management system of industrial safety and labor protection" by *E.V. Klovach* and *V.A. Tkachenko*; "Real-time monitoring of the fire protection condition of an object" by *D.V. Shikhalev*; "Analysis of physical and chemical properties of aerosols intended for testing fire detectors" by *A.V. Panasenko* and *M.A. Vasil'ev*.

Many interesting papers were devoted to a wide range of problems of information and cybersecurity management: "A digital platform of information scientific and educational resources as a tool to achieve a given level of information security and data reliability" by *V.I. Medennikov*; "Detection of heterogeneous manifestations of cyber attacks on examples of web resource analysis" by *A.O. Iskhakova*; "An approach to creating secured network tunnels in distributed systems based on Cryptographic Message Syntax (CMS)" by *R.E. Asratyan*; "On the security of domestic software" by *E.A. Kurako*; "Vulnerability analysis of RFID tags in access control systems of critical information infrastructure objects" by *E.A. Nenasheva*; "Information security principles in social networks" by *L.N. Loginova* and *A.D. Korolev*; "Query analysis in application level protocols during the enhanced authentication of access subjects" by *A.Yu. Iskhakov*; "Principles of open network multi-key matching" by *A.D. Sinyuk* and *A.A. Tarasov*; "Requirements management, verification and validation of software in industrial control systems of nuclear power plants" by *E.F. Jharko*; "Advantages and drawbacks of classical face identification methods" by *Yu.V. Timirshayakhova* and *N.A. Shagin*; "The method of averaged influence coefficients for forming a fuzzy knowledge base during information security risk assessment" by *A.D. Kozlov* and *N.L. Noga*; "Critical information infrastructure assessment: cyber targets and criticality evaluation" by *E.A. Abdulova*; "Document storage, information security aspects" by *N.D. Khodnev* and *A.E. Krasnov*; "Influence of magnetic media archives on some reliability indices of distributed data processing systems" by *S.K. Somov*; "A method to justify the information security tasks of organizational and technical systems" by *L.E. Mistrov*; "The development of automated means for detecting potentially dangerous configurations of the information system of a small enterprise" by *D.A. Eronin* and *A.A. Melikhov*; "Analysis of hardware characteristics for information security tasks" by *A.A. Salomatin*.

The papers can be found in the conference proceedings[1] or on the official conference website: https://iccss2022.ipu.ru/.

In his closing remarks, the Conference Chair, Dr. Sci. (Eng.), Prof. *V.V. Kul'ba* announced plans to hold the 31st Anniversary International Conference on Problems of Complex Systems Security Control, according to the established tradition, in December 2022 at Trapeznikov Institute of Control Sciences RAS. 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 *Alla 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

Cite this paper
Shelkov, A.B. 30th International Conference on Complex Systems Security Control. *Control Sciences* **1**, 48–51 (2023). http://doi.org/10.25728/cs.2023.1.6

Original Russian Text © Shelkov, A.B., 2023, published in *Problemy Upravleniya*, 2023, no. 1, pp. 59–64.

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 30-oi Mezhdunarodnoi konferentsii "Problemy upravleniya bezopasnost'yu slozhnykh sistem" (Proceedings of 30th International Conference on Complex Systems Security Control), December 14, 2022, Moscow, Kalashnikov, A.O. and Kul'ba, V.V., Eds., Moscow: Trapeznikov Institute of Control Sciences RAS, 2022. (In Russian.)