PROTECTION AND SECURITY OF INFORMATION

INFORMATION SECURITY

GLOBAL TRENDS OF THREATS IN THE SPHERE OF INFORMATION SECURITY

In 2019, the information security divisions of MTS PJSC successfully implemented a set of organizational and technical measures that made it possible to ensure that the management and information security systems comply with the legislative requirements of the Russian Federation, the requirements of international standards, the current level of cyber threats and to prevent financial, reputational and other damage to the MTS Group.

In 2019, the most interesting goals for cybercriminals included: information assets (arrays) with personal data and telemetry of consumers of communication services, financial transaction data, know-how in the field of big data processing methods and artificial intelligence, information of limited access.

According to experts in the Company, the vector of attacks of 2019 will continue in the near future and target corporate information systems for managing, processing and storing information. The main areas of growth for cyber-tension for the corporate sector:

- The development of methods and forms of targeted attacks (Advanced Persistent Threat) based on artificial intelligence technologies and deep learning.
- Social engineering and direct recruitment of company personnel.
- Attacks on the corporate segment using user terminal equipment connected into managed intelligent botnets.
- Insufficient security and vulnerability of cloud services and solutions for the implementation of the secure Internet of Things (IoT) of domestic production.
- The presence of vulnerabilities in the program code of commercial and proprietary IT solutions.
- The use of personal mobile equipment of employees who do not have sufficient means of protecting information to access restricted information.
- Remote work of employees, increasing the risk of unauthorized access to corporate protected assets.

In the legislative sphere, we should expect a continuing trend in the extension of mandatory information protection measures to non-state information resources (personal data, professional and commercial secrets, public communications networks, critical information infrastructure facilities, etc.).

INFORMATION SECURITY RISKS

Risk	Description / Risk Factors
Risk of information security breach	Violation of the confidentiality, integrity or accessibility of information due to the inconsistency of the information-protection system with current information-security threats, failure by administrators and users of information systems or partners of MTS PJSC to fulfill the company's information security policy. As a result, possible damage arises due to leaks of information constituting a commercial secret, claims of individuals or partners due to violation of personal data security, communication secrets, commercial secrets of partners or other restricted information.
Information security regulatory risks	Sanctions of controlling bodies or negative conclusions of auditors (the General Prosecutor's Office, the Ministry of Communications, Roskomnadzor, FSTEC and FSB of Russia, controlling bodies of the countries where we operate, SOX, PCI DSS auditors, etc.) due to the failure to comply with the requirements of Russian, international or national legislation for information security protected by laws in the countries where we operate. Moreover, the laws establish different IS requirements for one-and-the-same object of regulation, which may differ. In this case, no priority of laws is established.
Information security contract risks	Refusal to conclude state or other contracts due to failure to comply with competitive conditions for information security (no FSTEC and FSB licenses, Russian or international certificates for IS processes and systems, IS infrastructure required for providing services, etc.)

INFORMATION SECURITY SYSTEM AT MTS

- MTS' information protection system is a unified complex of interrelated organizational and technical actions, with centralized infrastructure and information-security management and support processes unified in MTS Group. The system has been built with consideration of the best global practices on the basis of international standards of the ISO 27000 and 15408 series.
- The personal data protection system provides for the third level of PD protection in accordance with the legislation of the Russian Federation.
- Protection of secrecy of communication in communication networks with information-protection mechanisms built into communication facilities meets the international communication standards and requirements of the industry regulator.
- MTS PJSC is a licensee of FSTEC and FSS of Russia for operations of technical and cryptographic protection of confidential information and monitoring of IS events, and may provide the corresponding services.

2019 RESULTS AND ACHIEVEMENTS:

- The British Standards Institution for the first time certified the corporate information security management system of MTS PJSC for compliance with the international standard ISO/IEC 27001: 2013 INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS – REQUIREMENTS and issued Certificate No. IS 719403. It also expands the opportunities for the company to participate in competitions and tenders focused on international information security standards.
- In 2019, the security forces prevented damage to the business (financial, reputation or otherwise) as a result of cyber attacks on the company.
- Continuity of all business and technological processes is provided in accordance with the requirements of regulators, shareholders and management of MTS PJSC.
- The number of clients of a commercial service for monitoring and responding to information security incidents has been increased.

