INFORMATION PROTECTION AND SECURITY

RESULTS OF THE SECURITY UNIT PERFORMANCE IN 2020 AND PLANS FOR 2021

The work of the Security Unit of the MTS PJSC Corporate Center (hereinafter referred to as the Security Unit), as well as of the security departments in the MTS PJSC branches and subsidiaries, was organized and carried out in 2020 in strict adherence to the current legislation of the Russian Federation, the Strategy, internal regulations and action plans of MTS PJSC.

Pursuant to the guidance documents, the main efforts for integrated security management in 2020 were aimed at the following:

- implementation of tasks to ensure the sustainability and continuity of business development of the MTS Group, identification and prevention of risks in the field of corporate security;
- protection of the interests of the Company's shareholders, personnel and clients, as well as its business processes, assets, property and information resources, from internal and external threats;
- implementation of measures to prevent and fight terrorist and criminogenic threats;
- improvement of the economic security system and corruption prevention.

As a result of inspections and official investigations carried out in 2020 by security personnel in cooperation with the Company's divisions, the damage in the amount of 2,309.593 million rubles was prevented, the damage in the amount of 373.718 million rubles was established and the damage in the amount of 189.149 million rubles was compensated.

In order to prevent illegal acts in the field of procurement, 53,269 inspections of draft contracts, supplement agreements, orders and supplier selection reports were carried out, and information on 36,509 counterparties was studied, of which 1,366 were rejected as unreliable.

While examining the candidates for entering into labor relations with the Company, 3,763 persons were denied employment on negative grounds (as not meeting the requirements of MTS PJSC for candidates, excluding professional qualities).

Work on the facts and attempts to steal and damage the Company's property, to identify violations of the requirements for communication secrecy, information security standards and compliance with the commercial secret regime was carried out on an ongoing basis.

Based on the materials of the Security Unit (following the results of verification activities), law enforcement agencies initiated 333 criminal cases against the persons engaged in illegal activities and acting to the detriment of corporate security of MTS PJSC in 2020.

OBJECTIVES FOR 2021

Implementing a set of measures aimed at achieving the main goal: ensuring stability, reliability, continuity of development and functioning of the Company's business in 2021. Ensuring consistent operation in the best interests of increasing business profitability, creating effective barriers to prevent losses and damages, countering fraud and maintaining a high level of safety of personnel and facilities.

[1] The launch date of the solar power plant is January 13, 2021.

\\ 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 Digital Development, Communications and Mass Media of the Russian Federation, 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. Imperfection of information security legislation in the context of creating "digital economy". The existing industry approach to governing information protection is not applicable when integrating information, information processes and systems to build a "digital environment". The presence of different information security requirements for one object of protection in regulations creates the risk of non-compliance.
Contractual risks associated with information security	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.).
Risk of clients' claims to information protection in the Company's innovative products	As for the innovative products offered to consumers, it is necessary to create their own information protection system, taking into account the current threats and applicable requirements of the legislation of the Russian Federation. A product developer requires a high level of competence in the development of information protection mechanisms in order to exclude clients' claims due to non-compliance of the product with legal requirements or information security breaches.

INFORMATION SECURITY

GLOBAL TRENDS OF THREATS IN THE SPHERE OF INFORMATION SECURITY

In 2020, the Security Operations Center (SOC) of MTS PJSC recorded multiple cyberattacks on the subscriber personal accounts of MTS PJSC and its subsidiary, MGTS PJSC, as well as DDoS attacks on various services, including the MTS Money fintech resource (payment.mts.ru). The analysis of the mechanisms for implementing attempts to maliciously affect subscribers and own infrastructure of information and communication technologies (ICT), as well as the study of open sources showed that, in addition to the previously noted interest of criminals in obtaining information assets (arrays) with personal data and telemetry of communication service consumers, financial transactions data and other limited access information, there is a clearly visible trend for the attacker to take over hidden parallel control over the software and hardware means of processing the information of the victim company for long-term operation in accordance with their goals.

The COVID-19 pandemic also brought new challenges to the agenda of information security services, especially large tech companies, due to the massive transfer of employees to remote working. Well-protected corporate perimeters turned out to be permeated with thousands of unauthorized entry points from employees' personal devices, which often did not meet corporate requirements for information security and were not equipped with information security means. No video monitoring tools in places of remote work of employees who may access confidential information could also lead to a decrease in the level of security of information belonging to companies.

In general, despite the unforeseen events caused by the global spread of the coronavirus infection and related structural changes in business processes, the following threats can be predicted for the corporate sector to stay relevant in 2021.

