Kaspersky Operating System:

Подход к защите инфраструктуры в рамках «Умного города»

kaspersky

Митюшин Дмитрий
Менеджер по развитию бизнеса
CISSP, CISM
Dmitry.Mityushin@Kaspersky.com

Умный город: прекрасная утопия

- Улучшение качества жизни людей
- Сокращение затрат и потребления ресурсов
- Увеличение прозрачности и оптимизации процессов
- Повышение производительности
- Извлечение доходов из новых типов данных

kaspersky

Базовые элементы Умного города

Городские сервисы и управление

ЖКХ и энергетика

Общественная безопасность

Умный транспорт и инфраструктура

Умная медицина

Системы предупреждения ЧС

kaspersky

IoT - более половины подключений к сети

24 млрд. IoT устройств к 2020 году

	2019	2025	CAGR
Wide-area IoT	1,5	5,4	21%
Short range IoT	9,3	19,5	11%
Мобильные телефоны	7,8	8,6	1.5%
ПК/Ноутбуки	1,6	17,3	1%
Стационарные телефоны	13,6	13,3	-1%

https://www.ericsson.com/en/mobility-report

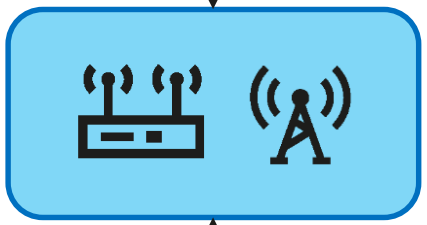
Mobility Report, Ericsson, 2019

kaspersky

Архитектура IoT

Системы управления, приложения

Связь и агрегация

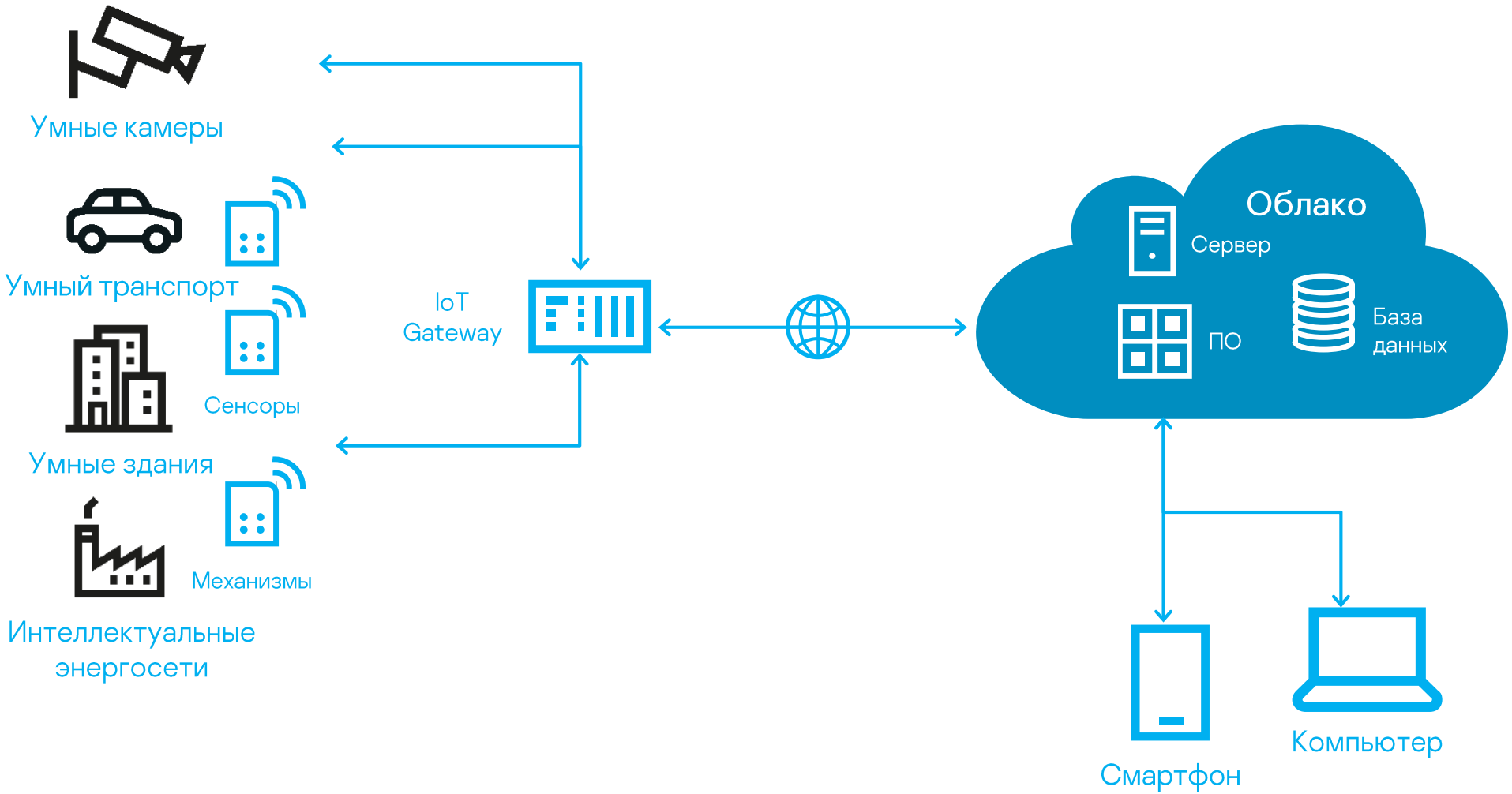


«Вещи»

