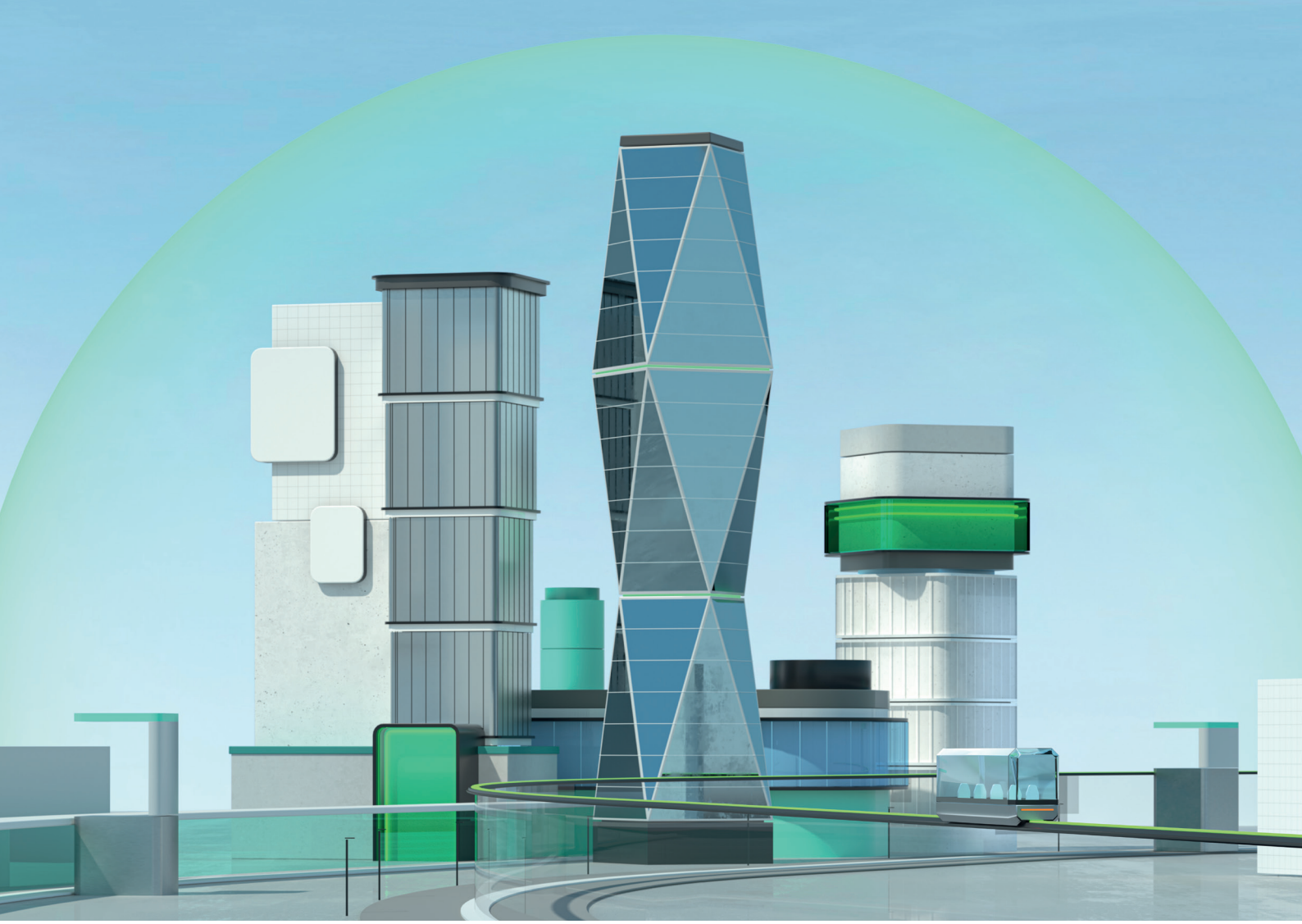


Kaspersky IoT Infrastructure Security

KasperskyOS

Активируем кибериммунитет

Kaspersky
IoT Infrastructure
Security

Защита интернета вещей на уровне шлюзов

Интернет вещей может сделать мир безопаснее, комфортнее и технологичнее. Он позволяет экономить ресурсы и эффективно управлять цифровыми инфраструктурами в самых разных сферах (от систем видеонаблюдения до целых умных городов), а также помогает промышленности быстрее стать частью Индустрии 4.0.

