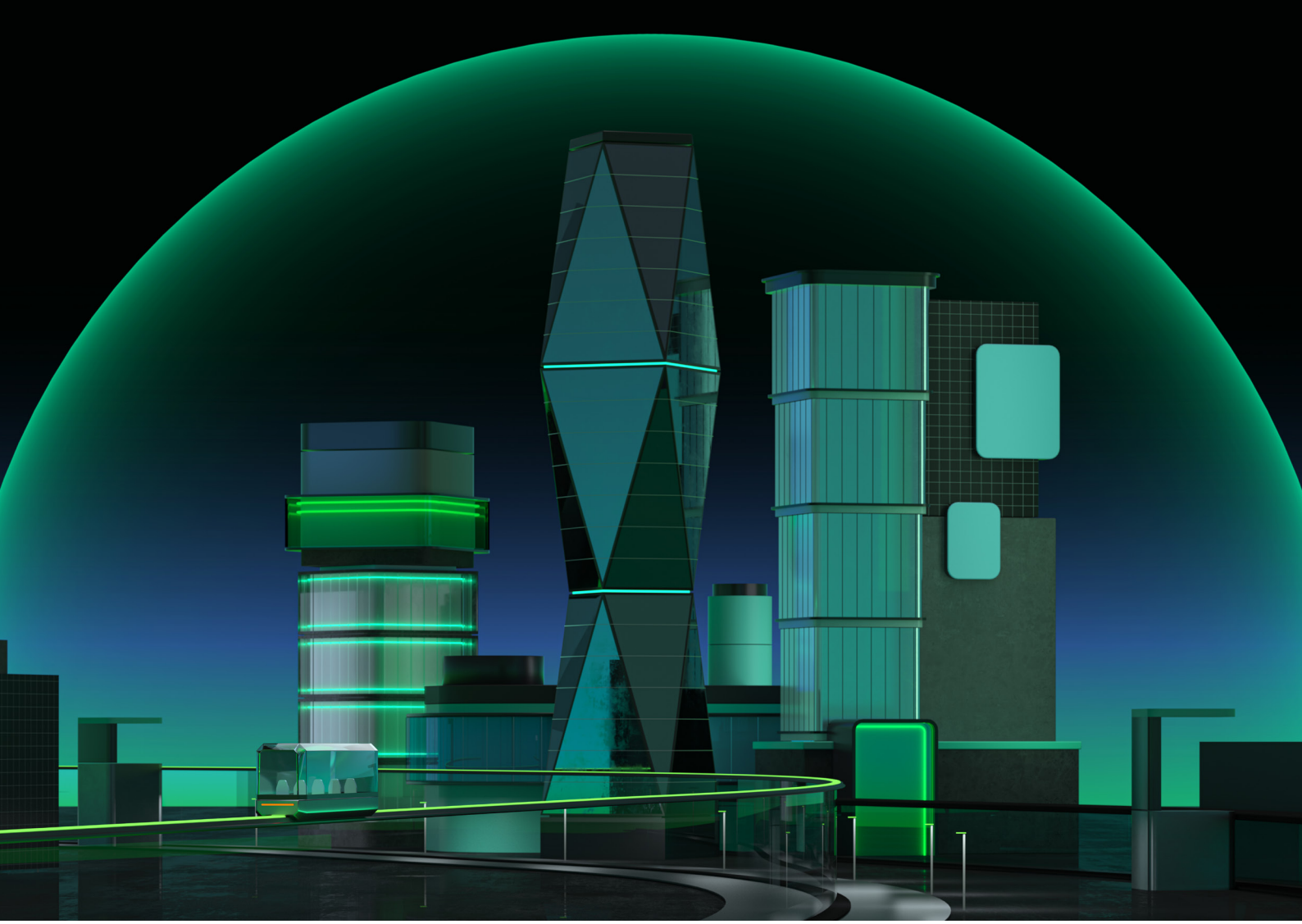


Building a cloud-based control room for urban management

Kaspersky: smart city protection in Orenburg

kaspersky

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И СТРАТЕГИИ

KasperskyOS

"Our task is to ensure a steady increase in the quality of life for residents of the region and create a comfortable urban environment for everyone through the use of digital technologies. When using modern technologies, the top priority for us is protecting the city's infrastructure from cyberthreats. That's why we turned to Kaspersky, an expert in this field, to implement a solution that provides data protection in the housing and public utilities system for remote monitoring and management of building engineering systems."

Dmitry Vecherenko,
First Deputy Minister of Digital Development and Communications of the Orenburg Region

As part of the nationwide Housing and Urban Environment project and the Digital Economy national program, the Ministry of Construction, Housing and Utilities of the Russian Federation is implementing the **'Smart City' project for the digitalization of the urban economy**. Its goals are to increase the competitiveness of Russian cities, form effective urban management systems, and create safe and comfortable living conditions for citizens.

