Кибербезопасность интернета вещей в умных городах

Kaspersky IoT Infrastructure Security

Умный город — это концепция интеграции множества информационных и коммуникационных технологий. В их число входят системы интернета вещей (IoT) для управления городской инфраструктурой — транспортом, здравоохранением, системами ЖКХ и безопасности. Анализ данных, собранных с тысяч жилых и нежилых объектов, позволит снизить потребление ресурсов, оптимизировать затраты на обслуживание инженерных систем и оперативно взаимодействовать с жителями.

Увеличение степени автоматизации и активное проникновение информационных технологий в городскую инфраструктуру значительно повышают риски, связанные с кибератаками на городские объекты. «Лаборатория Касперского» предлагает **Kaspersky IoT Infrastructure Security** — комплексное решение для построения защищенных систем умного города.

kaspersky

KasperskyOS

Задачи облачной диспетчерской

- Удаленный мониторинг общедомовых показателей и инженерных систем
- Оптимизация затрат на обслуживание этих систем
- Снижение потребления ресурсов
- Увеличение скорости реагирования на аварии и инциденты
- Контроль качества обслуживания ЖКХ

Датчики и контроллеры на объектах обеспечивают:

- Сбор параметров электроснабжения: напряжение по фазам, частота и сила тока
- Сбор параметров водоснабжения: потребление ГВС/ХВС, температура и давление воды в трубопроводе
- Сбор параметров теплоснабжения: температура теплоносителя до и после автоматизированного узла управления, температура теплоносителя до подачи потребителю, потребленная тепловая энергия
- Сбор параметров комфортности среды в подъездах: температура, освещенность, влажность, уровень CO_2, уровень шума
- Работоспособность лифтов, открытие дверей в шахтах
- Работоспособность домофонов
- Срабатывание пожарной сигнализации
- Срабатывание систем контроля доступа

Городская платформа диспетчеризации

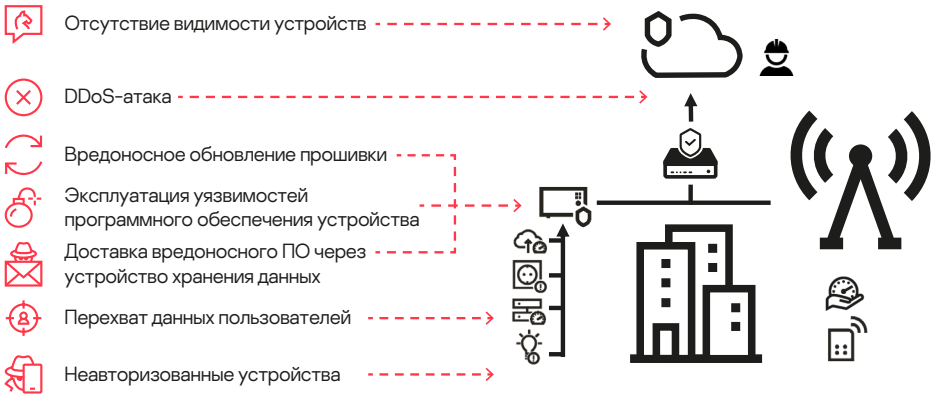
Вручную собирать и анализировать данные, полученные с нескольких тысяч жилых и нежилых объектов, почти невозможно без облачной диспетчерской. Отсутствие централизованного сбора показателей с объектов снижает эффективность управления ими и не позволяет корректно отразить общегородскую ситуацию в сфере коммунального хозяйства.

Решение, позволяющее реализовать единую диспетчерскую платформу, строится на технологиях интернета вещей. С каждым годом они все активнее используются в инфраструктуре городов, однако без внимания этот сегмент не оставляют и киберпреступники.

Необходимость защиты инфраструктуры умного города

Умные города развиваются быстрее, чем средства их защиты, и это оставляет большой простор для деятельности злоумышленников. Формирование единых стандартов кибербезопасности интернета вещей только начинается; при этом на рынке появляется все больше и больше IoT-решений, многие из которых не отвечают основным требованиям информационной безопасности.

Для инфраструктуры умного города применима модель угроз, характерная для интернета вещей.



От безопасности интернета вещей может зависеть работа критически важных городских структур, а вместе с ними — жизни людей. Например, если хакеру удастся получить доступ к системе пожарной сигнализации, городские службы могут вовремя не получить оповещение о возгорании.

Особенности реализации

На каждом объекте размещается ряд датчиков, подлежащих мониторингу. Большинство датчиков передает данные по протоколу Modbus RTU с интерфейсом RS-485.

Датчики горячего и холодного водоснабжения передают данные по беспроводному протоколу LoRa.

