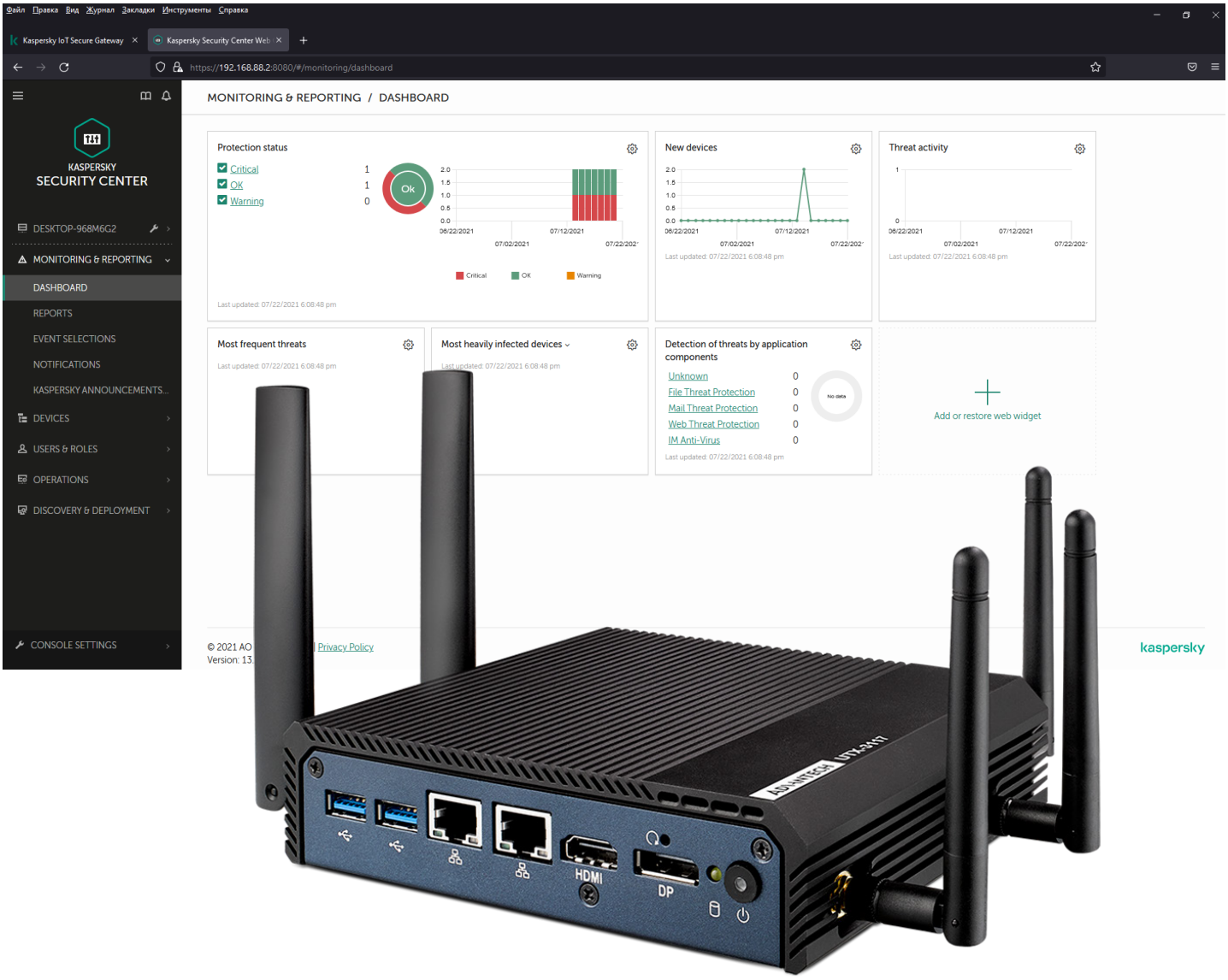


Кибериммунный шлюз для защищенного, прозрачного и функционального интернета вещей

