6.9. CYBERSECURITY

In 2020, to conform with the requirements of Federal Law No. 187 On the Security of the Critical Information Infrastructure of the Russian Federation dated 26 July 2017 and regulations thereunder, measures at Transneft Group subsidiaries were taken to:

- improve the management and organisational structure of information security units;
- introduce end-to-end processes to ensure the security of critical information infrastructure at all lifecycle stages;
- develop a regulatory framework for the security of critical information infrastructure facilities;
- develop and implement standard technical solutions to protect information at critical information infrastructure facilities.

As part of the information security processes optimisation, including counteracting hacker attacks in 2020, the following measures have been implemented:

- provision of secure remote access to information resources for employees under the quarantine measures;
- development of the information security perimeter protection system;
- improvement of information resources security, including against distributed denial-of-service attacks;
- improvement of technical policy in terms of creating information security systems and accelerating the implementation of projects in the field of information security;
- updating regulatory documents on the protection of information processed in information and automated systems;
- re-engineering processes for managing vulnerabilities and information security incidents;
- improvement of interaction with the Russian State System for Detection, Prevention, and Mitigation of Computer Attacks (GosSOPKA);
- raising the personnel awareness around information security issues;
- conducting emergency response drills with a variety of hacker attack scenarios to exercise the emergency protocols with information security units, console operators and automation systems maintenance personnel

In 2020, the hacker attacks on the informational resources of Transneft Group subsidiaries were repelled and did not lead to failure of automated and information systems.

As part of ensuring cybersecurity in 2021, great attention will be paid to:

- compliance with legislation of the Russian Federation on security of critical information infrastructure, personal data and trade secrets;
- improving the information security management structure;
- development of technical measures to protect information;
- optimisation of regulatory and methodological documentation to ensure information security;
- increasing the level of information resources security, centralising information security systems.