IoT — это огромное количество устройств, технологий, программного обеспечения и протоколов передачи данных. Такая неоднородная среда подвержена множеству рисков на всех уровнях.

Защитить интернет вещей от кибератак можно на уровне **шлюза, или гейтвея**. Именно через него проходят все данные между устройствами и облачными платформами, а значит, от его безопасности зависит безопасность всего IoT.

«Лаборатория Касперского» предлагает исходно безопасные IoT-шлюзы, разработанные на основе операционной системы KasperskyOS. Эти шлюзы, ключевые компоненты решения **Kaspersky IoT Infrastructure Security**, помогают строить надежные и функциональные системы интернета вещей.

Первым на рынок выходит кибериммунный шлюз данных для промышленности **Kaspersky IoT Secure Gateway 100** на аппаратной платформе Siemens SIMATIC IOT2040, который безопасно передает данные с индустриального оборудования по протоколу OPC UA в облачные платформы. Он создан совместно с НПО «Адаптивные Промышленные Технологии» (Апротех) — дочерней компанией «Лаборатории Касперского», помогающей производственным предприятиям пройти цифровую трансформацию.

В решение также входит шлюз с функцией защиты и мониторинга **Kaspersky IoT Secure Gateway 1000** под управлением Kaspersky Security Center. Он работает на аппаратной платформе Advantech UTX-3117, собирая данные и позволяя управлять подключенными устройствами по протоколу MQTT поверх TLS. Комплекс из двух продуктов защищает IoT-инфраструктуры на уровне шлюзов, помогая отслеживать их состояние и управлять событиями из единого центра.

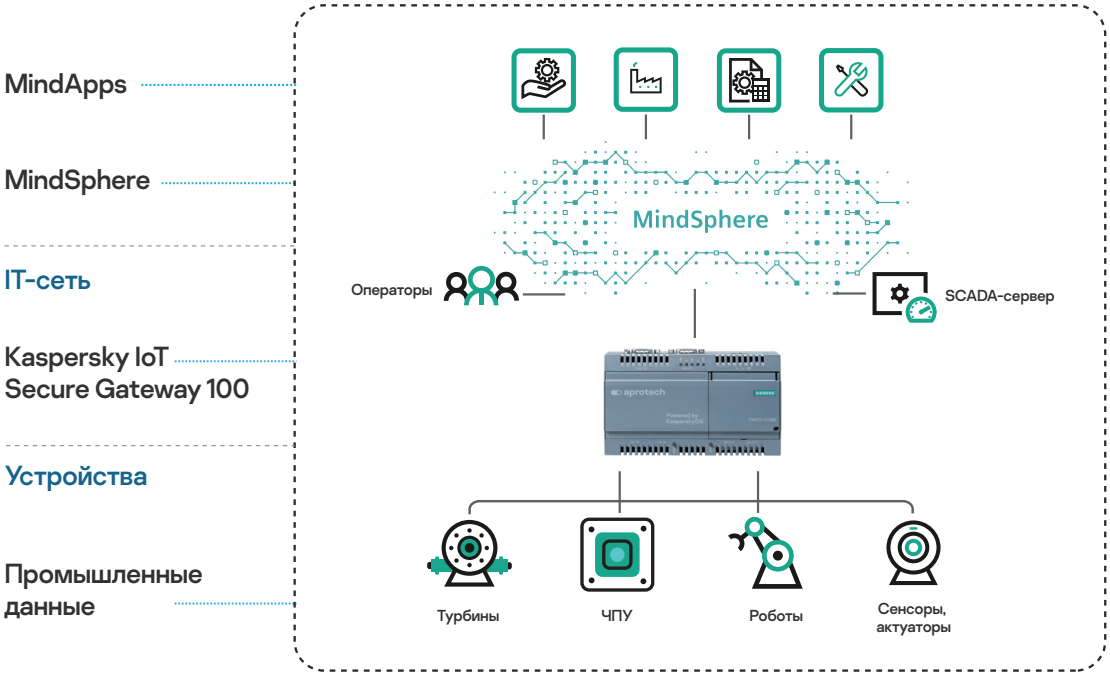
В дальнейшем линейка **Kaspersky IoT Infrastructure Security** будет расширяться.

