Кибербезопасный умный город

Алексей Лафицкий
Руководитель по продажам
продуктов на базе KasperskyOS

kaspersky

Содержание

kaspersky

Базовые элементы

Умная городская среда

Интеллектуальные системы экологической безопасности

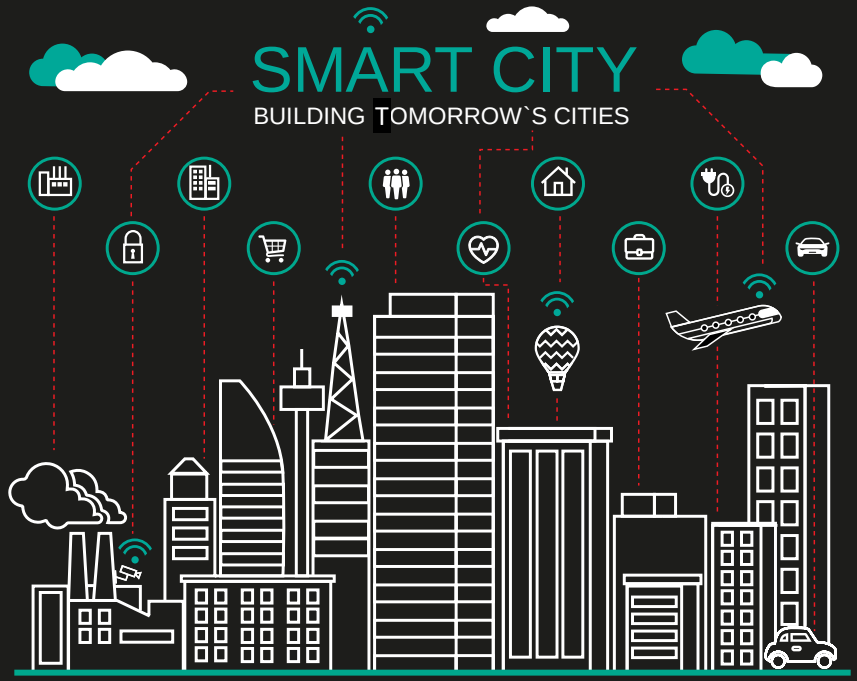
Умное ЖКХ

Умный городской транспорт

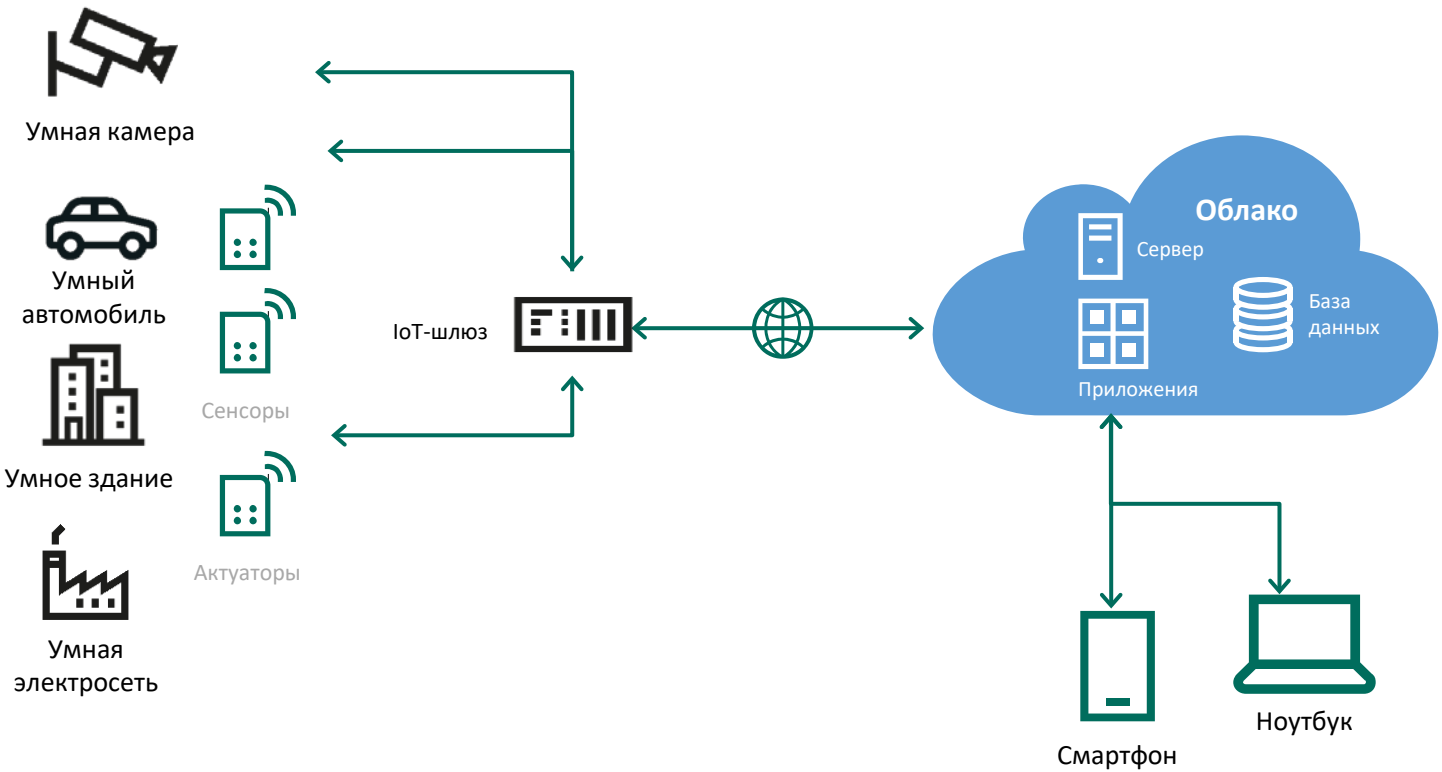
Интеллектуальные системы общественной безопасности