- Coordinated targeted attacks (Advanced Persistent Threat) on the clients, online services, ICT infrastructure of tech companies, including in order to get a wide range of information about the information security architecture of the existing ecosystems, processes and measures for its implementation.
- Social engineering and direct recruitment of the Company personnel, especially those employees who work from home.

- No means to manage and control employees' personal mobile computing equipment that provides a secure working environment equivalent to desktop platforms in functionality and convenience.
- Zero-day vulnerabilities in cloud services, lack of security mechanisms acceptable for large companies.
- Errors in the program code of commercial and proprietary IT solutions, as well as their development without considering the requirements for the safe program code production.
- Generation of botnets based on terminal user equipment or ICT infrastructures of companies in order to implement unauthorized and malicious cyber attacks.
- Inconsistency of protection mechanisms in the Internet of Things (IoT) solutions with modern threats and lack of updates for outdated devices still in operation.
- Development of the trend in the complication 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 SYSTEM AT MTS

- Protection of the interests of MTS PJSC in the information sphere is achieved by a set of interrelated organizational and technical measures forming a unified information security management and provision system. An integrated approach allows for protecting the Company and its subsidiaries from modern threats to information security and infrastructure of information and communication technologies and ensuring compliance with the legislative requirements of the Russian Federation, international standards, as well as for preventing financial, reputational and other damage. The information security system has been built and is developing 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 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 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 it provides the corresponding services.

INFORMATION SECURITY RESULTS AND ACHIEVEMENTS IN 2020

- The manageability of information security units was fully preserved during the emergency mass transfer of the Company's personnel to remote working and continuous monitoring of compliance with the requirements of local regulations on information security was ensured.
- The development of the information security management and ensuring systems 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 2020". The planned tasks were completed, and the set goals were achieved.
- The protection systems of critical databases were upgraded, 125 online services were provided with WAF protection, the uninterrupted operation of the public key infrastructure and three certification centers of MTS PJSC was guaranteed.
- The information security processes were integrated into the processes of product transformation, the ecosystem of MTS PJSC is protected and support is provided to the product teams.
- Target architecture was developed for the solution to integrate subsidiaries into the MTS PJSC security perimeter and to provide secure controlled access to the employees of the MTS Group companies.
- Permanent representation of experts from the Information Security Department in government programs and in working departmental groups was organized, interaction with regulatory authorities was established.
- A system of interaction with the Main Center of GosSOPKA (State System for Detection, Prevention and Elimination of the Consequences of Computer Attacks) was introduced to inform the NCCCI (National Coordination Center for Computer Incidents) about the incidents of the CII systems (Critical Information Infrastructure) and the clients of commercial SOC, CII subjects.
- Following the oversight audit held in 2020, the British Standards Institution conformed the compliance of the Information Security Management System of MTS PJSC with the international standard ISO/IEC 27001:2013 Information technology – Security

techniques – Information security Management systems – Requirements and extended the Certificate of Conformity No. IS719403 for 2021. The certification expands the capabilities of MTS PJSC to participate in bidding and tenders requiring compliance with international IS standards and practices.

2020 LESS RESULTS AND ACHIEVEMENTS

- 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 complexes have been installed on communication networks, the presence of which makes it possible to provide new communication technologies (NB IoT, IMS, RCS, 5G, eSIM), as well as new convergent services (MTS Connect with Virtual Number and MultiAccount functionality, WiFi Calling, VoLTE/ViLTE, RCS IP Messaging, Virtual PBX, WiFi for business).
- 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.

MAIN OBJECTIVES IN THE FIELD OF MANAGEMENT AND ENSURING INFORMATION SECURITY FOR 2021

- Ensuring compliance of the Information Security Management System of MTS PJSC with the international standard ISO/IEC 27001:2013 Information technology – Security techniques – Information security Management systems – Requirements.
- Infrastructure IS changes as part of the ecosystem construction:
- participation in the development of new products and services;
- ensuring compliance with the IS requirements in the production of new products and services;
- transition of IS divisions to a service model of working with product teams, as well as introduction of IS services for product teams;
- development and use of IS platforms in subsidiaries of the MTS Group.
- Development of IS products:
- expanding the services of the Security Operation Center (SOC);
- creation of a Threat Intelligence platform for timely detection and prevention of cyber threats;
- formation of a Red Team to identify and counter cyberattacks.
- Automation and improvement of IS processes in terms of automating the processes of drawing up a non-disclosure agreement (NDA), creating an automated system for confidential electronic document management (EDM), as well as automating the audit process.
- Compliance with the legal requirements for the security of critical information infrastructure and the protection of personal data, as well as development of the security system for significant facilities of the MTS PJSC CII.
- Participation in preparing drafts of new regulations of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation in the area of IS.
- Implementation of the Information Security Awareness Program for personnel.