Kaspersky IoT Secure Gateway 100

Кибериммунный шлюз для индустриального интернета вещей

Kaspersky IoT Secure Gateway 100 — первый кибериммунный продукт на KasperskyOS, выходящий на рынок. Шлюз помогает индустриальным компаниям пройти через цифровую трансформацию: это универсальное средство быстрого и безопасного соединения любого устройства из мира управления технологическими процессами (OT) с миром корпоративных IT-систем.

Подключение промышленного оборудования к облачной платформе позволяет детальнее понимать работу устройств, лучше ее контролировать, оптимизировать и предотвращать простои, что в результате повышает эффективность всего бизнеса. Kaspersky IoT Secure Gateway 100 напрямую подключается к разнообразному оборудованию, безопасно собирает данные и конвертирует их в удобный формат, а затем передает в облачную платформу Siemens MindSphere для хранения и обработки.



Kaspersky IoT Secure Gateway 100 в индустриальной IoT-инфраструктуре

Этот IIoT-шлюз способен воспринимать большие объемы информации, которую генерируют устройства. Например, типовой SCADA в АСУ ТП для оперативного мониторинга и управления достаточно всего 10-15% данных от оборудования. Однако этого объема не хватит для машинного обучения, предиктивного анализа, построения математических моделей.

Однонаправленная передача данных через Kaspersky IoT Secure Gateway 100 не дает получить доступ к оборудованию извне. Технологии KasperskyOS в основе кибериммунности шлюза защищают его от кибератак по умолчанию. Микроядро KasperskyOS, в паре с системой безопасности Kaspersky Security System, блокирует все неразрешенные процессы еще до их исполнения.

Таким образом, Kaspersky IoT Secure Gateway 100 обеспечивает доверенность телеметрии и позволяет разрабатывать на ее основе надежные пользовательские приложения для Siemens MindSphere, а также эффективно работать с системами ERP и MES для планирования производства и контроля за его исполнением.

Возможности и преимущества KISG 100

Подключение	
OPC UA (версия 1.04)	Сбор и передача данных в облако через проверенный протокол
Siemens MindSphere	Хранение и обработка информации в специальном облаке для IoT
Спецификация ПО	
Операционная система	KasperskyOS, поддержка SSL/TLS

Спецификация поддерживаемого аппаратного обеспечения KISG 100

Siemens SIMATIC IOT2040	
Процессор	Intel Quark X1020
Размеры	53 (Д) x 144 (Ш) x 90 мм (В)
Память	1 GB DDR3-SDRAM
Ethernet	Поддержка 100 Mbps LAN 2 x Ethernet (RJ45)
I/O-интерфейс	1 x USB 2.0, 1 x USB-клиент 2 x COM-порта (RS 232, RS 485)
Хранилище	1 x слот для карты microSD

О сервисах НПО «Адаптивные Промышленные Технологии»

Чтобы помочь промышленным предприятиям пройти цифровую трансформацию, Апротех предлагает следующие услуги в партнерстве с компанией Siemens:

- **Консалтинг БАЗА 4.0**
  Позволяет обнаружить «узкие» места технологического контура или отдельного технического процесса промышленной компании. Цифровой аудит упрощает переход к новым технологиям для дальнейшей плавной оптимизации бизнес-процессов. По результатам аудита Апротех может помочь с внедрением технологий, которые способны повысить эффективность бизнеса (например, с подключением оборудования к облаку).
- **Разработка приложений для облачной платформы (Siemens MindSphere)**
  На IIoT-платформе представлены готовые сервисы по базовому мониторингу работы подключенного оборудования, а также специальные приложения по предиктивной аналитике, анализу больших данных и эффективности работы производства.
- **Сервис OEE (Overall Equipment Effectiveness)**
  Сервис включает в себя анализ общей эффективности оборудования и составление индивидуальных экспертных рекомендаций по улучшению OEE на уровне отдельной машины/производственной линии. При этом оцениваются три главных фактора: доступность оборудования, его производительность, качество выпускаемой продукции.