Интеллектуальный центр городского Управления

Умный город

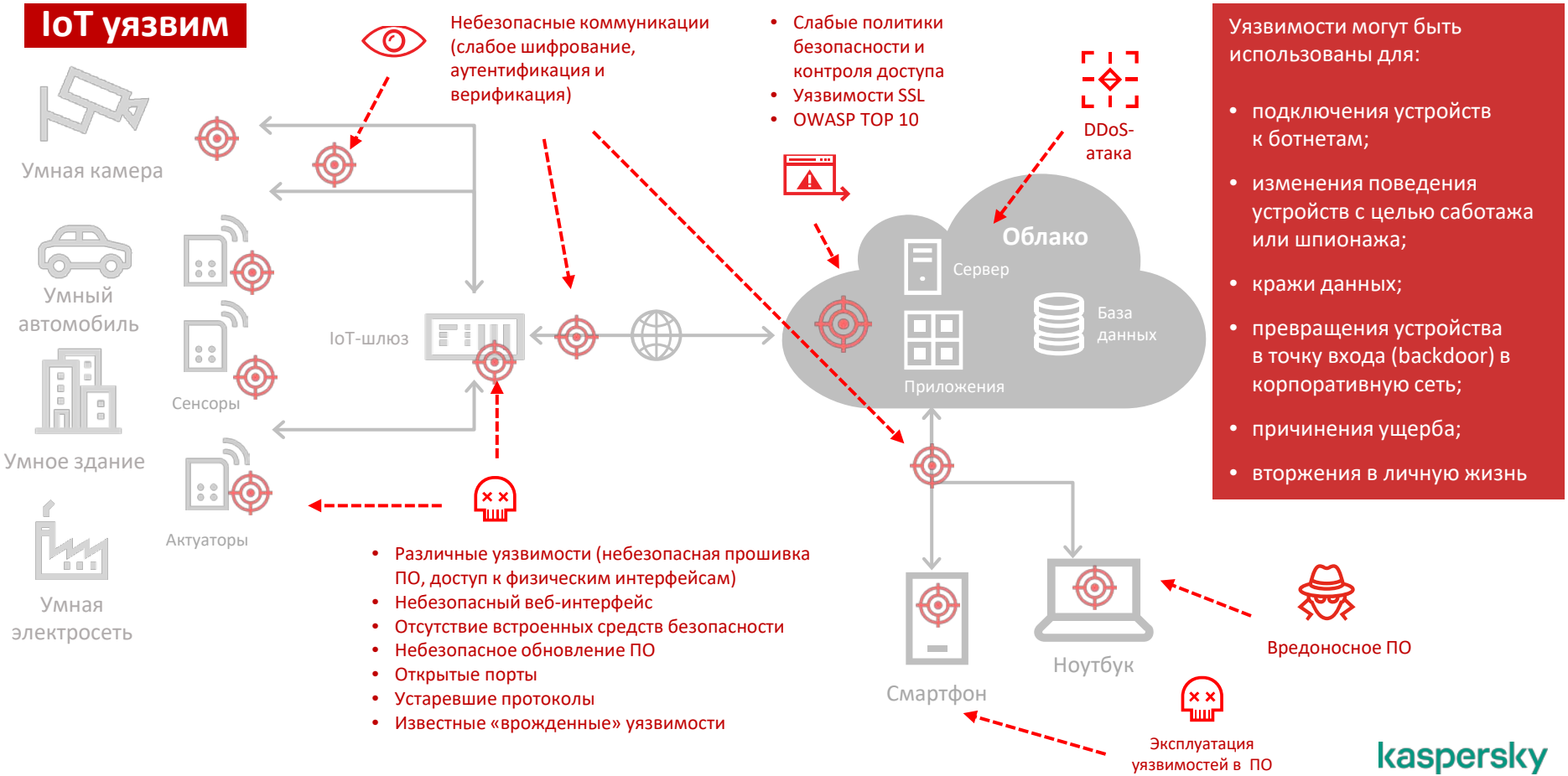


Различные вертикали используют IoT-технологии



kaspersky

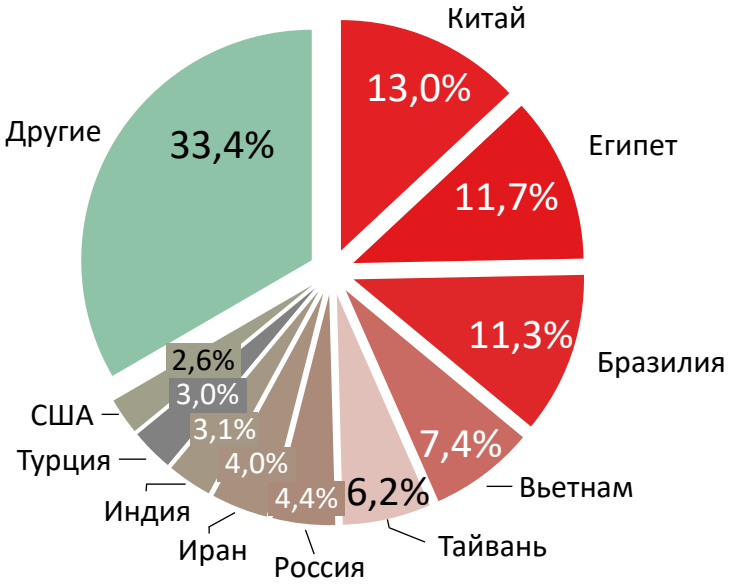
