Security of banking operations

Economic security

Economic security is an overriding priority for Sberbank. We devote special attention to preventing threats and ensuring the stable work of the Bank. In 2017 we identified and prevented 529 attempts to use stolen (lost) or forged passports, identified 22 attempts at fraud using forged payment documents, and prevented 71 cases of theft using forged powers of attorney of a total of RUB 600 million in funds from the deposits of Sberbank clients.

In all, the economic security divisions sent 1,055 statements to law enforcement agencies concerning attempts to cause damage to Sberbank or its clients, and 526 criminal cases were instigated.

We take a proactive approach to the identification of counterfeit banknotesIn 2017, 4,041 counterfeit or intentionally damaged (partial) banknotes were identified, as well as 80 mass influxes of banknotes. Sberbank branches and the Corporate Investment Center detected 949 instances when clients presented counterfeit banknotes of the Bank of Russia. In addition, 1,577 counterfeit banknotes of various face values were removed from circulation. Fifteen people were arrested in 2017 for distributing counterfeit banknotes, with criminal proceedings instigated against one person.

As part of the “Red button–AR” fraud monitoring procedures, 313 audits were performed on corporate borrowers in 2017 at the request of the underwriting service due to suspicions of loan fraud. Instances of loan fraud were confirmed in 169 cases, in the amount of RUB 7.5 billion.

Reviews of 54.3 thousand loan applications of individuals using “Credit Factory” technology were also performed in 2017 and sent on for additional review to the economic security divisions.

Information security

We use state-of-the-art information security systems to ensure secure, fully functional servicing of clients. Artificial intelligence and analytical tools were used in 2017 to identify fraudulent operations when clients voluntarily transfer information to con-men, making it possible to hedge nearly 97% of this risk on the client side. During 2017 more than 300 thousand attempts to steal the funds of individuals and legal entities were stopped, preventing damage of more than RUB 40 billion.

Around 40 major DDoS[1] attacks on Sberbank were averted, ensuring 100% protection of the Bank's infrastructure.

The Bank pays close attention to cyber-security. The Bank has learned how to successfully combat cybercrime using an intelligent client protection system. The Sberbank project "Fraud monitoring for remote retail channels", for instance, was the bronze medalist at the international IPMA International Project Excellence Award 2017 competition. As part of this large-scale project, which lasted 15 months, Sberbank implemented a unique fraud monitoring system created based on artificial intelligence. The system automatically protects clients from inappropriate actions caused by a lack of knowledge of cyber-security rules. Every day we uncover several thousand suspicious transactions using this system.

The development of the systems to combat cyber fraud will continue in 2018, to ensure 100% protection of all Sberbank's client service channels.

Organization of the processing and protection of personal data

At Sberbank, personal data is protected through a single integrated system of organizational, technical and legal measures to protect confidential information (trade secrets, bank secrets, personal data), taking into consideration the requirements of federal legislation (including Federal Law No. 152–FZ dated 27 July 2006 "On Personal Data") and also global best practices.

When processing personal data, we take the necessary legal, organizational and technical measures to protect data against unlawful or accidental access, destruction, alteration, blocking, copying, provision, dissemination and also against any other unlawful actions with the personal data.

Measures to ensure the safety of personal data include but are not limited to:

- allocation of a controlled area where Sberbank's automated systems function;
- protection of the machine information media on which personal data are stored and/or processed;
- anti-virus protection;
- identification and prevention of intrusions;
- control and analysis of the security level of personal data;
- ensuring the integrity of Sberbank's automated systems and personal data;
- ensuring the accessibility of personal data;
- protection of the virtualization environment;

[1] Distributed Denial of Service

- protection of hardware;
- protection of automated systems, their tools, communications and data transmission systems;
- identification of and response to incidents that might lead to breakdowns or disruptions in the functioning of the automated systems and/or to the appearance of security threats to personal data.

In order to neutralize existing threats to personal data security, we use information security tools that have duly passed procedures to assess their compliance with the requirements of Russian information security law.

Access to the personal data being processed is given only to those Sberbank employees who require this data to perform their job duties. Everyone hired by Sberbank signs a non-disclosure agreement covering personal data and other confidential information. This agreement remains part of the employee's personal file.

In order to improve their information security awareness, knowledge and skills, employees undergo training in the form of mandatory remote training courses.

Sberbank has also organized internal controls (audits) of the compliance of personal data processing with Law 152–FZ and regulations adopted in accordance with this law, personal data protection requirements, Sberbank policy on handling personal data, and Sberbank's internal regulations. The internal audit is performed by the Internal Audit Service of Sberbank as part of audit reviews.

The Cybersecurity Service of Sberbank monitors the protection of personal data during processing in automated systems. Monitoring of protection in the information infrastructure uses instrumental verification and penetration testing.