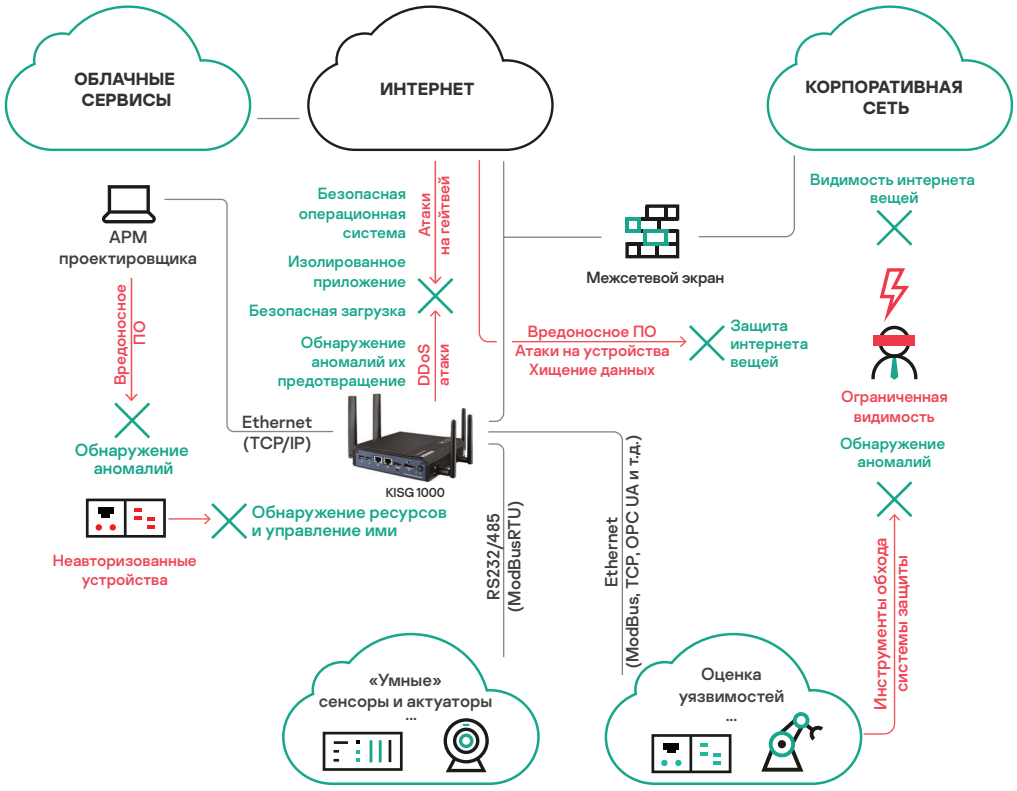
Kaspersky IoT Secure Gateway 1000

Защищенный шлюз для безопасного интернета вещей

Kaspersky IoT Secure Gateway 1000 на основе KasperskyOS помогает строить надежные системы интернета вещей. Он не только сам обладает исходной безопасностью, но и обеспечивает кибербезопасность всей IoT-инфраструктуры. В состав гейтвея входят функции межсетевого экрана, а также технологии активной защиты, предотвращения и обнаружения вторжений. KISG 1000 обеспечивает важный для интернета вещей безопасный доступ в публичные или приватные облака. Централизованное управление и мониторинг осуществляются с помощью платформы Kaspersky Security Center.

Особенности Kaspersky IoT Secure Gateway 1000:

- может применяться как в промышленности, так и в других отраслях;
- агрегирует данные, собранные по разным протоколам (Zigbee, LoRa, Modbus, CanBus, PROFINET, OPC UA и другие), и конвертирует их для передачи по сотовым сетям и Ethernet (MQTT, CoAP, AMQP, XMPP);
- не только собирает, проверяет и распределяет телеметрию, но также передает на устройства управляющие команды, полученные по MQTT;
- выполняет функции безопасности: обнаруживает и классифицирует устройства, регистрирует события безопасности в IoT-системах и защищает от сетевых атак (IDS/IPS).