Различные вертикали используют IoT-технологии



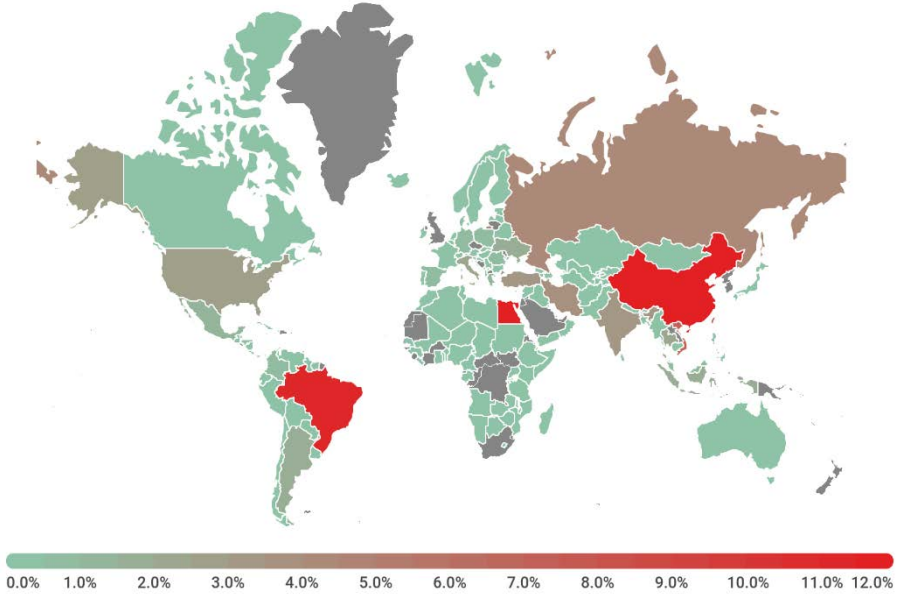
kaspersky

Исследование «Лаборатории Касперского»: атаки на устройства IoT (Q1/2020)

