Ensuring Stability and Reliability

The merger increased the load on the Bank's IT systems from two to four times. In 2017, an average of 2.8 million transactions were conducted through the the Bank's primary systems. In 2018, this increased to 3.5 million transactions. The load on peak days in 2018 was four times higher than the average for the year for card transactions and 11 times higher for non-card transactions.

Immediate and medium-term measures were taken that enabled the Bank to make it through the peak New Year season (2019) with no failures, while ensuring the availability of twice as much bandwidth as was needed. Measures are being taken to reduce process windows, e.g., the introduction of DevSecOps will reduce periods of partial or complete unavailability of the Bank's IT systems for customers by 30-70% (from 16 to 8 hours). Work is under way to fully implement the service level agreement for each parameter for critical services.

Throughout 2018, the Bank's clients experienced temporary restrictions when using the VTB mobile application, including while conducting various operations. To prevent similar situations in the future, technical steps were taken to increase the traffic capacity of the Bank's IT systems. In addition, a plan was developed for further measures to improve the fault tolerance and performance of software. In particular, the plan provides for the distribution of information load across various domains depending on the service provided: sales and assistance for Bank products or the provision of customer services. The purchase of additional equipment is also planned.

In 2018, information security issues were the subject of close scrutiny. The adoption of timely measures enabled the Bank to avoid the possible ramifications of both global cyberattacks and attacks aimed specifically at VTB Bank, as well as to pass an inspection on compliance with information security requirements.

As a result, the Bank **fended off 100% of cyberattacks: 68,509 cyberattacks** (malware attacks on the site and emails). Of these, **759 attacks used modified malware not detected by anti-virus tools.**

Key achievements in 2018 in the area of information security:
- The creation of a closed perimeter that ensures a high degree of protection for critical banking systems.
- The introduction of "sandboxes", i.e., software and hardware packages that analyse incoming information flows and protect the system against phishing emails and emails that contain viruses before they get beyond the Bank's firewall.
- The creation of project support services, which made it possible to involve information security at all stages of project work.
- Ensuring compliance with the regulatory requirements of the Bank of Russia; the Federal Security Service of the Russian Federation; the Federal Service for Technical and Export Control; the Federal Service for Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor); the SWIFT code system; and others in the field of information security.

Key objectives of the technological transformation within VTB Group
- **Transformation of the IT landscape of the unified Bank**
- **Formation of the unified Bank's branch network**
- **Increasing the number of foresight projects**
- **Development of remote service channels (mobile-first strategy)**