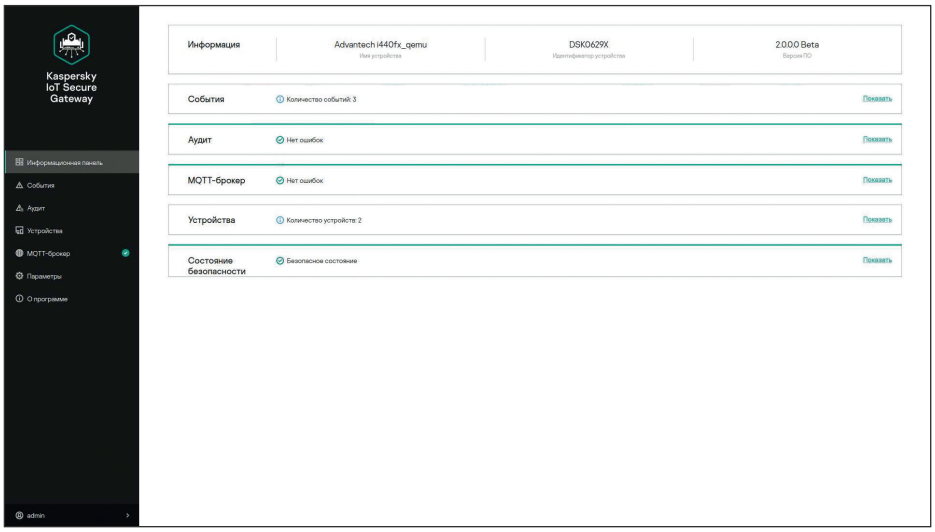


Защита IoT с использованием Kaspersky IoT Secure Gateway 1000

Kaspersky IoT Secure Gateway 1000 можно рассматривать в качестве шлюза безопасности, специализированного пограничного сетевого средства защиты IoT- и IIoT-инфраструктуры от хакерских атак. Его можно настраивать и дополнять функционалом продукции партнеров.

Возможности и преимущества KISG 1000

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 1000

Спецификация поддерживаемого аппаратного обеспечения KISG 1000

Advantech UTX-3117	
Процессорная система	Intel Pentium N4200, 2 MB L2 Cache
RAM	Двойной канал DDR3L 1600MHz, 4 GB