Информация с датчиков системы контроля управления доступом (СКУД) передается на контроллер через модуль ввода/вывода дискретных сигналов (DI / DO).

После того как данные собраны на контроллере, KISG 1000 обеспечивает безопасную передачу данных в облако по GSM-каналу.

Администрирование всех шлюзов, находящихся в составе сети, происходит с помощью Kaspersky Security Center.

Решение

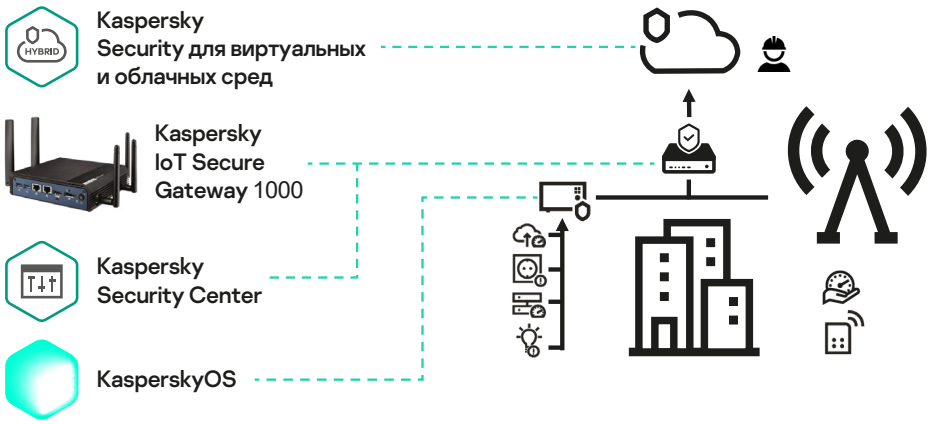
В жилом доме устанавливаются системы контроля потребления ресурсов, управления электричеством и водоснабжением. Внутриквартирные счетчики подключаются по беспроводному протоколу LoRaWAN. За физическую безопасность систем отвечают системы видеонаблюдения с удаленным доступом, замки, датчики движения и открытия дверей, а за информационную безопасность — решения «Лаборатории Касперского».

Kaspersky IoT Secure Gateway (KISG) 1000 — кибериммунный шлюз, работающий под управлением операционной системы **KasperskyOS**. Он не только сам обладает «врожденной» защитой от кибератак, но и помогает обеспечить безопасность всей IoT-инфраструктуры. Централизованное управление и мониторинг событий KISG 1000 осуществляется с помощью платформы **Kaspersky Security Center**. Вместе эти два продукта образуют комплексное решение **Kaspersky IoT Infrastructure Security**.

На удаленных объектах в качестве ПЛК установлены контроллеры под управлением **KasperskyOS**.

На уровне облака защита осуществляется **Kaspersky Security для виртуальных и облачных сред**. Это комплексное решение для автоматизированной защиты инфраструктуры гибридного облака и предотвращения эксплуатации уязвимостей (в том числе нулевого дня) вредоносным ПО.

Подход «Лаборатории Касперского» к защите IoT



Кибериммунитет — новый подход к разработке исходно безопасных IT-решений на базе KasperskyOS. Такие решения защищены от подавляющего числа кибератак (как существующих, так и еще неизвестных) и будут выполнять свои критичные функции даже в условиях агрессивной среды.

KasperskyOS — операционная система, которая применяется там, где существуют повышенные требования к безопасности: в умном городе, транспорте, промышленности, электроэнергетике, госсекторе и других областях. Она позволяет обеспечить конфиденциальность и целостность данных и обезопасить их от подмены.

Функции Kaspersky IoT Secure Gateway 1000

Сбор данных	Защита шлюза	Защита IoT-инфраструктуры	Мониторинг
Агрегация собранных с датчиков данных и их передача по сотовым сетям и Ethernet. Работа с облачными системами по протоколу MQTT	Безопасность на уровне ядра операционной системы. Безопасная загрузка и обновление	Межсетевой экран для защиты от несанкционированного доступа. Технология обнаружения и предотвращения вторжений (IDS/IPS)	Обнаружение и категоризация устройств. Оповещение администратора о подключении новых устройств