Kaspersky IoT Secure Gateway 1000

kaspersky

KasperskyOS

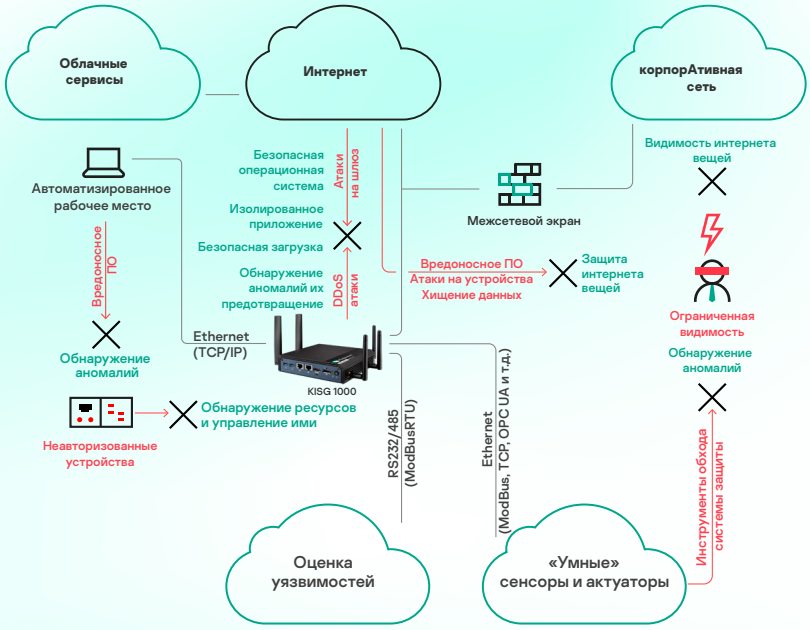
Kaspersky IoT Secure Gateway 1000

Внедрение технологий промышленного интернета вещей позволяет более точно рассчитывать общую эффективность оборудования (OEE). Этот показатель помогает определить шаги для повышения эффективности производственных процессов. Ключевым элементом инфраструктуры интернета вещей являются IoT-шлюзы. Через них проходят все данные между устройствами и облачными платформами, а значит, от их безопасности зависит безопасность всей инфраструктуры. Kaspersky IoT Secure Gateway (KISG) 1000 —шлюз данных для интернета вещей, работающий на операционной системе KasperskyOS. Он не только собирает данные с IoT-устройств, но и помогает обеспечить надежную киберзащиту.

IoT-шлюз — ключевой элемент инфраструктуры интернета вещей. В его функции входят:

- Агрегация данных от устройств
- Конвертация протоколов
- Передача данных в облачную платформу

Для эффективного функционирования IoT-инфраструктуры, шлюз должен обладать стеком необходимых протоколов, средствами защиты от кибератак и прозрачными и удобными средствами мониторинга и управления. Всеми этими свойствами обладает KISG 1000.



Защита IoT с использованием Kaspersky IoT Secure Gateway 1000

Сбор данных

KISG 1000 может применяться как в промышленности, так и в других отраслях. Шлюз позволяет организовать централизованный сбор данных с устройств интернета вещей (датчиков, сенсоров, контроллеров и т.п.) и обеспечить безопасную передачу данных в облачную платформу по протоколу MQTT.

Защита на уровне ОС

KISG 1000 обладает кибериммунитетом — исходной защищенностью на уровне архитектуры ОС. Это означает, что подавляющее большинство типов кибератак на шлюз не смогут влиять на выполнение им критических функций, то есть устройство будет надежно функционировать даже в условиях агрессивной среды.

Защита IoT от киберугроз

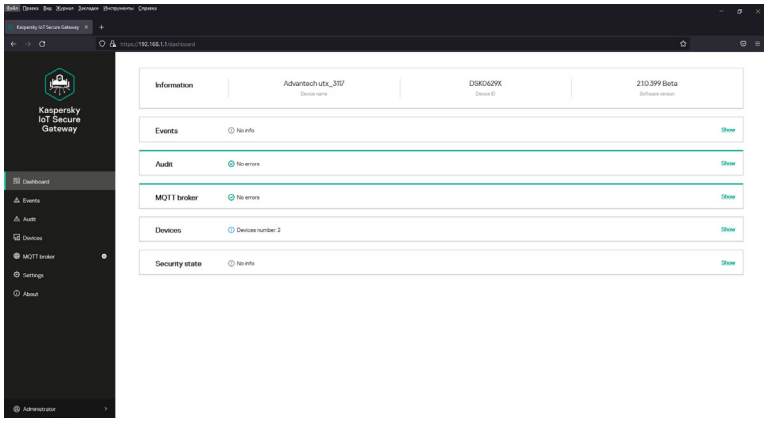
В состав Kaspersky IoT Secure Gateway 1000 входят функции межсетевого экрана, а также технология предотвращения и обнаружения вторжений. Шлюз обеспечивает безопасную передачу данных в публичные или приватные облака.

Централизованное управление

Централизованный мониторинг и управление всеми событиями KISG 1000 осуществляются с помощью платформы Kaspersky Security Center. Вместе два продукта образуют комплексное решение Kaspersky IoT Infrastructure Security.