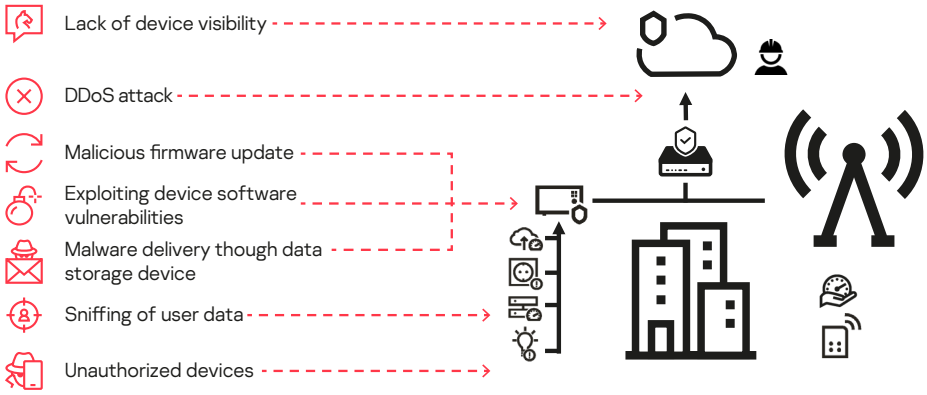
Orenburg is one of the cities participating in the project. Kaspersky collaborated with the Orenburg regional government in the creation of a cloud-based control room.

Objective

In large cities, it is almost impossible to effectively manage thousands of residential and non-residential objects and correctly reflect the city-wide situation in the field of public utilities without **automated data collection from a single center**. This is where a cloud control room can help.

The technologies of the internet of things (IoT) make it possible to build such a platform. But because the IoT infrastructure has numerous vulnerabilities, it's necessary to provide reliable cybersecurity. The functioning of the city's critical structures, and with them people's lives, may depend on the quality of that cybersecurity. For example, if a hacker manages to gain access to a fire alarm system, city services may not receive a fire alert in time.

Kaspersky specialists carried out research and compiled a threat model characteristic of urban IoT solutions.



Attack vectors on the IoT infrastructure

Solution

Based on the threat model that was created, Kaspersky developed an approach that makes use of several solutions for protection at different levels of the urban IoT infrastructure.

The cloud level is protected by **Kaspersky Hybrid Cloud Security**. This comprehensive solution for automated protection of hybrid cloud infrastructure performs the following functions:

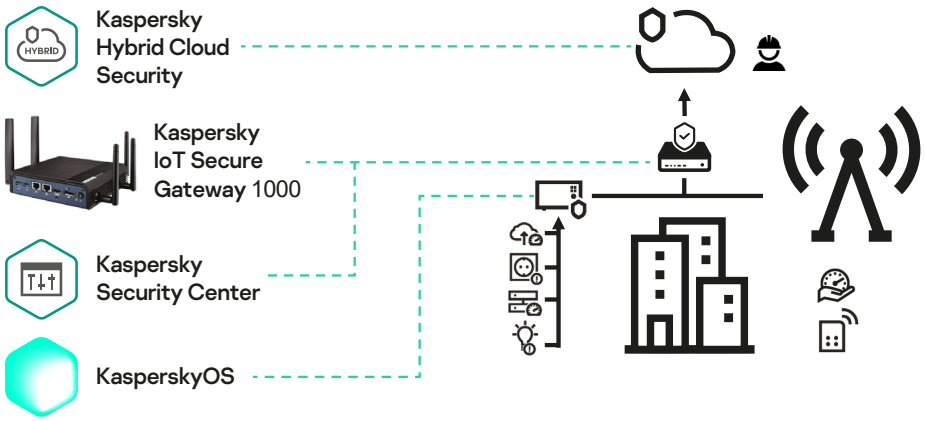
- **Application Control.** Makes it possible to switch all workloads in the hybrid cloud to Default Deny mode to enhance system protection and specify where authorized programs can run and what is available to them
- **Device Control.** Allows you to configure which virtualized devices can access cloud resources. The Web Control function protects the environment against cyberthreats from the internet

- **Network segmentation.** Allows you to organize transparent automated network protection in the hybrid cloud infrastructure, which checks individual networks and ports
- **Protection against vulnerabilities.** Prevents the use of unpatched vulnerabilities by advanced malware and zero-day threats

The data transfer channel from the controller (PLC) to the cloud is protected by **Kaspersky IoT Secure Gateway (KISG) 1000**. This gateway is based on the technologies of KasperskyOS. It not only has Cyber Immunity – innate protection against cyberattacks – but also helps ensure the security of the entire IoT infrastructure. The **Kaspersky Security Center** platform allows you to centrally manage KISG 1000 and track its events. Together, these two products form **Kaspersky IoT Infrastructure Security**.

