kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky IoT Infrastructure Security

Комплексная защита инфраструктуры интернета вещей

Интернет вещей меняет мир прямо на наших глазах. Он может сделать его безопаснее и комфортнее, помочь экономить ресурсы и эффективно управлять целыми производствами.

Концепция IoT охватывает огромное количество устройств, технологий, программного обеспечения и протоколов передачи данных. Эта неоднородная среда подвержена множеству рисков, которые могут угрожать безопасности различных сторон нашей жизни.

Сложность инфраструктуры интернета вещей предоставляет злоумышленникам массу возможностей для осуществления различных атак. Например, производители конечных умных устройств часто игнорируют основные принципы кибербезопасности: аппаратное обеспечение не контролирует целостность прошивки, устройства поставляются с предустановленными паролями (включая пароли администратора), не говоря уже о слабых настройках сетевой безопасности или использовании старых и уязвимых версий программного обеспечения.

Получается, что **основным источником угроз для интернета вещей является он сам** – его инфраструктурная и технологическая сложность в совокупности с высокими темпами его развития.

Векторы угроз для IoT

Kaspersky IoT Infrastructure Security – это комплексное решение для защиты и контроля инфраструктуры интернета вещей на всех уровнях: от самих умных устройств, гейтвеев и облачных платформ до каналов передачи данных. Основным его компонентом является продукт **Kaspersky IoT Secure Gateway**, который обеспечивает безопасность систем на уровне шлюзов. Мониторинг и управление осуществляются с помощью **Kaspersky Security Center**.