Топ-10 стран, в которых располагались устройства, осуществлявшие атаки на Kaspersky Honeypots



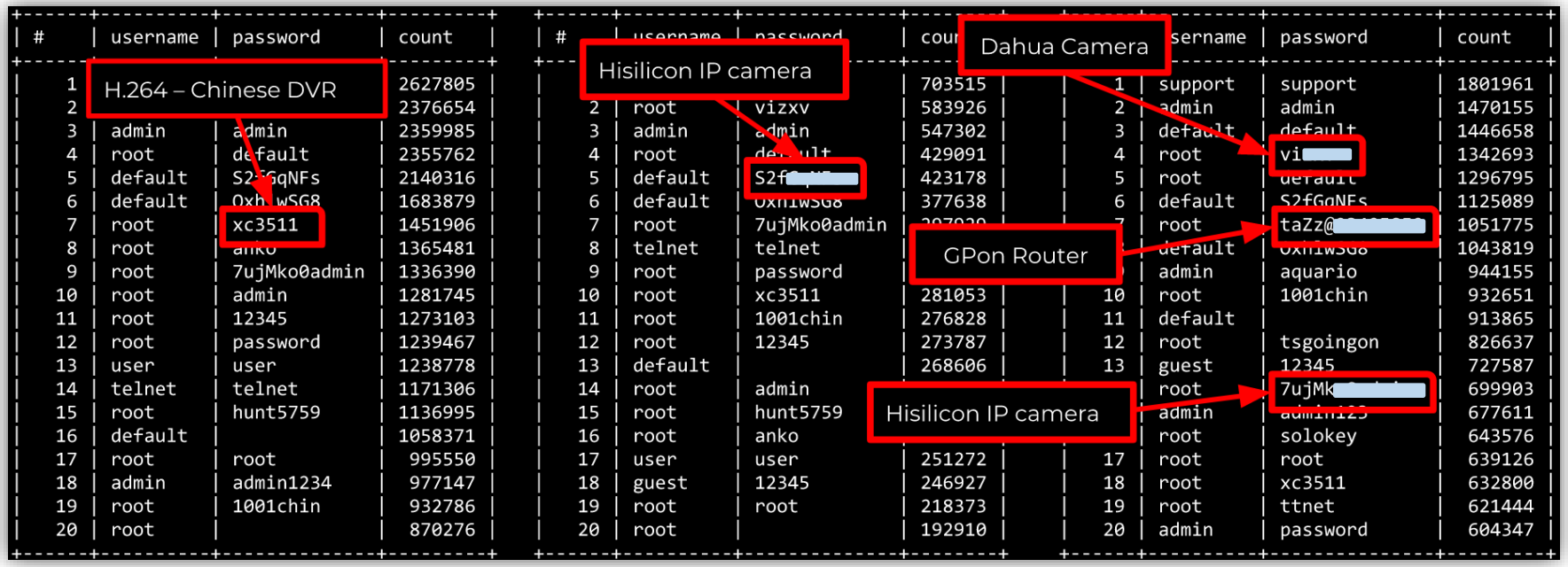
География IP-адресов устройств, с которых были предприняты атаки на Kaspersky Honeypots



https://securelist.com/it-threat-evolution-q1-2020-statistics/96959/

kaspersky

Kaspersky's research:
Top 20 passwords used for attacking IoT devices



#	username	password	count
1			2627805
2			2376654
3	admin	admin	2359985
4	root	default	2355762
5	default	S2fGqNFs	2140316
6	default	Oxhlw5G8	1683879
7	root	xc3511	1451906
8	root	anko	1365481
9	root	7ujMko0admin	1336390
10	root	admin	1281745
11	root	12345	1273103
12	root	password	1239467
13	user	user	1238778
14	telnet	telnet	1171306
15	root	hunt5759	1136995
16	default		1058371
17	root	root	995550
18	admin	admin1234	977147
19	root	1001chin	932786
20	root		870276