Ethernet	1 GB DDR3-SDRAM
I/O-интерфейсы	1 x RS-232 с 5v/12v 2 x USB 3.0 1 x интерфейс SATA, бортовая поддержка SSD TPM Infineon SLB9665. Поддержка TPM 2.0
Хранение данных	1 x отсек SATA II SSD (32 GB) mSATA 1, совместное использование со слотом H/S miniPCIE

Совместное использование KISG 100 и KISG 1000

Kaspersky IoT Secure Gateway 1000 может использоваться вместе с Kaspersky IoT Secure Gateway 100 в промышленном интернете вещей, устанавливаясь «выше» — на границе IoT-инфраструктуры и внешних сетей передачи данных.

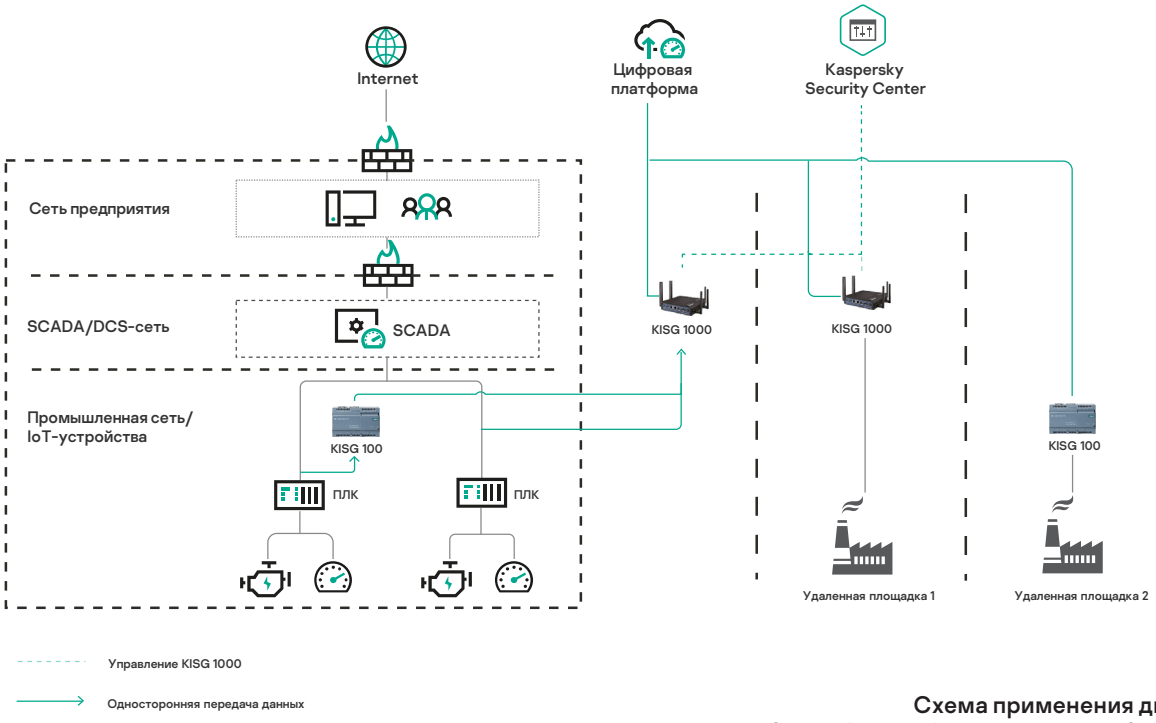
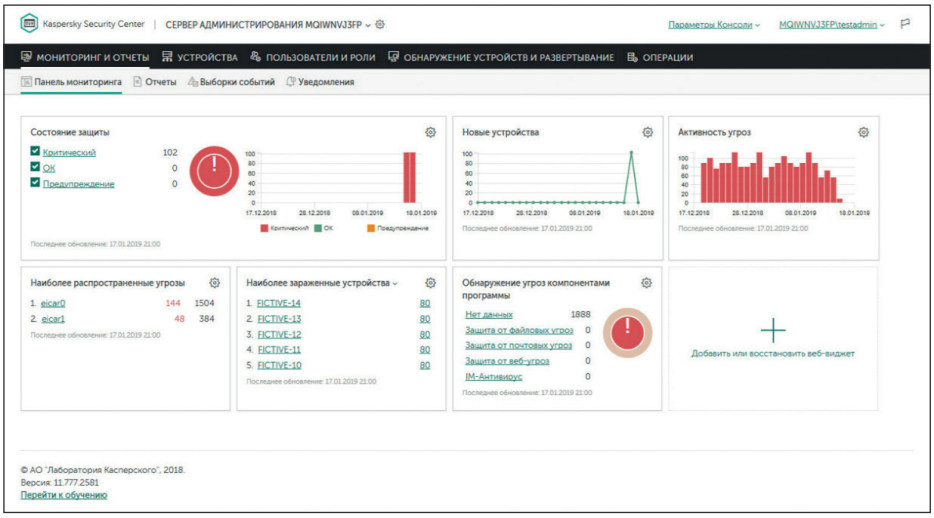