Роли KISG 1000 в защите систем видеонаблюдения

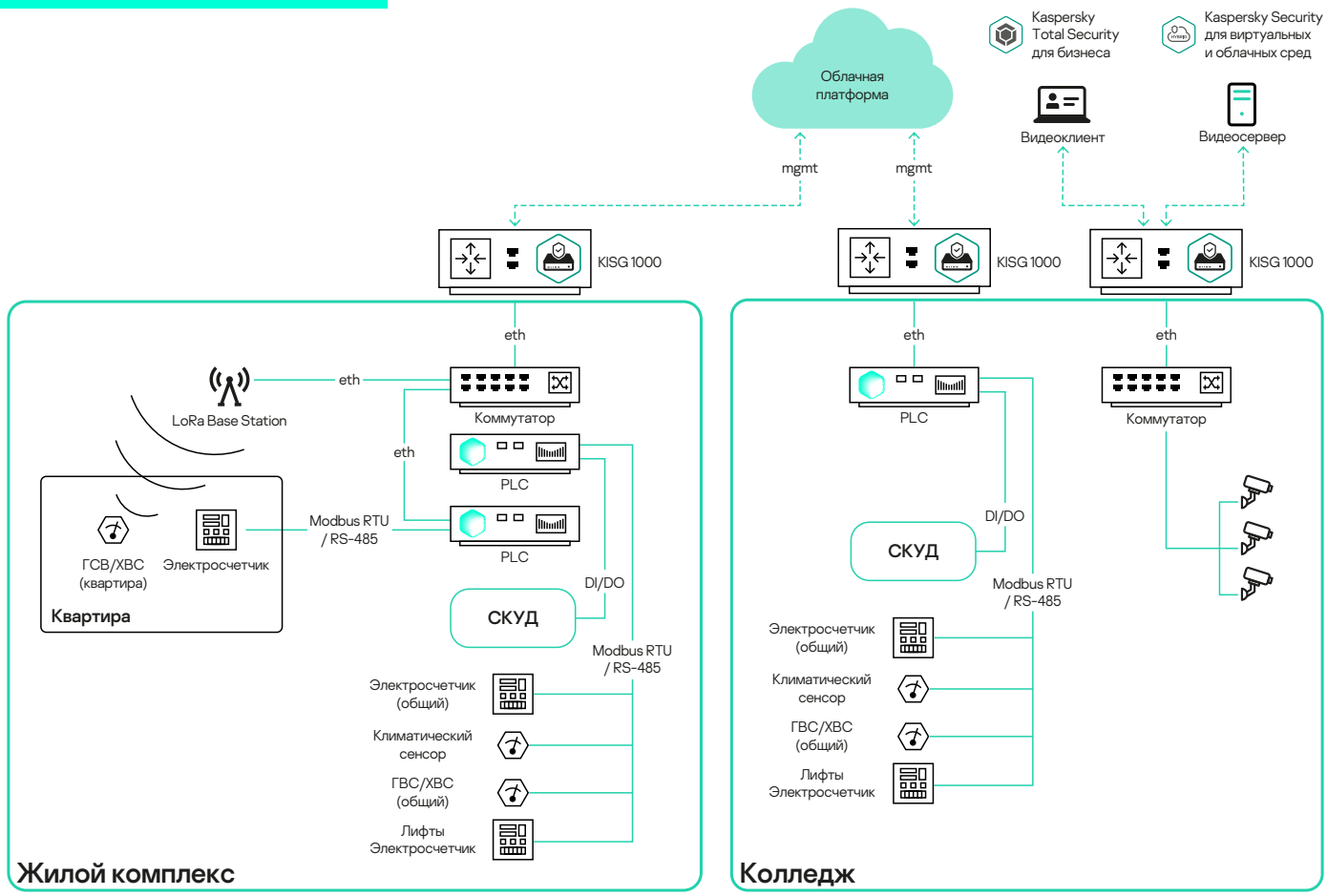
- Блокирует все неразрешенные взаимодействия между видеосервером и камерами
- Предотвращает атаки со стороны камер
- Блокирует попытки атак камеры со стороны видеосервера и видеоклиента
- Сообщает о появлении в локальной сети неавторизованного устройства (что также может свидетельствовать о подмене камеры)
- Сообщает о выведении камер из строя

В инфраструктуре умного города функции мониторинга и безопасности выполняют системы видеонаблюдения. Современные умные видеокамеры так же подвержены хакерским атакам, как и другие устройства интернета вещей.

Подход «Лаборатории Касперского» к защите локальных и облачных систем видеонаблюдения включает в себя:

- **Kaspersky IoT Infrastructure Security**
  - **Kaspersky IoT Secure Gateway 1000**
  - **Kaspersky Security Center**
- **Kaspersky Security для виртуальных и облачных сред**
- **Kaspersky Total Security для бизнеса** — защитное решение не только для конечных устройств и серверов, но и для других узлов корпоративной сети

Защита систем умного города с помощью технологий «Лаборатории Касперского»



KasperskyOS

Kaspersky IoT Infrastructure Security

Подробнее на os.kaspersky.ru

www.kaspersky.ru