Kaspersky
IoT Secure Gateway

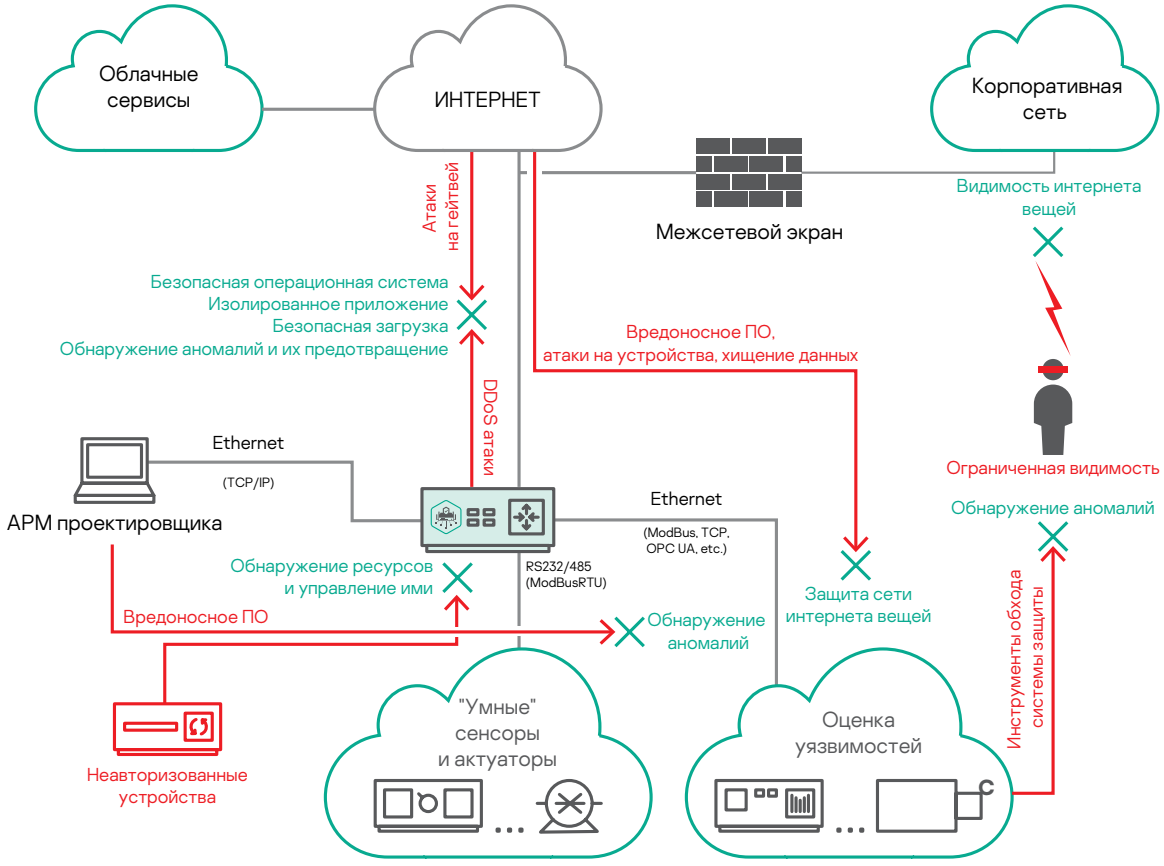
Kaspersky IoT Secure Gateway β*

Защищенный шлюз для безопасного интернета вещей

Одно из самых важных, но в то же время уязвимых устройств в IoT-сети – гейтвей, или шлюз. Подключение к внешним сетям и зачастую прошивка на базе устаревших версий ОС делают его мишенью для атак и внедрения вредоносного ПО. Кроме того, злоумышленники могут воспользоваться его мощными вычислительными способностями. Поэтому из всех элементов IoT-инфраструктуры гейтвей нуждается в надежной защите в первую очередь.

Продукт **Kaspersky IoT Secure Gateway** на основе KasperskyOS предназначен для построения безопасных систем интернета вещей. Он защищает данные на уровне шлюзов, получая, проверяя и распределяя сообщения датчиков, полученные по протоколу MQTT, а также передавая управляющие команды на актуаторы. К основным функциям безопасности продукта относятся обнаружение и классификация устройств, регистрация событий безопасности в IoT-системах и защита от сетевых атак (IDS/IPS).

Kaspersky IoT Secure Gateway можно настраивать и дополнять функционалом продукции партнеров.