2018 – Q3

#	username	password	count
1			703515
2	root	vizxv	583926
3	admin	admin	547302
4	root	default	429091
5	default	S2fGqNFs	423178
6	default	Oxhlw5G8	377638
7	root	7ujMko0admin	207020
8	telnet	telnet	
9	root	password	
10	root	xc3511	281053
11	root	1001chin	276828
12	root	12345	273787
13	default		268606
14	root	admin	
15	root	hunt5759	
16	root	anko	
17	user	user	251272
18	guest	12345	246927
19	root	root	218373
20	root		192910

2018 – Q4

#	username	password	count
1	support	support	1801961
2	admin	admin	1470155
3	default	default	1446658
4	root	vi	1342693
5	root	default	1296795
6	default	S2fGqNFs	1125089
7	root	taZz@	1051775
8	default	Oxhlw5G8	1043819
9	admin	aquario	944155
10	root	1001chin	932651
11	default		913865
12	root	tsgoingon	826637
13	guest	12345	727587
14	root	7ujMk	699903
15	admin	admin123	677611
16	root	solokey	643576
17	root	root	639126
18	root	xc3511	632800
19	root	ttnet	621444
20	admin	password	604347

2019 – Q1

https://securelist.com/iot-a-malware-story/94451/

kaspersky

Примеры IoT-зловредов

MIRAI

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

IoTroop/Reaper

Усовершенствованная версия Mirai, которая может эксплуатировать более 12 уязвимостей в IoT-устройствах (роутеры, камеры, телевизоры, телеприставки и т.п.). В феврале 2018 года сообщалось о нескольких атаках на финансовый сектор, осуществленных с ботнет-устройств, зараженных IoTroop/Reaper. Исследователи заявляют о миллионах потенциально уязвимых устройств.

BASHLITE

IoT-троян, заражающий Linux-системы для организации распределенных DDoS-атак с устройств IoT. В 2014 году BASHLITE эксплуатировал уязвимости Shellshock (также известные как Bashdoor). В 2016 году сообщалось об обнаружении 1 миллиона устройств, зараженных BASHLITE.

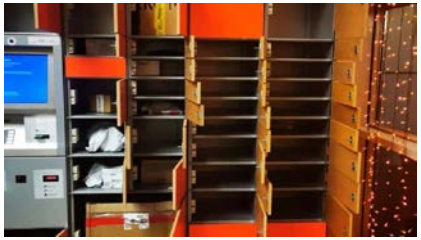
SATORI

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

Кибератаки в 2020 году

Атака на камеры видео наблюдения

В 2020 году хакеры скомпрометировали 15 тысяч камер наблюдения в Москве. В результате пострадали устройства, расположенные в жилых домах, магазинах, банках, торговых центрах и других частных организациях.



Атака на PickPoint

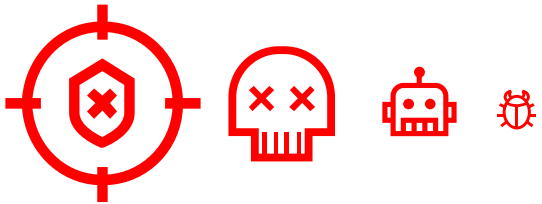
В конце 2020 года произошла первая в мире атака на постаматы. Из 8000 точек, которые обслуживает компания PickPoint, 2732 пункта было выведено из работы в результате кибератаки.

Кибератаки на медицинские учреждения

10% всех организаций, подвергшихся кибератакам в 2020 году, – госпитали и другие медучреждения

В 2020 году был подтвержден первый случай, когда в результате кибератаки на устройства госпиталя умер пациент – ему вовремя не оказали экстренную помощь

В начале пандемии был атакован крупнейший госпиталь в Чехии, занимающийся лечением больных COVID-19



Эксплуатация уязвимостей

Регулирующие документы

- ISO/IEC 30146:2019
- ПНСТ «Информационные технологии. Умный город. Показатели ИКТ»
- ПНСТ «Информационные технологии. Умный город.
  Общая схема развития и функционирования»
- ПНСТ «Информационные технологии. Умный город.
  Руководства по обмену и совместному использованию данных»
- ПНСТ «Информационные технологии. Умный город.
  Общие положения по интеграции и функционированию инфраструктур умного города»
- ПНСТ «Информационные технологии. Умный город.
  Руководящие указания по передовой практике в области перевозок»
- ПНСТ «Информационные технологии. Умный город. Функциональная совместимость»
- И другие