Связь с физической реальностью

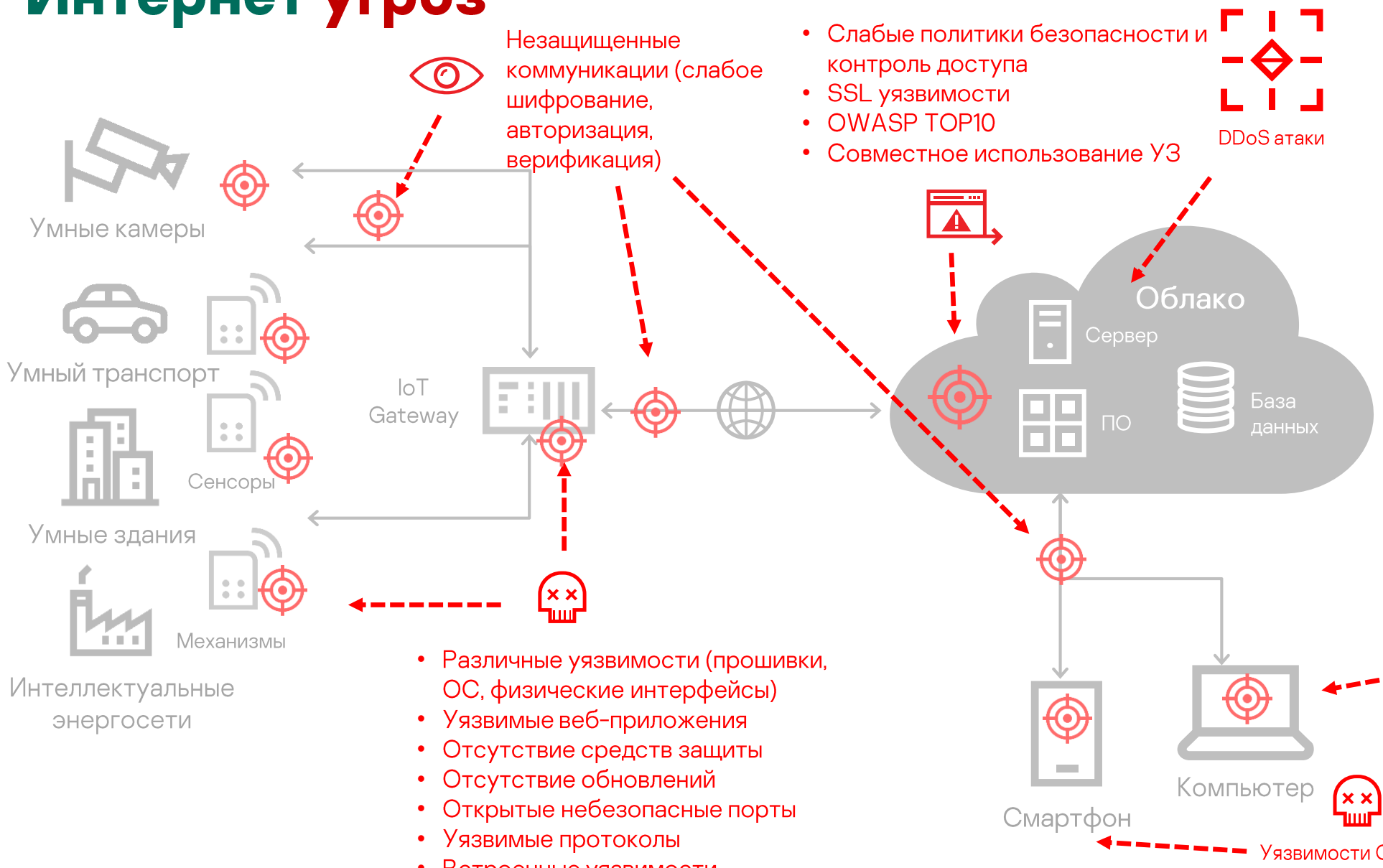
kaspersky

Интернет вещей



kaspersky

Интернет угроз



Примеры негативных сценариев:

- Включение устройств в бот-сети
- Изменение поведения устройств для слежки, саботажа
- Кража важных данных
- Взлом учетных записей
- Использование устройств как бекдоры для доступа к другим сетям
- Вторжение в частную жизнь
- Непредсказуемые физические последствия

kaspersky

Примеры исследований об уязвимостях Умного города

kaspersky

Атаки на Интернет вещей

MIRAI

Mirai впервые был обнаружен в августе 2016-го. Это исполняемый файл Linux (ELF), созданный для атак преимущественно на видеоприставки, роутеры, IP-камеры, Linux-серверы и другие устройства, использующие Busybox, распространенный среди IoT и встраиваемых устройств.

IoTroop/Reaper

Усовершенственная версия Mirai, которая способна эксплуатировать более 12 уязвимостей в IoT устройствах (роутеры, камеры, ТВ, видеоприставки и т.п.). В Феврале 2018 сообщалось о нескольких атаках на финансовый сектор, осуществленных с ботнетов устройств, зараженных IoTroop/Reaper. Исследователи заявляют о миллионах потенциально уязвимых устройств.

BASHLITE

IoT-троян, заражающий Linux-системы с целью организации распределенных DDoS-атак с устройств IoT. В 2014 BASHLITE эксплуатировал уязвимости Shellshock (так же известны как Bashdoor). В 2016 сообщалось о обнаружении 1 миллиона устройств, зараженных BASHLITE.