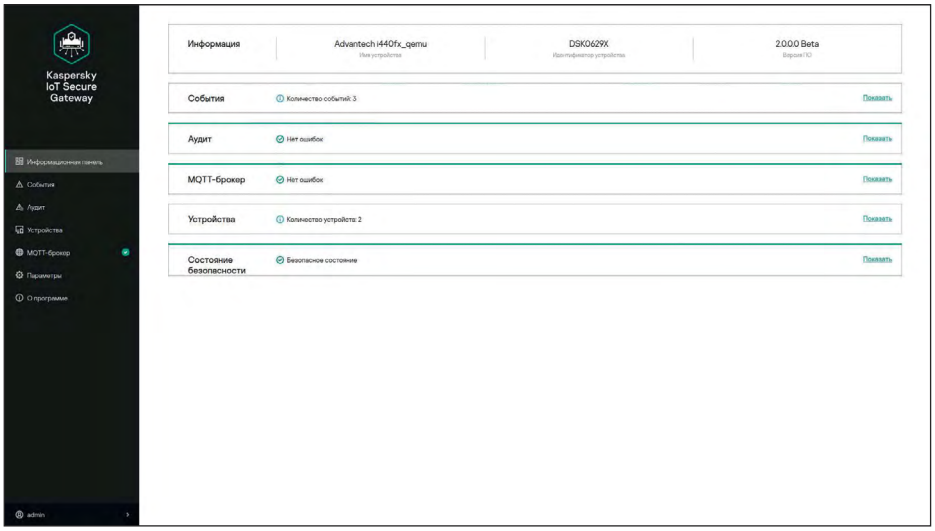


Защита IoT с использованием Kaspersky IoT Secure Gateway

* Текущая версия продукта предназначена для некоммерческого пилотирования

Возможности и преимущества

Подключение	
Ethernet	Подключение к сетям передачи данных через протокол Ethernet
Маршрутизация и NAT	Связь между внутренней и внешней сетями; использование механизмов NAT
DHCP-сервер	Построение сетей конечных устройств с функцией динамического выделения их IP-адресов
MQTT-брокер	MQTT-брокер на базе Mosquitto позволяет осуществлять сбор данных и управление подключенными IoT-устройствами (сенсорами и актуаторами, умными реле и т.д.)
OpenSSL/TLS	Поддержка распространенных механизмов криптографической защиты передаваемых данных
MQTT поверх TLS	Безопасное подключение и защищенная передача данных между шлюзом и облачной платформой
Интеграция с облачными сервисами	MS Azure, Amazon AWS, IBM Bluemix и т.д. Работа с любыми облачными системами по протоколу MQTT; поддержка одновременной работы с несколькими облачными платформами
Мониторинг	
IoT Device Detection & Classification	Обнаруживает и категоризирует IoT-устройства на основе их сетевой активности. В пользовательском интерфейсе можно увидеть все устройства сети, а новые будут обнаружены при подключении к ней в течение 60 секунд
Отчеты и уведомления (MQTT, SYSLOG, Push-уведомления)	При обнаружении нового подключенного к сети устройства администратору будет отправлено соответствующее оповещение
Гибкое управление защитой и шлюзом	
Веб-интерфейс	Удобная настройка и мониторинг IoT-сети, видимость и прозрачность благодаря WebGUI. Информативный дэшборд позволяет быстро получить все необходимые сведения
Защита IoT-шлюза от кибератак	
Исходная безопасность	Безопасность на уровне ядра операционной системы (KasperskyOS)
Безопасная загрузка (Secure Boot)	Верификация целостности и подлинности прошивки с использованием криптографических методов на IoT-устройствах перед загрузкой образа. Несанкционированно измененная или поврежденная прошивка не будет загружена. Безопасная загрузка может использоваться совместно с аппаратным хранилищем ключей
Безопасное обновление (Secure Update)	Работая в комплексе с Безопасной загрузкой, технология позволяет обновлять прошивку только с использованием правильно подписанных и зашифрованных образов из доверенных источников
Защита IoT-инфраструктуры	
IDS/IPS и межсетевой экран (Firewall)	Два дополняющих друг друга механизма для защиты от сетевых атак. Межсетевой экран защищает от несанкционированного сетевого доступа, а обнаружение вредоносной активности (IPS/IDS) позволяет своевременно заблокировать атаку на узлы защищаемой сети
Корень доверия (Root of trust)	Этот подход базируется на цепочке доверия (chain of trust). Начальная точка доверия выбирается в зависимости от требуемых гарантий и в сложных случаях устанавливается на уровне аппаратной части



Интерфейс Kaspersky IoT Secure Gateway β*

Спецификация поддерживаемого аппаратного обеспечения

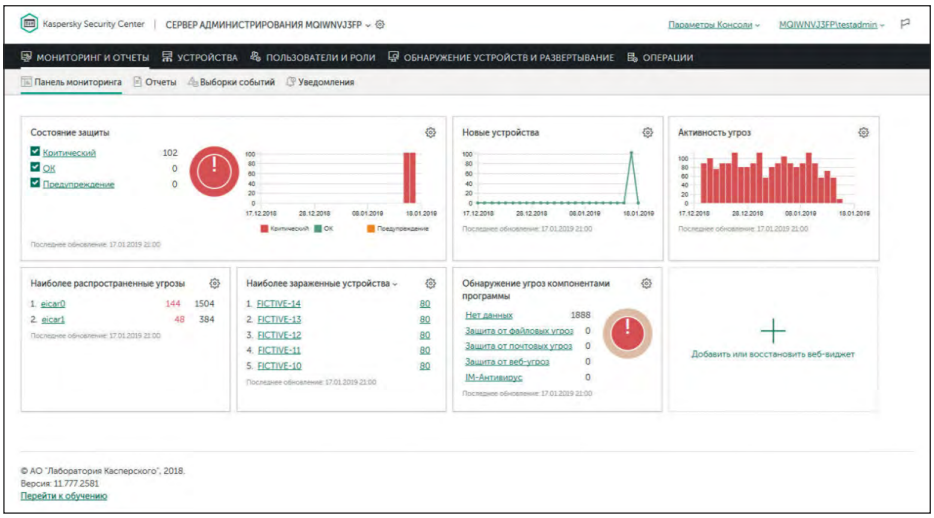
Advantech UTX-3117	
Процессорная система	Процессор серии Intel Apollo Lake E3900 & N, 2MB L2 Cache
RAM	Двойной канал DDR3L 1867MHz, до 8GB
Графика	Интерфейс Intel Apollo Lake E3900 Series SoC, Intel Apollo Lake N series SoC HDMI: 1, макс. разрешение до 3840 x 2160 @ 30Hz DP1.2: 1, макс. разрешение до 4096 x 2160 @ 60Hz
Ethernet	Поддержка Dual 10/100/1000 Mbps LAN LAN1: Intel I210AT LAN2: Realtek RTL8111G
I/O-интерфейсы	1 x RS-232 с 5v/12v 1 x RS-422/485 full duplex с разъемом Phoenix 2 x порта USB3.0 1 x интерфейс SATA, бортовая поддержка чипа SSD TPM Infineon SLB9665. Поддержка TPM2.0
Хранение данных	1 x отсек SATA II SSD mSATA 1, совместное использование со слотом H/S miniPCIE
Расширение	1 x поддерживающий полуразмерный Mini PCIe модуль Sub1G или mSATA 1 x полноразмерный модуль Mini PCIe с поддержкой 3G/LTE и держателем SIM 1 x модуль Wi-Fi M.2 с поддержкой электронных ключей