Kaspersky IoT Secure Gateway 1000 внесен в единый реестр российских программ для электронных вычислительных машин и баз данных 29.10.2021 под номером 11928.

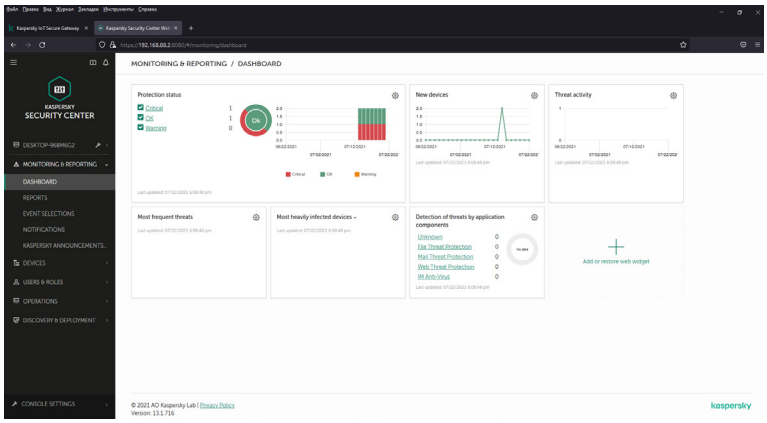
Веб-интерфейс KISG 1000



Доступ к настройкам шлюза и мониторингу событий безопасности осуществляется через веб-интерфейс. Он состоит из следующих разделов:

- **Информационная панель.** Информация о последних событиях, обнаруженных устройствах и состоянии компонентов системы.
- **События.** События безопасности.
- **Аудит.** События аудита системы.
- **Устройства.** Обнаруженные в сети устройства.
- **MQTT-брокер.** Профили MQTT-брокера.
- **Параметры.** Просмотр и изменение параметров системы.
- **О программе.** Краткая информация о системе.
- **<Имя пользователя>.** Меню пользователя.

Kaspersky Security Center

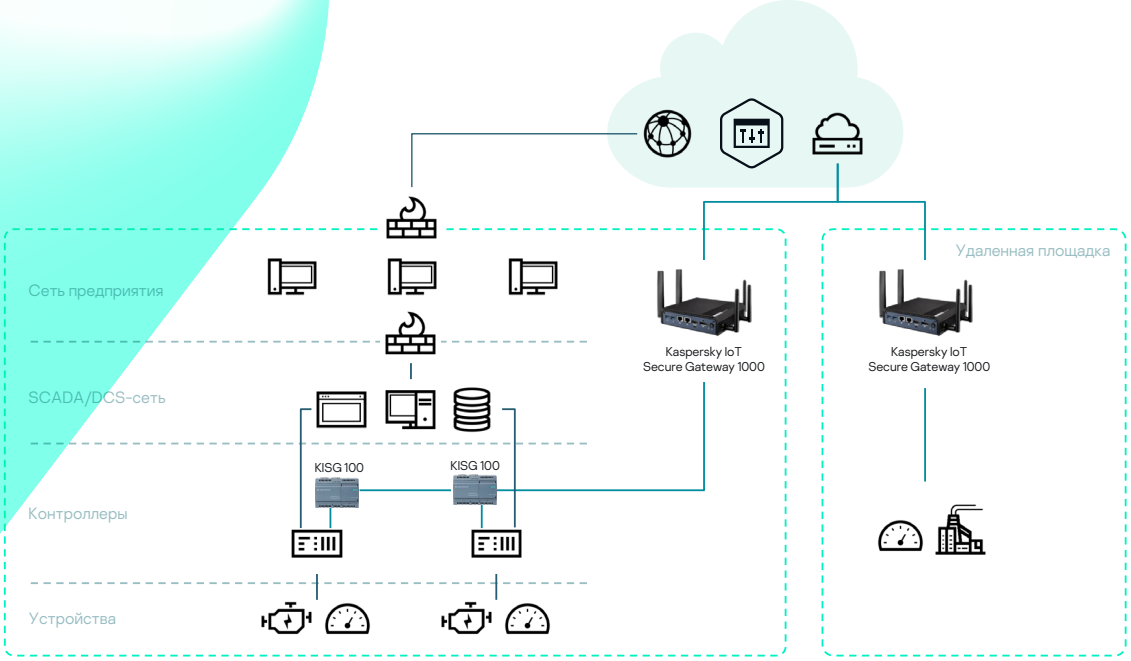


Kaspersky Security Center (KSC) позволяет удаленно управлять KISG 1000. Используя возможности KSC можно:

- Настраивать параметры MQTT-брокера.
- Настраивать параметры сети.
- Управлять межсетевым экраном.
- Управлять системой обнаружения вторжений.
- Настраивать параметры веб-сервера.
- Настраивать отправку сообщений на syslog-сервер.
- Настраивать отправку push-уведомлений.
- Настраивать дату и время.
- Управлять политикой паролей.
- Настраивать параметры взаимодействия с Kaspersky Security Center Web Console.
- Перезагружать и обновлять Kaspersky IoT Secure Gateway.

