# METHODS AND MODELS FOR EFFECTIVE INFORMATION SYSTEMS RISK MANAGEMENT

**Nemchaninova S.V., Minzov A.S.[1]**

Dubna State University, 19 University St., Dubna, Moscow Region, 141982, Russia, +79175156807, sbobylova94@gmail.com
[1]Dubna State University, 19 University St., Dubna, Moscow Region, 141982, Russia, +79265650570

Active implementation of information technologies in all spheres of our society and the implementation of the national program for the digital economy have led to a significant increase in the number of information systems.

Practical experience in using various information systems has shown that they are not always used effectively, are susceptible to various risks from the internal and external operating environment, technical and software failures, and vulnerability to cyber threats. The consequences of these risks for the state and society can be significant, especially for critical information infrastructure and socially significant objects. Hence, there is a need to study methods and technologies for managing the most important risks to improve the efficiency of these information systems.

The concept of "business continuity" is considered as the "strategic and tactical ability of an organization to plan its work in case of incidents and disruptions to its activities, aimed at ensuring the continuity of business operations at an acceptable level." General approaches to creating a system for ensuring the continuity of information system operations have been outlined in a regulatory document. The standard is based on known practices and is presented in the form of recommendations. This approach does not allow for detailed consideration of specific issues related to the selection of protection, recovery, management, and monitoring measures for ICT. Another feature of this standard is that it also applies to information security management systems. The standard implements a risk-oriented approach to incident prioritization. However, the risk methodology used only solves one task: establishing risk priorities based on relatively coarse classifications in the form of linguistic variables. The use of fuzzy set mechanisms does not provide confidence in the results because the obtained risk parameter values cannot be compared with anything, and there are no methods for assessing their error. This prevents solving tasks related to evaluating the effectiveness of risk-oriented ICT recovery methods and their optimization.

Thus, the existing level of methodological support for the continuity of information system operations does not allow for the automation of these processes due to the lack of parametric management models for information risks and uncertainty in the initial data.

**References.**

1. *Decree of the Government of the Russian Federation dated December 29, 2021 No. 2531 "On the Approval of the Rules for Maintaining a List of Domestic Socially Significant Information Resources."*
2. *GOST R 53647.22009: Business Continuity Management.*
3. *GOST R ISO/IEC 27031-2012. Information technology. Security techniques. Guidelines for information and communication technology readiness for business continuity.*