SATORI

Взлом устройств, использующих устаревшие версии прошивок. Ботнет сканировал устройства на открытые порты 52869 и 37215, ассоциированых с известными уязвимостями (CVE-2014-8361 уязвимость в Realtek SDK-based устройствах и CVE-2017-17215 zero-day в Huawei routers). Используя всего эти две уязвимости, Satori собрал от 500,000 до 700,00 устройств.

kaspersky

Уязвимости и атаки на городскую инфраструктуру

- Атаки на камеры фиксации нарушений ПДД (ЦОДД)

  https://www.interfax.ru/moscow/351263

- Исследование уязвимостей камер видеонаблюдения

  https://securelist.com/does-cctv-put-the-public-at-risk-of-cyberattack/70008/

- Уязвимости в датчиках дорожного движения

  https://securelist.ru/how-to-trick-traffic-sensors/28387/

- Уязвимости городских терминалов самообслуживания

  https://securelist.ru/fooling-the-smart-city/29286/

- Уязвимости в умных домах и зданиях

  https://threatpost.com/smart-locks-bricked-by-bad-update/127427/
  https://securelist.ru/fibaro-smart-home/94294/

- Исследование уязвимостей в системах подключенных автомобилей и car sharing

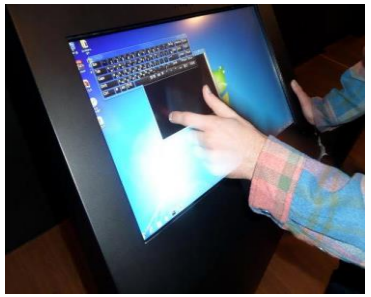
  https://securelist.ru/on-the-iot-road/94389/
  https://securelist.ru/a-study-of-car-sharing-apps/90804/

- Исследование уязвимостей публичных Wi-Fi сетей (FIFA2018)

  (https://securelist.ru/fifa-public-wi-fi-guide/90142/)

- ...

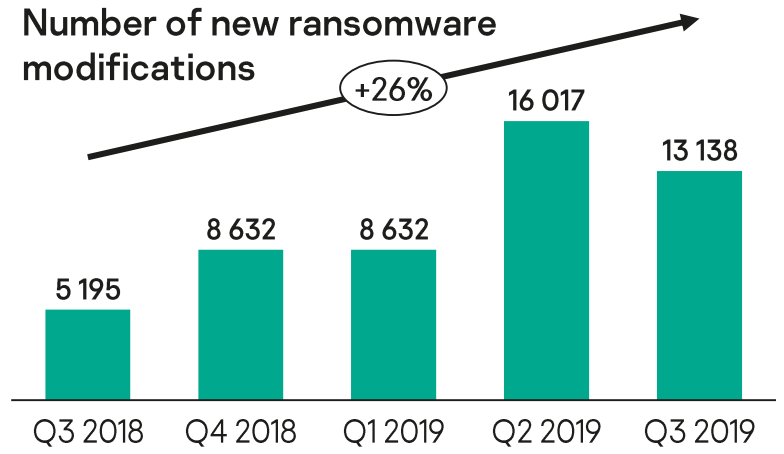




kaspersky

Атаки шифровальщиков на городскую инфраструктуру

- 174 муниципальных организации столкнулись с шифровальщиками в 2019 году.
- В мае 2019 года вымогатель Robin Hood полностью парализовал городские службы Балтимора. Чиновники потратили $ 18 млн. на восстановление своей ИТ-инфраструктуры.
- Июнь 2019 года. Флорида-Сити заплатила $ 600 тыс. хакерам, захватившим контроль над ее компьютерной системой.
- Июнь 2019 года, Лейк-Сити был атакован вредоносным ПО, известным как «Triple Threat», городское правительство одобрило выплату $ 460 тыс.
- ...