- In order to fulfill the requirements of the Federal Law of July 26, 2017, No. 187-FZ "On the Safety of Critical Information Infrastructure of the Russian Federation," the following measures were taken in 2019:
  - a commission was created to categorize critical information infrastructure (CII) facilities of MTS PJSC;
  - categorization of MTS PJSC CII facilities was carried out in accordance with the methodology of RF Government Resolution No. 127;
  - a list of MTS PJSC CII facilities has been approved and sent to the FSTEC of Russia; and
  - a technical project has been developed to create a security system for MTS PJSC CII facilities.
- Support was provided for the new management structure of the Company through the unification of the process of developing the information security requirements, the accounting of protection objects and their characteristics was organized.
- In order to ensure the failure-proof operation of special complexes installed on the MTS PJSC network, actions are organized and held on a permanent basis to prevent and support the equipment and software.
- As part of fulfilling the tasks of implementing the requirements of Federal Law No. 374-FZ, work is underway on the network of MTS PJSC to implement special complexes in accordance with the concept and deadlines for implementing the Law agreed upon with the Federal Security Service (FSB) of Russia.
- Special equipment has been installed on communication networks, the presence of which provides the ability to provide new services and services: NB IoT, MTS Connect, WiFi Calling, VoLTE/ViLTE, WiFi for Business, Virtual PBX.
- Work on the modernization of the special equipment supporting the activities of authorized state bodies was carried out on a scheduled basis, in accordance with the approved investment program, in strict accordance with the requirements of the regulatory legal acts. Scheduled events were held in full.

THE MAIN OBJECTIVES IN THE FIELD OF MANAGEMENT AND ENSURING INFORMATION SECURITY FOR 2020

- Ensuring compliance of the Information Security Management System of MTS PJSC with the international standard ISO/IEC 27001: 2013.
- Improving measures and means of information protection simultaneously with the process of introducing new information technologies.
- Monitoring compliance with the requirements for certification of equipment and software of information protection under the standards of FSTEC and organization of certification in accordance with the requirements of FSTEC and FSS of Russia for the latest information security tools while ensuring the protection of personal data.
- Implementation of protection measures established by regulatory legal acts of the Ministry of Communications, FSTEC and the FSB of Russia, which provide a minimum sufficient level of information security.
- Participation in the work of regulators, public organizations, and the Digital Economy NCP to improve information security legislation.
- Creation of a security system for MTS PJSC CII facilities.

An important element in maintaining a high professional level of specialists in the field of information security of the Company is their training in special educational institutions, improving professional skills, expanding and deepening the quality of knowledge, which is achieved by participating in thematic events, including international ones, and targeted retraining in specialized courses. In 2019, retraining was conducted according to the standards of information security of higher professional education of 16 employees of the Company. Prepared by 3 leading auditors according to ISO 27001:2013..

ECONOMIC SECURITY

In 2019, the Economic Security and Anti-Corruption Units of MTS PJSC successfully implemented a set of measures that made it possible to protect the vital interests of MTS Group of Companies from internal and external economic threats.

In 2019, emphasis was placed on the implementation of the following areas of development:

- assistance in increasing the efficiency of business processes and procedures in the interests of increasing business profitability while using the minimum necessary barriers to guarantee the prevention of damages and losses;
- improvement of contractors' verification mechanisms;
- development of a sustainable system for ensuring HR security of the Company;
- increasing the return on the formed system of measures to minimize and recover overdue receivables; and
- studying and applying the experience of the economic security departments of other key telecom operators for the Company's economic security.

In order to ensure the economic security of the Company for 2020, the following priority objectives are set:

- improvement of the functionality of internal security;
- organization and implementation of measures to prevent manifestations of corruption;
- analysis and control of investment project preparation;
- improvement of the verification of counterparties before concluding agreements and contracts;
- checking candidates before employment;
- taking part in the activities to collect, minimize and prevent overdue accounts receivable; and
- verification of execution of contracts concluded as a result of procurement procedures;

In 2019, the efficiency of the work to protect the economic interests of the Company increased, which, in turn, had a positive impact on the performance of other structural divisions.

On an ongoing basis, support was provided for the processes of procurement and contractual activities, and implementation of investment projects. The employees of the security departments participated as experts at all stages of the procurement procedures, which allowed to gain a significant economic effect.

Information was collected about legal entities participating in the process of procurement procedures for purchasing products, works and services. At the same time, financial and economic activities of potential contractors were analyzed, and a conclusion was drawn about their reliability. Upon receipt of information about problems with contractors (decision on liquidation, bankruptcy claim, lawsuits, etc.), information was transferred to the Procurement Management Unit. Problem contractors were entered into the "List of Problem Suppliers," which blocked the possibility of concluding new contracts with them.

Work was done on studying candidates for jobs, rejecting those who do not meet the requirements, and is also a member of the List of Organizations and Individuals for which there is information about their involvement in extremist activities or terrorism.

