To the Risk Management section

Cybersecurity risks

Managing information security risks is an essential priority. If they materialise, information security threats may disrupt or suspend IT services, the process flow and operations of the Company, including leakage of restricted information.

The main risk factors related to the security of Russian Railways' information infrastructure include tampering by third parties to gain unsanctioned access to the information of the Company and its counterparties, including hacker and virus attacks, as well as internal threats of employee misconduct and analysis and SIEM tools failure.

The key information security measures implemented by Russian Railways include:

- classification and categorisation of Russian Railways' systems, information security threat modelling, development of information protection requirements (based on the classification of information assets, information security threats, and the requirements of applicable Russian laws on information protection);
- proper arrangement of information infrastructure components with due account of information security, design and implementation of relevant protection systems in the Company's information infrastructure, assessment of Russian Railways' systems for compliance with information security requirements;
- employee training in information protection
- ensuring the security of Russian Railways' information systems in use, identification and handling of information security incidents, conducting internal investigations into information security violations;
- arrangement of the Company' workflow with due account of information security requirements;
- enhancement of the Company's information security policies and guidelines.

Risk management initiatives in 2021 included:

- development of functional requirements to set up a single centre for monitoring of Russian Railways' information security;
- implementing initiatives aimed at developing access control hardware and software for privileged and other users;
- taking steps to analyse the security level (penetration tests, security control, source code analysis) and ensure compliance with information security requirements when developing and running Russian Railways' systems;
- developing Russian Railways' information security management system and its components, including the anti-virus protection system and the migration of the Information Security Management System of Russian Railways to a new platform, as well as implementation of the Targeted Attack Protection System, the Information Transmission Monitoring and Control System, and the Security Control System hardware and software.

Risk management initiatives planned for 2022:

- improving Russian Railways' internal regulations on information security;
- developing the Information Security Management System of Russian Railways, developing and implementing the ID Management System, rolling out the Information Transmission Monitoring and Control System, and privileged/other access control hardware and software;
- implementing the framework to set up a single centre for monitoring of Russian Railways' information security;
- implementing information security systems for standard data processing centres of Russian Railways; upgrading of the centralised node of access to information systems of Russian Railways;
- implementing Perimeter, the DoS attack prevention hardware and software product.