aprotech Kaspersky IoT company

KasperskyOS Operating system

Kaspersky IoT Secure Gateway

Cyber Immune gateways for connecting objects of **CRITICAL URBAN INFRASTRUCTURE AND URBAN HOSEHOLDS** to cloud management and monitoring services and business systems

Scenario №1

Gateway as a software data diode (one-way data transmission)

- **Safe and secure transport** of previously unavailable data
- **Trusted data** received from the gateway help to build digital analytics and equipment operation forecasting services
- **Universal software data diode** converter to transmit telemetry data to CIS*
- **Protection of a critical urban infrastructure** and urban households
- **Realization of scenarios** related to the environmental monitoring of urban objects
- **Protection of a traffic lights network** and a road infrastructure
- **Protection** of an urban parking infrastructure

*Corporate Information System

Scenario №2

Gateway as a router (two-way data transmission)

- **Sending security events** via the Syslog protocol
- **Safe and secure** two-way data transport of previously unavailable data
- **Detection of IDS/IPS intrusions** to provide protection from external threats
- **Remote monitoring and engineering systems management** of large separate buildings (shopping malls, business centers (A, B class)) * **
- **Overall protection** of industrial (dangerous) objects in urban areas
- **Protection and realization** of scenarios «Smart house» in elite residential complexes and villages **
- **Overall protection** of a federal and urban data centers' infrastructure
- **Monitoring and defense** of an urban engineering infrastructure (water supply, power supply, central sewage, waste storage areas)

Notes:

*Using ecosystem of Kaspersky Lab products: KISG+KUMA+ KSRW+KICS+KSC

**When integrating KISG (gateway) with BIM systems