Kaspersky IoT Secure Gateway 1000 detects and classifies all devices on the network. The gateway has firewall functions and protects against network attacks (IDS/IPS). It also provides the means to receive, scan and distribute sensor messages received via the MQTT protocol.

The **SEM Pro 5** controller, developed by Information Systems and Strategies, is installed as a PLC. The pre-installed **KasperskyOS** operating system ensures data intergrity: prevents data tampering, securely downloads firmware updates and protects certificates and controller policies.



Kaspersky approach to protecting the internet of things

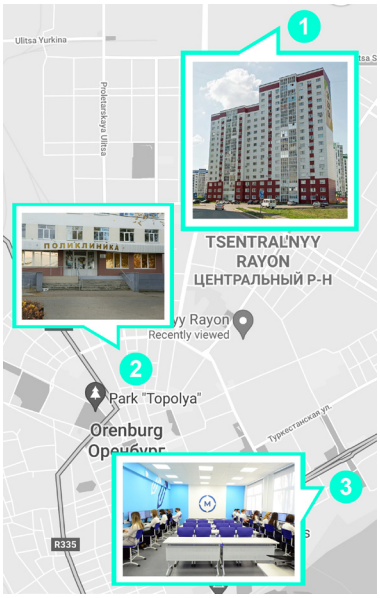
"Information Systems and Strategies and Kaspersky have been collaborating for a number of years. In that time the partnership has implemented a large number of joint projects. It's good to know that our positive experience of cooperation allows us to contribute to the development of the cybersecurity environment of a smart city implemented on the Inspark IoT Platform, and helps modernize the domestic range of information security products to counter complex threats."

Oleg Krupenko,
General Director of Information Systems and Strategies

Building a cloud control room within the framework of the Smart City project

In order to build an urban IoT infrastructure, three objects with different social functions were identified with the participation of the Ministry of Digital Development and Communications of the Orenburg Region:

1. Apartment building (155/6 Pobedy Ave.)
2. Polyclinic of Orenburg Regional Clinical Hospital №2 (24 Nevelskaya Street)
3. Orenburg College of Economics and Informatics (11 Chkalova Street)



Cloud control room tasks:

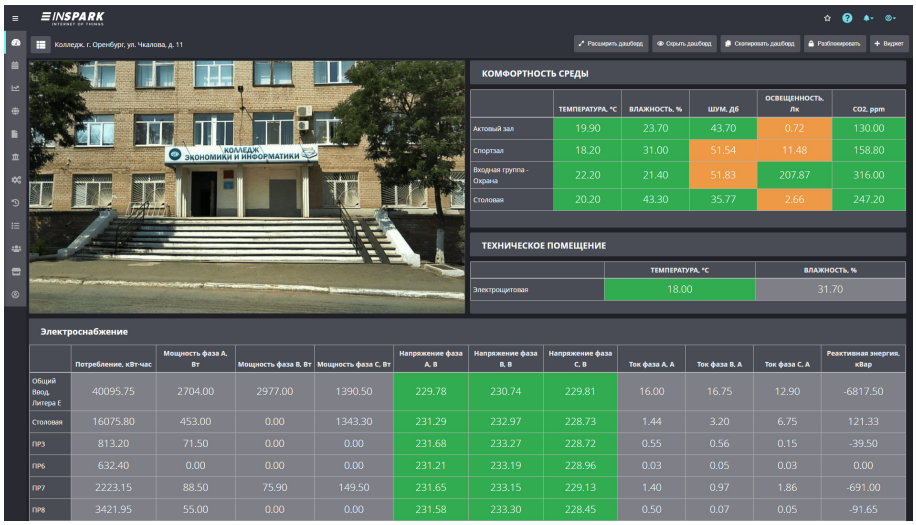
- Remote monitoring of residential building indicators and engineering systems
- Optimization of maintenance costs for those systems
- Reducing resource consumption
- Improving accident and incident response times
- Quality control of public utility services

The following parameters are collected from each object:

- power supply: phase voltage, current frequency, current strength;
- water supply: consumption of hot and cold water, hot water temperature and water pressure in the supply/return pipeline;
- heat supply: temperature of the heat transfer fluid up to the ACU, before it reaches the consumer, after the consumer and ACU, and the heat energy consumed;
- entrance hall environment: temperature, lighting, humidity, CO2 level, noise level;
- operation of elevators, opening of doors in elevator shafts;
- operation of intercom systems;
- triggering of the fire alarm;
- activation of access control systems.