Kaspersky IoT Infrastructure Security

Комплексная защита инфраструктуры интернета вещей

Kaspersky IoT Secure Gateway β*

Основа Kaspersky IoT Infrastructure Security

Защищенный шлюз для безопасных систем интернета вещей

- Обнаружение и классификация устройств
- Регистрация событий безопасности в IoT-системах
- Защита от сетевых атак (IDS/IPS)

Kaspersky Security Center

Централизованное управление и мониторинг всех объектов IoT-инфраструктуры

- Контроль безопасности из единого центра
- Журналирование и отчетность
- Удобные оповещения об инцидентах

* Текущая версия продукта предназначена для некоммерческого пилотирования

kaspersky

Кооперация с компанией Advantech (Тайвань)

Разработан Kaspersky IoT Secure Gateway **β***
на базе платформы **Advantech UTX-3117**

UTX-3117 Спецификация оборудования	
Процессорная система	Intel Pentium N4200, 2MB L2 Cache
RAM	Двойной канал DDR3L 1600MHz, 4GB
Ethernet	Поддержка Dual 10/100/1000Mbps LAN LAN1: Intel I210AT LAN2: Realtek RTL8111G
I/O-интерфейсы	1 x RS-232 с 5v/12v 2 x порта USB3.0 1 x интерфейс SATA, бортовая поддержка SSD TPM Infineon SLB9665. Поддержка TPM2.0
Хранение данных	1 x отсек SATA II SSD (32GB) mSATA 1, совместное использование со слотом H/S miniPCIE

* Текущая версия продукта предназначена для некоммерческого пилотирования

Проект «Умный город» (г. Оренбург)