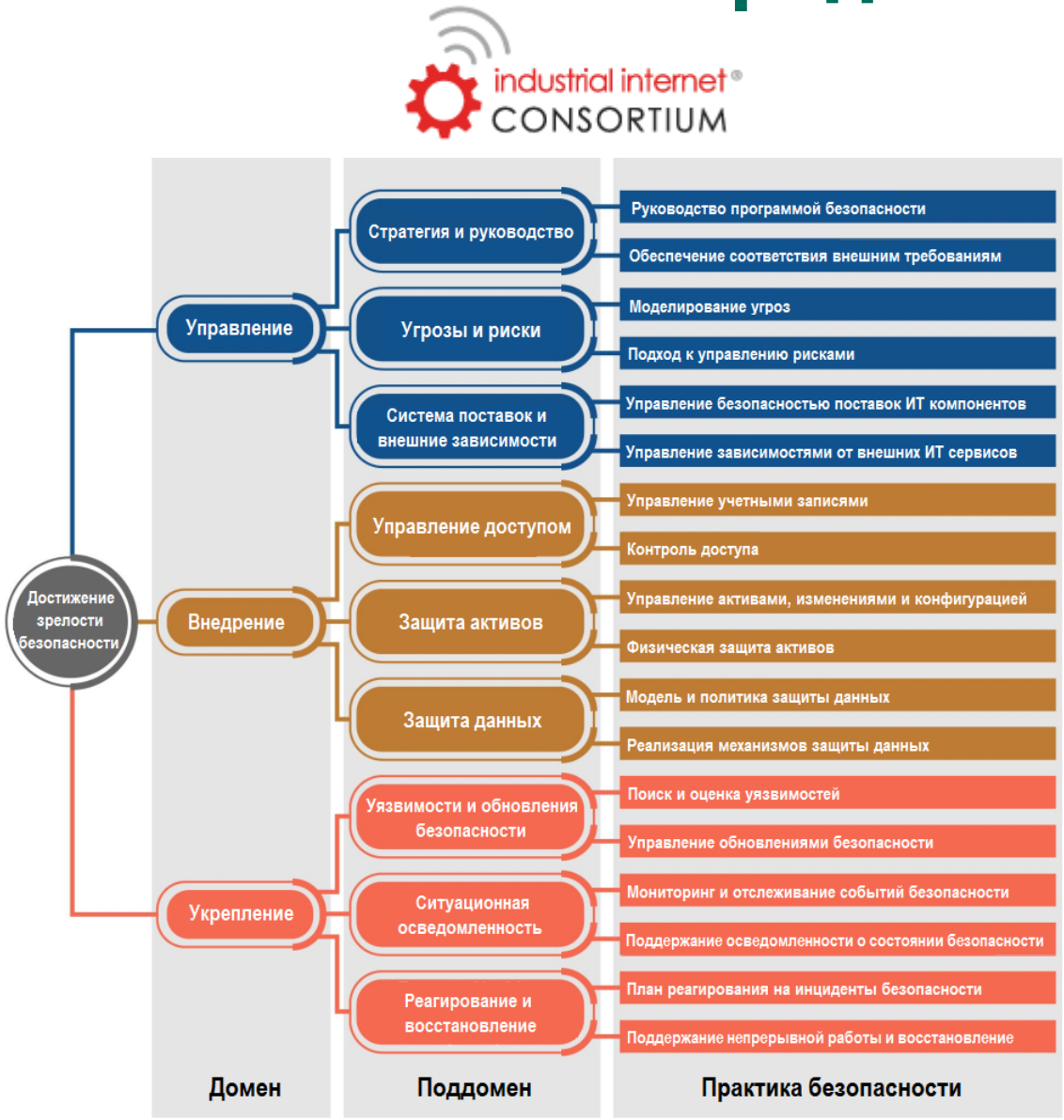


https://securelist.ru/story-of-the-year-2019-cities-under-ransomware-siege/95280/
https://www.kaspersky.ru/blog/baltimore-encrypted/22787/

kaspersky

Стратегия обеспечения безопасности Умного города

- Организационные
  - Применение стандартов (ISO,IEC, и д.р.)
  - Обучение и повышение осведомленности
- Технологические
  - Анализ угроз и рисков
  - Своевременное внедрение мер информационной безопасности
  - Применение ИММУННЫХ информационных систем



kaspersky

Безопасный фундамент для систем будущего

KasperskyOS

- Встроенная безопасность
- Микроядерная архитектура
- Разделение на домены безопасности
- Доверенное поведение

kaspersky

Не общее, а целевое назначение

ПРИМЕНЕНИЕ:

Телекоммуникационное оборудование

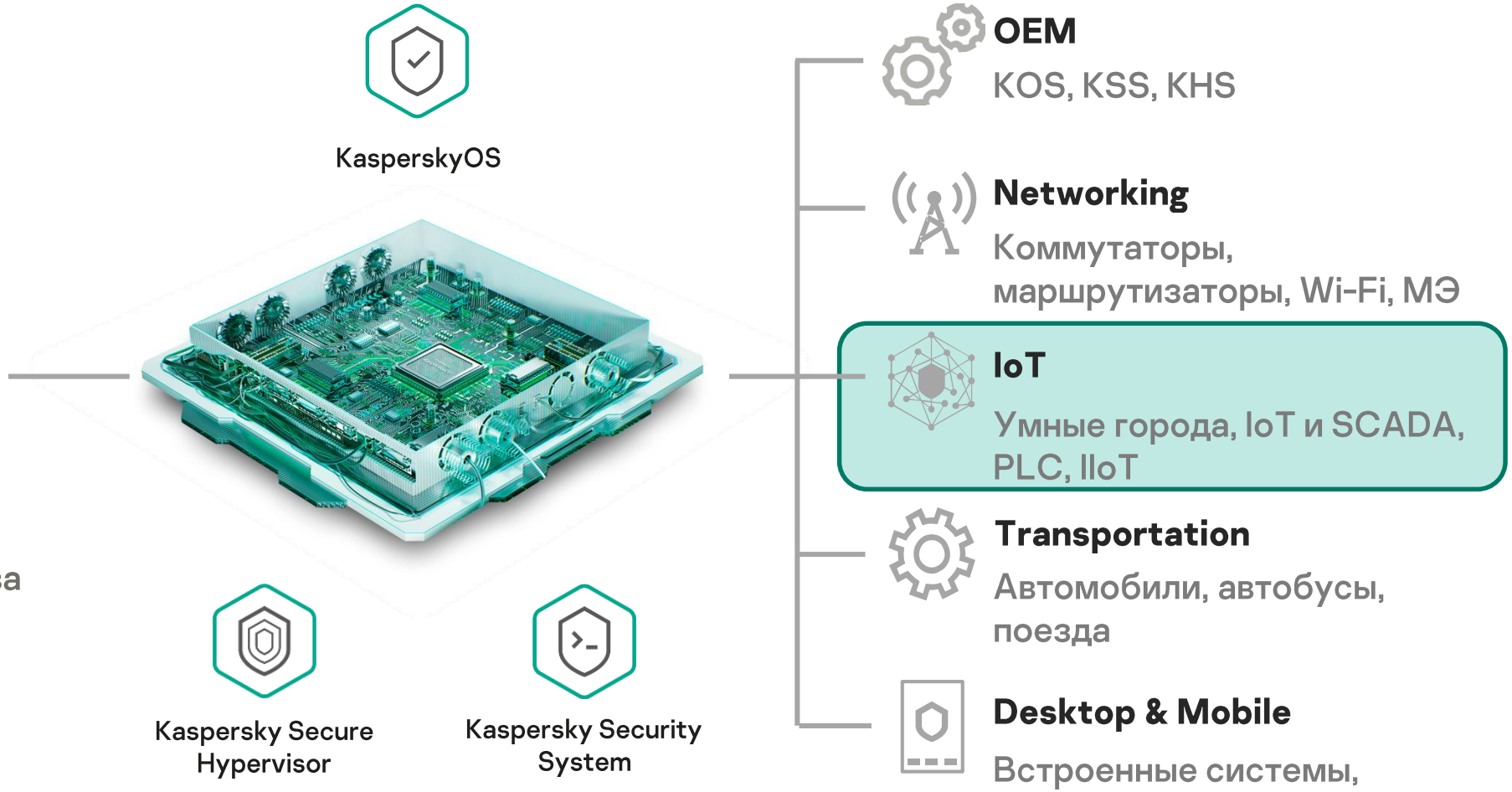
Интернет вещей и промышленный интернет вещей