Work was carried out at the various sites to install sensors and controllers along with the means of transmitting the collected data and their visualization:

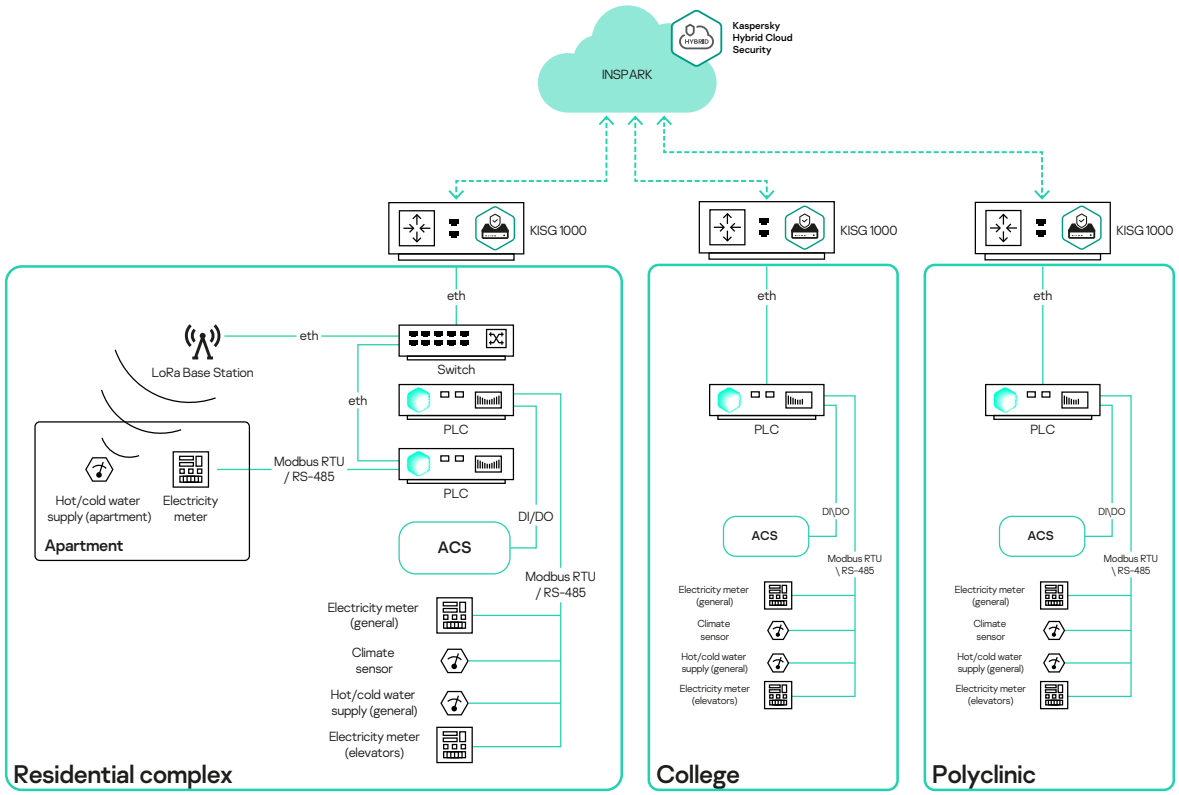
- most sensors transmit data via the Modbus RTU protocol with the RS-485 interface;
- sensors of hot and cold water supply transmit data via the LoRa wireless protocol;
- information from the access control system (ACS) sensors is transmitted to the controller through a digital input/output (DI/DO) module;
- after the data is collected on the controller, **Kaspersky IoT Secure Gateway 1000** provides secure data transfer to the **InSpark IoT Platform** cloud service via a GSM channel.



All the collected parameters are displayed on the dashboards of the cloud control room

Results

Testing of a smart city digital control room is a long-term project. Its effectiveness directly depends on the reliability of the entire IoT infrastructure. Kaspersky's technologies have helped protect it from cyberattacks at all levels.



Protection of public utilities systems in Orenburg using Kaspersky technologies

In the process of using the control room, the following results are expected:

- resource savings;
- timely notification of accidents and a reduction in the time taken to eliminate them;
- better control over the deterioration of utilities;
- increase in the transparency of public utilities management;
- successful resolution of other tasks.

Thanks to the cloud control room, it's possible to centrally collect relevant indicators from public utility services and monitor them comprehensively, consolidating data on a single platform.

All this also makes it possible to monitor the actual consumption of resources online, increasing the transparency of public services and, as a consequence, the level of trust in them.