Схема применения двух шлюзов Kaspersky IoT Secure Gateway в IIoT-инфраструктуре

Kaspersky Security Center

Централизованное управление и мониторинг Kaspersky IoT Secure Gateway 1000

Платформа Kaspersky Security Center помогает управлять всеми событиями Kaspersky IoT Secure Gateway 1000 β из единого центра, отслеживать их и удобно проводить конфигурацию. Связка этих продуктов образует **комплексное решение Kaspersky IoT Infrastructure Security** для прозрачного, функционального и безопасного интернета вещей.



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 KSC. Оптимизированные возможности резервного копирования

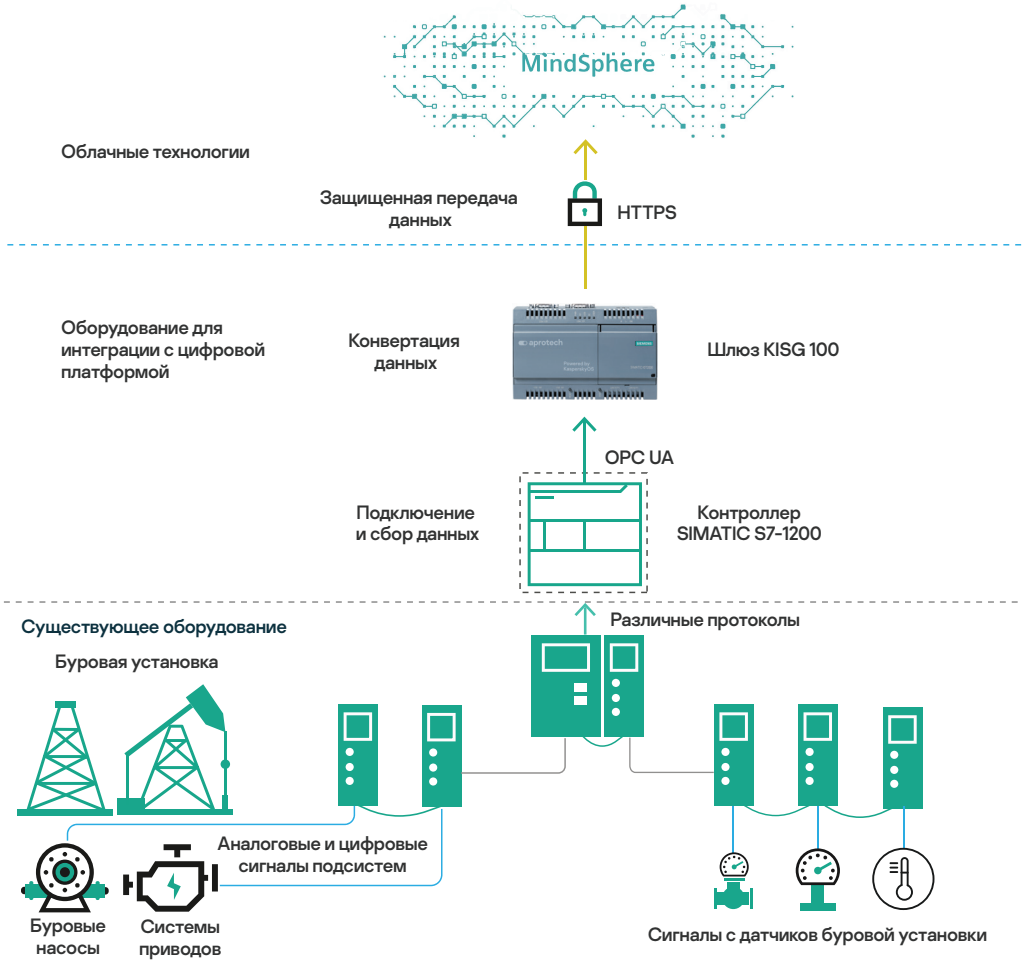
Расширяемая архитектура	В случае приобретения или выпуска нового приложения можно установить соответствующее расширение без повторной установки или исправления консоли
Удобное оповещение	Уведомления об инцидентах через различные каналы, удобные администратору (SMS, e-mail, push и т.д.)
Гибкая система отчетности	Настраиваемые и готовые отчеты с динамической фильтрацией и сортировкой по любому полю

Примеры использования шлюзов Kaspersky IoT Secure Gateway

Нефтегазовая отрасль

Нефтедобывающее предприятие хочет цифровизировать производственные процессы, внедрив машинное обучение и предиктивную аналитику работы оборудования. В этом может помочь интернет вещей с использованием облачных технологий. Для этого оборудование (буровые установки, насосы, системы приводов и др.) оснащается датчиками, подключается к шлюзу, а тот, в свою очередь, — к облачной или локальной платформе хранения и обработки данных.

Kaspersky IoT Secure Gateway 100 помогает выстроить функциональный промышленный интернет вещей, обеспечить доверенность телеметрии и подготовить ее к обработке. Шлюз собирает информацию со всех устройств по специализированным протоколам, конвертирует ее в удобный формат и безопасно транслирует в облако Siemens MindSphere, не позволяя скомпрометировать и перехватить данные, а также подключаться к оборудованию извне.