Системы промышленной автоматизации

Транспортные системы

Пользовательские устройства

Компьютерные системы специального назначения



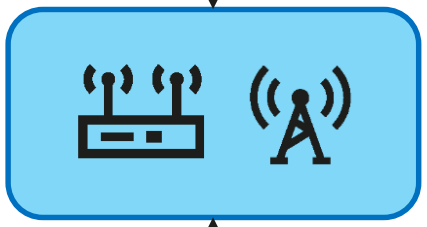
https://os.kaspersky.ru/markets/
https://os.kaspersky.ru/projects/

kaspersky

Технологии защиты инфраструктуры IoT

Системы управления, приложения

Связь и агрегация



«Вещи»

Стандартные средства защиты

Kaspersky IoT Vulnerability Monitor

Kaspersky IoT Secure Gateway

KasperskyOS

kaspersky

Kaspersky IoT Secure Gateway (Шлюз безопасности IoT)

Задача: Обеспечение сетевого транспорта (сбор и управление) и защиты инфраструктуры IoT

Доверенная ОС

IBM Bluemix
Yandex Core
ISS Inspark

MQTT
протокол

Обнаружение и
классификация
устройств

Централизованное
управление

МЭ,
IDS / IPS

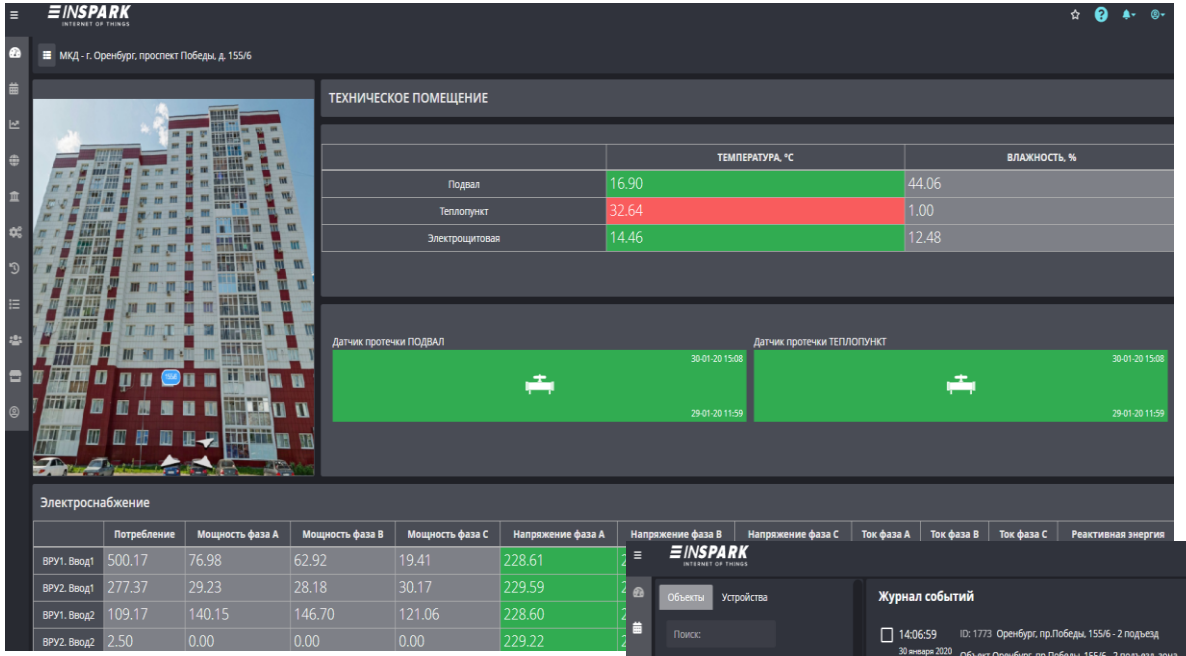
kaspersky

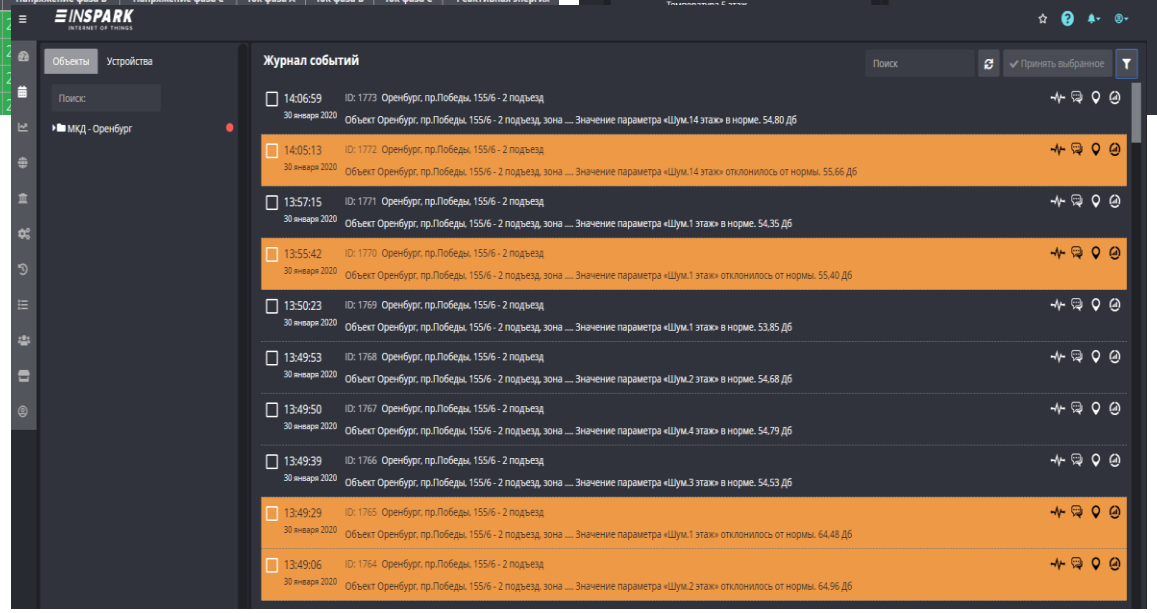
Облачная диспетчерская (г. Оренбург)

- Удаленный мониторинг общедомовых показателей и инженерных систем
  - Параметры электроснабжения
  - Параметры водоснабжения
  - Параметры теплоснабжения
  - Параметры комфортности среды в подъездах: (Температура; Освещенность; Влажность; Уровень CO2; Уровень шума)
  - Работоспособность лифтов, открытие дверей в шахтах
  - Работоспособность домофонов
  - Срабатывание пожарной сигнализации
  - Срабатывание систем контроля доступа
- Оптимизация затрат на обслуживание инженерных систем
- Уменьшение потребление ресурсов
- Увеличение скорости реагирования на аварии и инциденты
- Контроль качества жилищно-коммунального хозяйства

kaspersky

Облачная диспетчерская (г. Оренбург)





ИНФОРМАЦИОННЫЕ СИСТЕМЫ И СТРАТЕГИИ

INSPARK SERVICE MANAGEMENT

KasperskyOS

kaspersky

Спасибо за внимание!

Наш стенд – A10

https://os.kaspersky.ru/

kaspersky

Митюшин Дмитрий
Менеджер по развитию бизнеса
CISSP, CISM
Dmitry.Mityushin@Kaspersky.com