* Текущая версия продукта предназначена для некоммерческого пилотирования

Kaspersky Security Center

Kaspersky Security Center

Централизованное управление и мониторинг Kaspersky IoT Secure Gateway и всех объектов IoT-инфраструктуры



Интерфейс Kaspersky Security Center

Возможности и преимущества

Kaspersky Security Center содержит инструменты и технологии, образующие передовую интегрированную платформу для централизованного администрирования и мониторинга, а также обеспечения безопасности IoT-систем.

Упрощает выполнение повседневных задач

Уменьшает уязвимость к атакам

Помогает защитить все рабочие места и серверы

Облегчает администрирование

Обеспечивает целостность систем

Предоставляет полный обзор IT-среды

Единая консоль управления	Автоматизация, прозрачность, снижение расходов и повышение эффективности администрирования; корреляция событий из разных источников IoT-систем. Ограничение использования неподходящих или небезопасных приложений, устройств и веб-сайтов. Быстрое и простое применение политик безопасности на всех рабочих местах
Доступ на основе ролей	Каждый администратор может обращаться только к тем инструментам и данным, которые имеют отношение к его служебным обязанностям
Простое масштабирование	Масштабирование без изменения первоначальной настройки: управление до 100 000 физических, виртуальных и облачных рабочих мест с помощью одного сервера Kaspersky Security Center. Оптимизированные возможности резервного копирования
Расширяемая архитектура	В случае приобретения или выпуска нового приложения можно установить соответствующее расширение без повторной установки или исправления консоли.
Удобное оповещение	Уведомления об инцидентах через различные каналы, удобные администратору (SMS, e-mail, push и т.д.)
Гибкая система отчетности	Настраиваемые и готовые отчеты с динамической фильтрацией и сортировкой по любому полю.