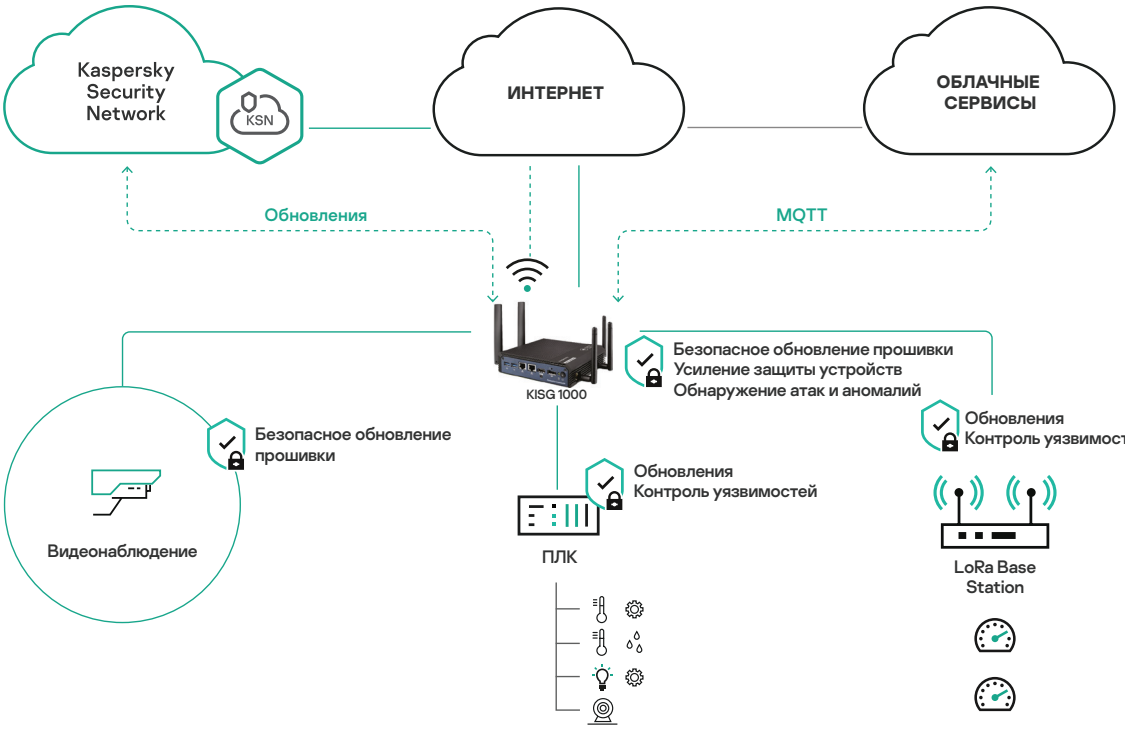
Даже если в подключаемых IIoT-устройствах окажутся уязвимости, кибериммунитет в основе Kaspersky IoT Secure Gateway 100 не даст злоумышленникам их эксплуатировать и влиять на работу остального оборудования.

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 1000**: 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.

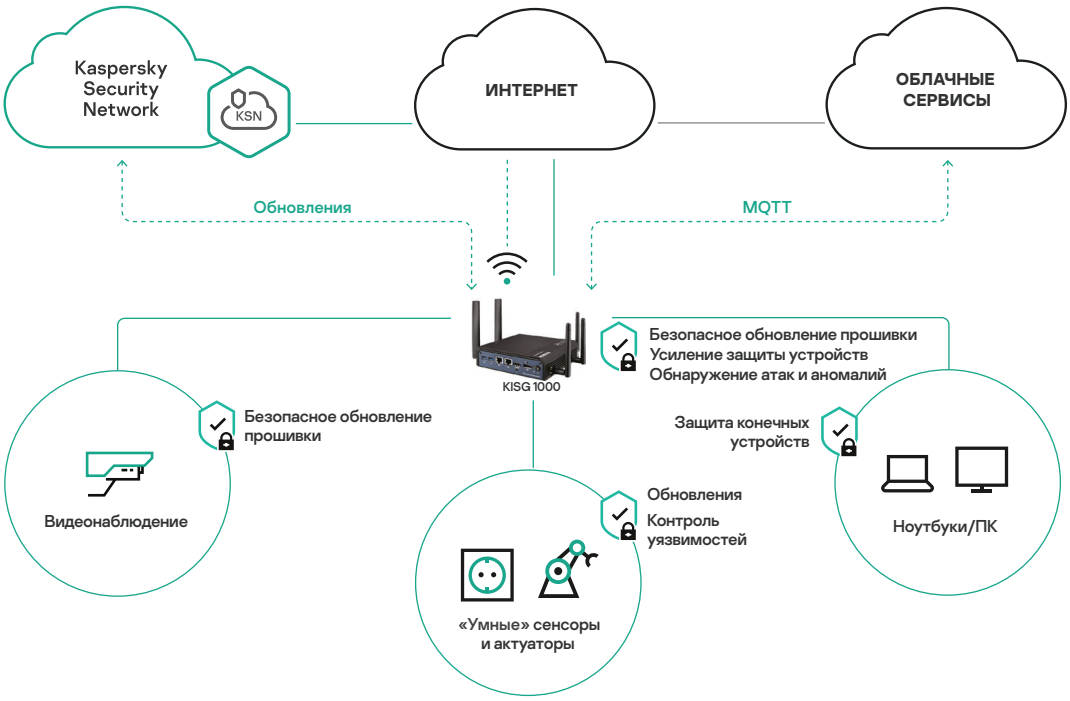


Умный склад

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 1000**. 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.



os.kaspersky.ru
www.kaspersky.ru

www.aprotech.ru

KasperskyOS
Активируем кибериммунитет

aprotech Powered by KasperskyOS