Совместное использование KISG 1000 и KISG 100

KISG 100 обеспечивает подключение промышленного оборудования по протоколу OPC UA и передачу данных в платформу Siemens MindSphere, а KISG 1000 устанавливается «выше» уровня шлюзов KISG 100 и агрегирует данные от KISG 100, а также от других устройств нижнего уровня. При этом, KISG 1000 также обеспечивает контроль и защиту устройств нижнего уровня от атак со стороны внешней сети.



Технические характеристики и возможности KISG 1000

Спецификации	
Процессор	Intel Pentium N4200, 1,1 ГГц, 2МБ L2 Cache
ОЗУ	4ГБ, DDR3L, 1600 МГц
Накопитель	SATA II SSD (32 ГБ)
Интерфейсы	2xGbE LAN, 2xMiniPCIe
Габариты	128x152x37 мм
Диапазон рабочих температур	От -20 до +60 °C
Дополнительно	3G/4G-модем (опционально)
Подключение	
Ethernet	Два интерфейса для подключения к различным сегментам сети по витой паре (LAN и WAN)
Сотовый модем	Возможность использовать мобильную сеть передачи данных в качестве основного или резервного канала связи
Маршрутизация и NAT	Автоматически настраиваемая маршрутизация между интерфейсами KISG 1000. Возможность управлять работой NAT (маскарадинг)
DHCP-сервер	Автоматическое распространение сетевой конфигурации на IoT и другие устройства, расположенные в локальной сети
MQTT-брокер	MQTT-брокер на базе Mosquitto позволяет осуществлять централизованный сбор данных IoT-устройств (сенсоров и актуаторов, умных реле и т.д.)
OpenSSL/TLS	Поддержка распространенных механизмов криптографической защиты данных, передаваемых по протоколам MQTT и Syslog
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
Мониторинг	
Обнаружение и классификация устройств	Обнаруживает устройства, расположенные в локальной сети на основе их сетевой активности. В пользовательском интерфейсе можно увидеть все устройства сети, взаимодействующие с KISG 1000, а новые будут обнаружены в течение 60 секунд
Отчеты и уведомления (MQTT, SYSLOG, push-уведомления, Kaspersky Security Center)	Администратор может получать события безопасности KISG 1000 в единую систему управления безопасностью предприятия — Kaspersky Security Center, а также передавать события в сторонние системы (SIEM, облачные платформы и т.п.) по протоколам Syslog и MQTT. KISG 1000 поддерживает интеграцию с Google Firebase для передачи push-уведомлений на мобильные устройства
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
Централизованная система управления	Платформа Kaspersky Security Center позволяет работать с событиями, получаемыми со всех KISG 1000, развернутых в инфраструктуре организации. Также она позволяет отслеживать состояние шлюзов и управлять их конфигурацией
Защита IoT-шлюза от кибератак	
Исходная безопасность (Secure by design)	Кибериммунная операционная система KasperskyOS исключает возможность компрометации устройства, а значит, делает невозможной утечку данных или проникновение в инфраструктуру предприятия
Безопасная загрузка (Secure boot)	Верификация целостности и подлинности прошивки шлюза с использованием криптографических методов перед загрузкой образа. Несанкционированно измененная или поврежденная прошивка не будет загружена
Безопасное обновление (Secure update)	Работая в комплексе с безопасной загрузкой, технология позволяет обновлять прошивку только с использованием правильно подписанных и зашифрованных образов
Защита IoT-инфраструктуры	
IDS/IPS и межсетевой экран (Firewall)	Межсетевой экран работает по принципу Default Deny. Администратор может быть уверен, что через шлюз будут проходить только разрешенные сетевые взаимодействия Модуль IDS/IPS (обнаружение и предотвращение вторжений) уведомляет и блокирует зловредные активности, обнаруженные с помощью подготовленного специалистами «Лаборатории Касперского» набора сигнатур

KasperskyOS

Kaspersky IoT Secure Gateway 1000

Подробнее на os.kaspersky.ru

www.kaspersky.ru