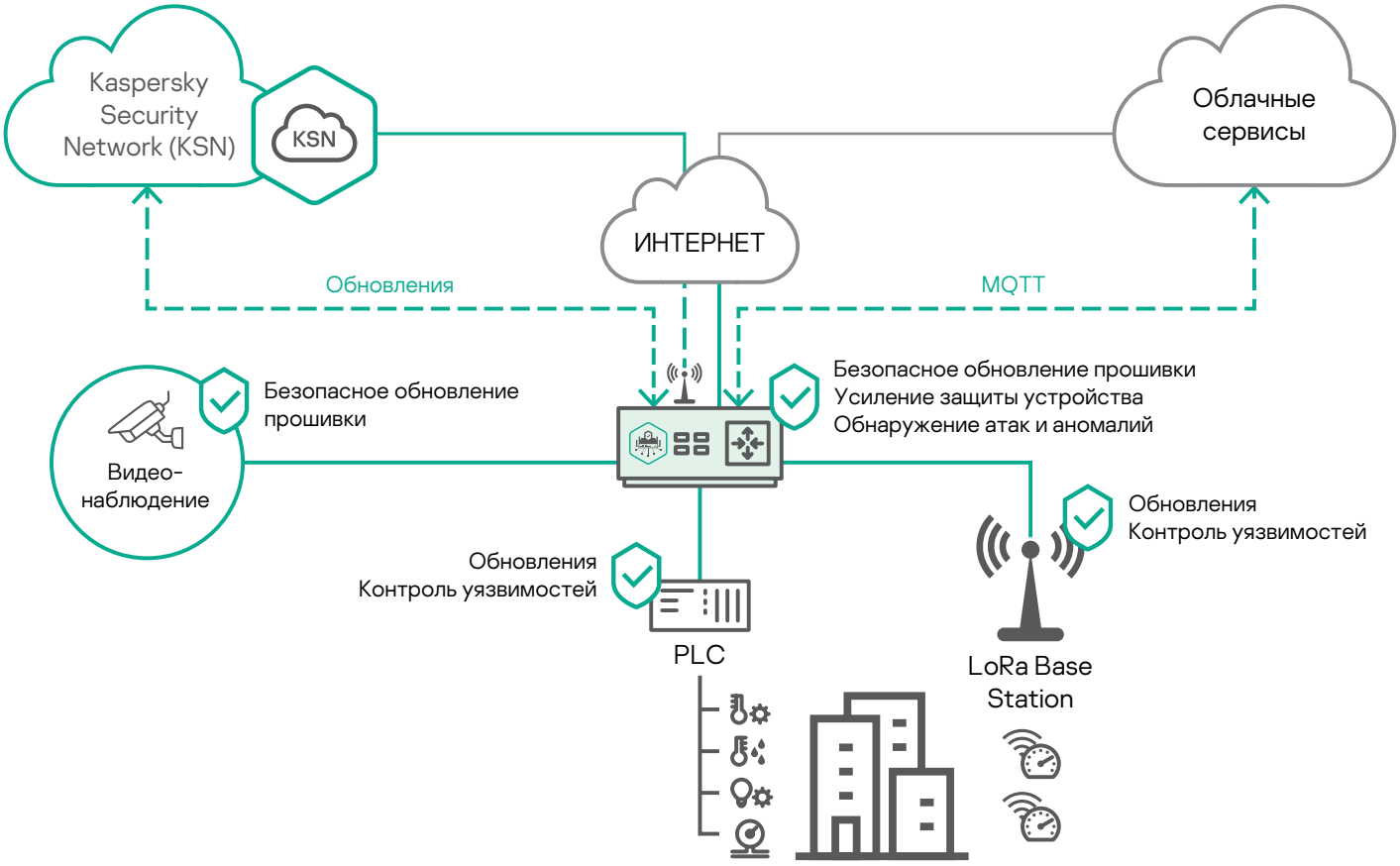
Примеры использования Kaspersky IoT Infrastructure Security

Умный город

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, датчики движения и датчики открытия дверей, а за информационную безопасность – **Kaspersky IoT Secure Gateway**: он блокирует атаки на локальные устройства и рабочие станции, выявляет неавторизованное подключение к сети, защищает периметр сети и связь с облаком.

Kaspersky Security Center обеспечивает удобное централизованное управление всей инфраструктурой интернета вещей, помогая контролировать ее безопасность и вовремя реагировать на инциденты.