ECONOMIC SECURITY

In 2020, the work of the economic security and anti-corruption units of MTS PJSC was focused on identifying financial and economic risks, preventing reputational and material damage, developing recommendations and taking measures to minimize them.

One of the activity areas is the minimization of financial and economic risks when exercising control over the selection of suppliers/contractors, the volume and cost of equipment/work/services and the execution of the Company's local regulations.

In order to improve the quality of corporate audits, investigations and claim settlement with counterparties to collect overdue receivables, the Economic Security Department was established within the structure of the Department for Economic Security and Countering Corruption of the BB CC (DES&CC).

DES&CC also detected the violations of the secrecy of subscribers' communications committed by the employees of MTS PJSC quite efficiently. In cooperation with law enforcement agencies, protection of the secrecy of communications was arranged. Positive results were achieved in the measures to identify and document the facts of theft of funds from the bank accounts of legal entities and the suppression of illegal activities in close cooperation with law enforcement agencies.

Due to the changes in the functional strategy of DES&CC, certain functional areas were redistributed: the Subscriber Fraud Countering Department and its functionality were transferred to the Anti-Fraud Center of MTS Group's BB CC.

In order to reduce the timing of procurement procedures, DES&CC actively participates in the implementation of the procurement transformation project. The regulations governing the Company's procurement and investment activities were updated. The new versions of the documents set the obligation of the buyers to get the DES&CC approval on the procurement procedure, the cost of which exceeds 1 million rubles, at the stage of drawing up the ToR. The principle of assigning DES&CC experts to specific areas of procurement was introduced.

DES&CC also updated the local regulations in the field of ensuring economic security and countering corruption. Fundamental changes were made to the Process Regulations RP-053 "Conducting an Internal Investigation". As a result of improvements in the new version of the RP, the process of conducting corporate audits was formalized.

PRIORITY AREAS FOR ENSURING ECONOMIC SECURITY AND COUNTERING CORRUPTION

- Ensuring control over procurement activities, investment planning, preparation and implementation of investment projects in the areas of economic security and anti-corruption.
- Improving the arrangement of ensuring economic security and countering corruption within the MTS Group.
- Participation in the development and implementation of the MTS Group Strategy in the field of comprehensive security of the MTS Group.
- Organization and control over the timely development and updates of the local regulations in the field of ensuring economic security and countering corruption.
- Methodological guidance, control and coordination of the activities of regional and subsidiary units in charge of economic security and countering corruption.

SAFETY OF PERSONNEL AND FACILITIES

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

- The work to ensure access and intra-facility regimes at MTS PJSC was based on the Standard "Requirements for ensuring the security of MTS PJSC facilities". Access control at the Company's facilities was carried out by the employees of SAFETI LLC using engineering and technical security equipment, access control and management systems, CCTV, signaling and communication systems.
- In 2020, the possibility of using the face recognition function to access the facilities of MTS PJSC in the Moscow Region was implemented within the investment project.
- The ability to use a smartphone as a pass using the Mobile Pass service was implemented in several regions in 2020.
- In order to prevent the occurrence of vandalism and theft of inventory at the facilities of the radio subsystem and to provide uninterrupted communication services, activities were continued to ensure the continuity of operation of the priority BS due to a significant increase in their equipping with security equipment.
- In order to check the readiness of the security personnel of the private security company in terms of acting in the event of emergency at the facilities of MTS PJSC, fire-fighting and anti-terrorist trainings were conducted together with the employees of the Administrative Unit throughout 2020. Security officers in all regions of MTS PJSC operation traveled around base stations in order to check their anti-terrorist protection.
- In 2020, scheduled measures were taken to identify and eliminate possible channels of leakage of speech information circulating in the premises of the Company's management through acoustic and technical channels.
- 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 2020 Action Plans for civil defense, prevention and response to emergency situations and ensuring fire safety, the MTS Group took measures along this line of activity.

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.
- Implementing measures to prevent theft of equipment and inventory from the facilities of MTS PJSC.
- Maintaining readiness for action of MTS PJSC's system for emergency prevention and response under threats and emergency conditions.