Together with the structural divisions of the Revenue Management Department, employees of the economic security and anti-corruption divisions took part in the work to recover overdue receivables. Delays in performance of contractual obligations were monitored and analyzed on an ongoing basis. The location of the problem counterparties, and, if necessary, their liquid assets, was established.

Primary claims activities were carried out at the stage of the pre-trial negotiation process to recover problem receivables.

Taking into account the successful experience of engaging security units to recovery of the Company's funds, in 2019 a new business area began to develop – claiming VAT with the participation of Department personnel.

In 2019, the Department carried out significant work to organize the fight against fraudulent activities using SIM cards to gain access to remote banking services. An effective system of measures has been implemented to identify and combat the facts of unlawful replacement of SIM cards by MTS PJSC subscribers for the subsequent theft of funds from their bank accounts. Constant monitoring was organized using the Intellinx system, which can significantly reduce the risks of theft of funds from the bank accounts of MTS PJSC' subscribers.

Work was carried out to combat corruption – the prevention and prevention of corruption, the identification and suppression of corruption offenses related to causing both material and image damage to the Company.

Work of the anti-corruption security units was carried out in close cooperation with the Internal Control and Audit Unit (ICAB). Within the framework of the Unified Hotline of MTS Group, which is curated by BVKA, the Unified Hotline of the Corporate Security and Regime Unit (CSRU) operates. Company employees are informed about the existing opportunity to report of corruption offenses.

A special place was taken by the events held by the economic security and anti-corruption units, together with other functional units of the Company, related to the prevention of financial and reputational risks for the MTS Group.

To ensure maximum security from these threats, a well-coordinated and effective protection system has been built that allows you to:

- forecasting of possible threats in the field of economy;
- organization of activities to prevent possible threats;
- identification, analysis and evaluation of the real emerged threats to economic security;
- decision-making and organization of measures to respond to emerging threats; and
- continuous improvement of the Company's economic security system.

Within the scope of development of the Unified Complex Security Center at the Company, the security system was developed, and improvements were made to the following business processes:

- the process of checking candidates and current employees in the List terrorists/extremists has been automated;
- changes were made to the Code of Business Conduct and Ethics;
- interaction with state authorities, the project of an automated system for the execution of law enforcement agencies and court requests is being implemented;
- safety of subscription service processes, observance of communication secrets;
- a database has been created for storing and exchanging information between security divisions of the MTS Group; and
- a project is being implemented to automate the system for studying and monitoring contractors in conjunction with the Big Data unit using state-of-the-art approaches and methods, including agile.

SAFETY OF PERSONNEL AND OBJECTS

The anti-terrorist protection and security of facilities was provided in accordance with the Strategy of MTS Group in the field of integrated security for 2019–2020, as well as the "Plan of measures for ensuring integrated security of MTS PJSC for 2019."

Work on ensuring access control and on-site regimes in MTS PJSC was based on the Standard "Requirements for ensuring the safety of facilities, conducting comprehensive inspections on civil defense, emergency situations and fire safety at the facilities of MTS PJSC. Access control at the facilities of the Company was carried out by the employees of SAFETI LLC using engineering and technical security equipment: access control and management systems, CCTV, signaling, communications, and fencing systems.

In 2019, in order to study the possibility of using the face recognition function to access the facilities of MTS PJSC, a pilot project was implemented to recognize the faces of MTS PJSC employees in the Moscow Region.

Since June 2019, employees of the Moscow region have had the opportunity to use the smartphone as the pass using the Mobile Pass service.

In order to prevent the occurrence of vandalism and theft of inventory at the facilities of the radio subsystem and to maintain uninterrupted communication services, activities were continued to ensure the continuity of operation of the highest priority BS due to a significant increase in their equipping with security equipment.

In 2019, at the facilities of MTS PJSC, anti-terrorism trainings and exercises were regularly held with the participation of the Company's employees and employees. Security officers in all regions of MTS PJSC operation traveled around base stations in order to check anti-terrorist protection.

In accordance with the legislation of the Russian Federation and the recommendations of the Ministry of Emergency Situations of Russia, as well as in accordance with the approved Action Plans for civil defense, prevention and response to emergency situations and ensuring fire safety, the CC and branches of MTS PJSC took measures in the field of civil defense and Emergency.

Priority areas in the field of personnel and facility safety:

- improving the efficiency of the security system and anti-terrorism protection of personnel and facilities of MTS PJSC;
- ensuring the safety of managers and employees, as well as facilities and infrastructure elements of MTS PJSC;
- implementation of measures to prevent theft of equipment and inventory from the facilities of MTS PJSC; and
- maintaining readiness for action of MTS PJSC's system for emergency prevention and response under threats and emergency conditions.