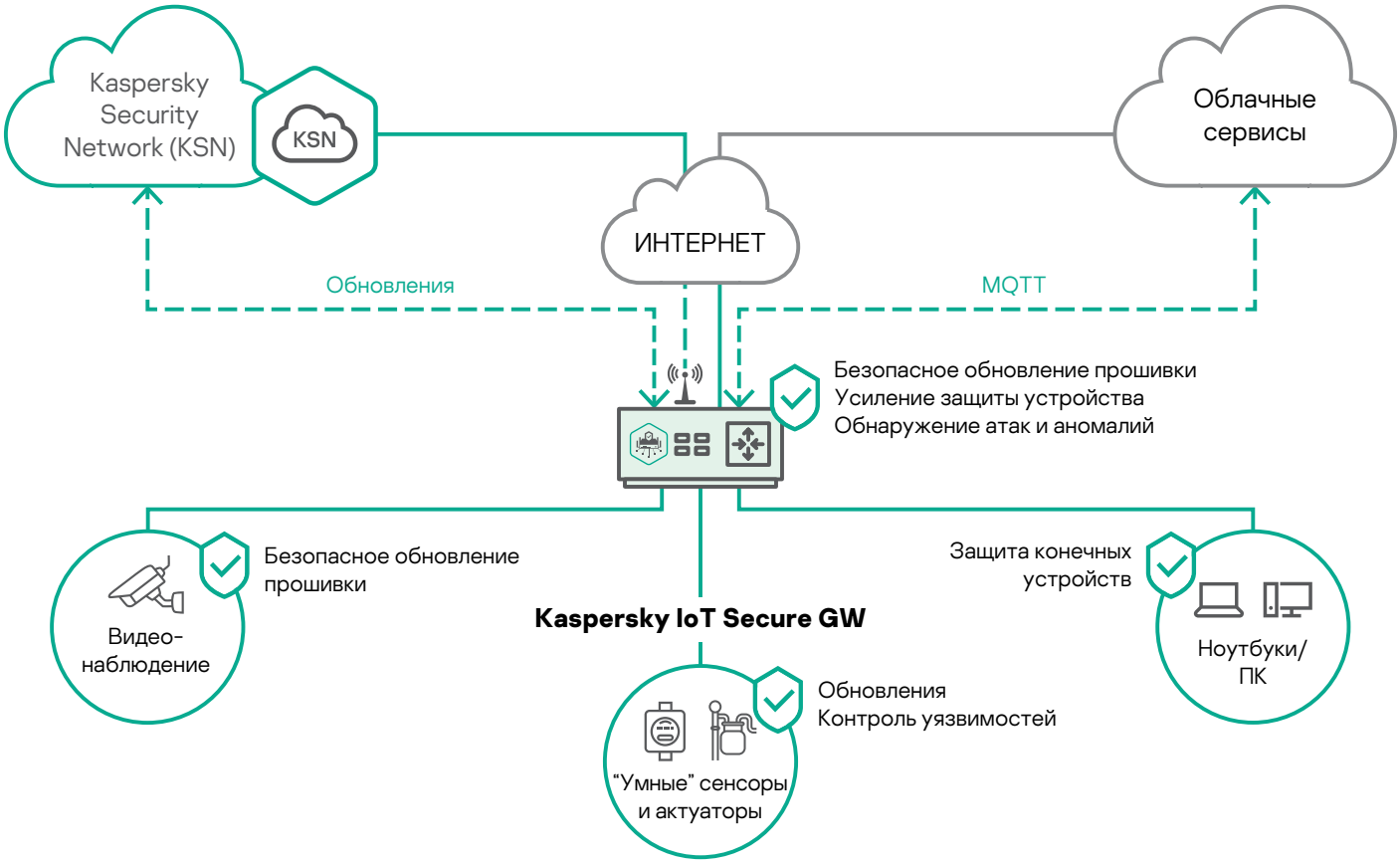


Умный склад

На складе устанавливаются системы контроля климатических параметров с возможностью управления из облака, чтобы непрерывно поддерживать и контролировать климат на складе из любой точки. Автоматизированный складской учет ведется с использованием RFID-датчиков и меток и контролируется как локально (с рабочих мест пользователей в сети), так и централизованно.

Системы удаленного видеонаблюдения и датчики объема и открытия дверей отвечают за физическую безопасность, а информационную безопасность обеспечивает **Kaspersky IoT Secure Gateway**. Он блокирует атаки на локальные рабочие станции, выявляет неавторизованное подключение к сети и защищает периметр сети и связь с облаком.

Kaspersky Security Center обеспечивает удобное централизованное управление всей инфраструктурой интернета вещей, помогая контролировать ее безопасность и вовремя реагировать на инциденты.



Kaspersky OS®

Kaspersky
IoT Infrastructure
Security

Подробнее на os.kaspersky.ru

www.kaspersky.ru