aprotech Kaspersky IoT company

KasperskyOS Операционная система

Kaspersky IoT Secure Gateway

Кибериммунные шлюзы для подключения **ОБЪЕКТОВ ГОРОДСКИХ ИНЖЕНЕРНЫХ СИСТЕМ** к облакам и бизнес-системам

Сценарий №1

Шлюз как программный диод данных с функцией преобразования прикладных протоколов (однонаправленная передача данных)

- **Безопасный и надежный транспорт** ранее недоступных данных;
- **Доверенные данные** со шлюза помогают строить цифровые сервисы по аналитике, прогнозированию работы оборудования;
- **Универсальный** программный дата-диод конвертер для передачи телеметрии в КИС;
- **Защита городской критической инфраструктуры** и городских домохозяйств;
- **Реализация сценариев** по экомониторингу городских объектов;
- **Защита** светофорной сети и дорожной инфраструктуры;
- **Защита** инфраструктуры городского парковочного пространства.

Сценарий №2

Шлюз как межсетевой экран с функцией маршрутизации данных (двунаправленная передача данных)

- **Использование шлюзов на объектах КИИ** в режиме FW по сертификации ФСТЭК;
- **Отправка событий безопасности** по протоколу Syslog;
- **Безопасный и надежный двунаправленный транспорт** ранее недоступных данных;
- **Анализ промышленных протоколов (с функцией обнаружения и предотвращения вторжения)** для защиты от внешних угроз;
- **Удаленный мониторинг и управление** инженерными системами отдельно стоящих крупных зданий (ТРЦ, БЦ (класс А,В));* **
- **Комплексная защита** промышленных (опасных) объектов на территории городов;
- **Защита и реализация** сценариев «Умный дом» в элитных и закрытых ЖК и поселках;**
- **Комплексная защита** инфраструктуры ЦОД федерального и городского уровня;
- **Мониторинг и управление** системой защиты городской инженерной инфраструктуры (водоснабжение, электроснабжение, центральная канализация, места хранения отходов).

Примечания:

*С использованием экосистемы продуктов «Лаборатории Касперского»: KISG+KUMA+KSRW+KICS+KSC;

**При интеграции шлюзов KISG с BIM-системами.