Облачная диспетчерская

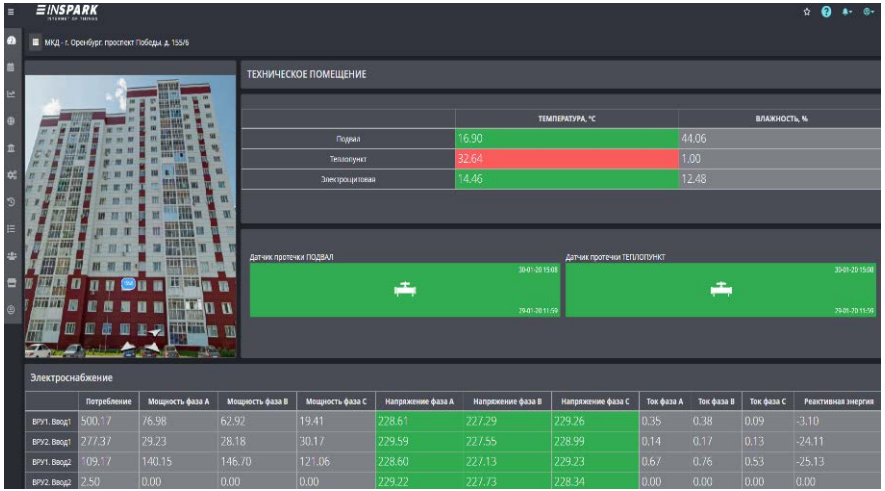
Облачная платформа

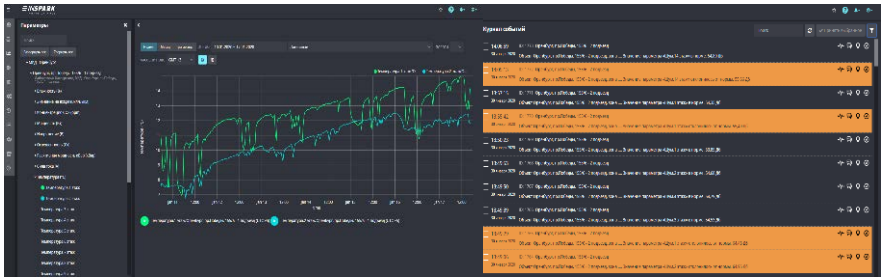
INSPARK SERVICE MANAGEMENT

Контроллеры

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И СТРАТЕГИИ

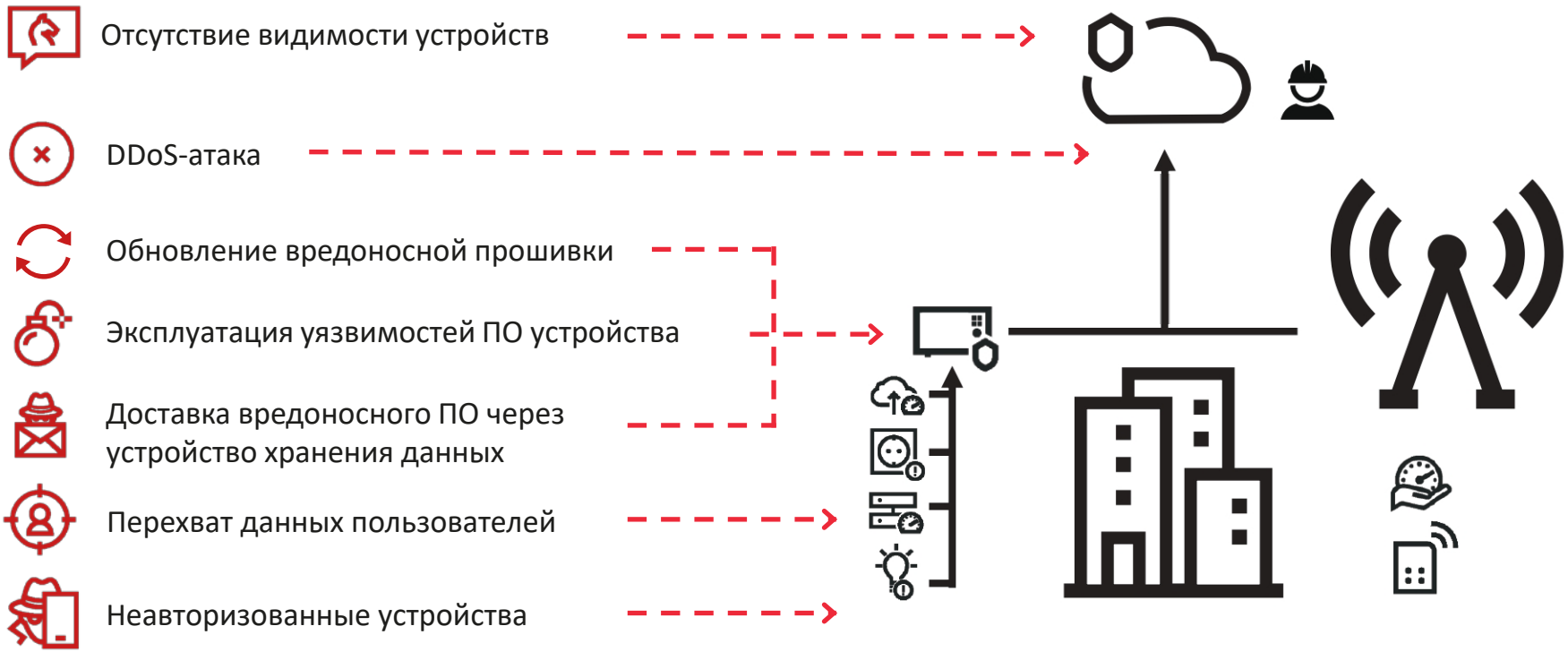
«Вещи»: сенсоры, датчики, актуаторы, …





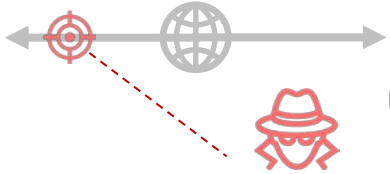
kaspersky

Потенциальные киберугрозы для облачной диспетчеризации



Защита систем видеонаблюдения

Kaspersky
IoT Secure Gateway β*



Внешние угрозы

- Сканирование интернета
- Эксплуатация уязвимостей
- Неавторизованный доступ

Kaspersky
IoT Secure Gateway β*

Доступ к
локальной сети

- Физическое подключение через внешние интерфейсы, перепрошивка
- Изменение конфигурации, смена пароля, подделка сертификата SSL
- Вредоносное ПО
- Замена SIM-карты

- Защита от угроз со стороны камер
- Защита облачных систем видеонаблюдения
- Инвентаризация устройств
- Ограничение доступа к видеосерверу

kaspersky

Спасибо!

Sales-KasperskyOS@kaspersky.com

Стенд C80

kaspersky