

Kaspersky IoT Secure Gateway

Узнайте больше о продукте
и успешных проектах
с его использованием

[os.kaspersky.ru/solutions/
kaspersky-iot-secure-gateway](https://os.kaspersky.ru/solutions/kaspersky-iot-secure-gateway)

Кибериммунный шлюз данных нового поколения на базе одноименной программной платформы (KISG), в основе которой лежит операционная система KasperskyOS, и аппаратной платформы Kraftway «Рубеж Н».



Основные области применения:

- Умные города/здания
- Транспорт и логистика
- Промышленность
- Нефтехимия
- Энергетика
- Другие индустрии

Назначение

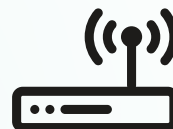
Шлюзы данных соединяют мир операционных технологий (OT) с миром информационных систем (IT). С помощью этих устройств можно подключать промышленное оборудование, комплексы автоматизации и мониторинга объектов к различным системам визуализации, обработки и хранения данных: от стандартных корпоративных систем MES/ERP до продвинутых IoT-платформ с аналитическими цифровыми сервисами.

Два режима работы

Устройство подключается к сети интернет посредством технологий Ethernet или 3G/LTE и может работать в двух режимах:



«Диод данных» — сбор данных по промышленным протоколам с последующей конвертацией и однонаправленной передачей в корпоративные и облачные системы. На данный момент уже реализовано подключение через IoT-протокол MQTT. В будущем функциональность будет расширяться.



«Роутер» — маршрутизатор с функциями межсетевого экрана, анализа и фильтрации промышленных протоколов, системы обнаружения и предотвращения вторжений IPS/IDS, а также брокера MQTT.

Ключевые преимущества KISG



Безопасный транспорт данных

Кибериммунный шлюз обеспечивает надежный транспорт данных и защиту сетевой инфраструктуры от киберугроз. Дополнительные функции сетевой безопасности (Firewall, IPS,) позволяют осуществлять контроль сетевых взаимодействий и своевременно реагировать на инциденты.



Централизованное управление

Управление шлюзами обеспечивается из единой консоли администрирования Kaspersky Security Center (KSC). Консоль позволяет отслеживать события безопасности, регистрируемые KISG, а также осуществлять удаленную настройку и обновление компонентов системы.



Сторонние приложения с Kaspersky Appcenter

Платформа Kaspersky Appcenter включает в себя все необходимые инструменты для создания, распространения и работы со сторонними приложениями на устройстве, включая приложения с функциональностью граничных вычислений. Доставка приложений на устройства осуществляется через консоли администрирования, например, Kaspersky Security Center, что гарантирует аутентичность приложений и их безопасную установку.



Граничные вычисления

Шлюз поддерживает приложения с возможностью граничных вычислений (edge computing), которые обеспечивают:

- унификацию оборудования на местах при поддержке разнообразия сенсоров;
- унификацию интерфейсов взаимодействия с информационными системами (ИС);
- сокращение трафика и ресурсов облака за счет аналитики на месте;
- управление без задержки;
- безопасную установку и обновление приложений.



Кибериммунитет

Подход «Лаборатории Касперского» к разработке конструктивно безопасных систем. Кибериммунный шлюз данных выполняет критичные функции даже в условиях агрессивной среды и защищен не только от известных, но и от еще неизвестных угроз на уровне архитектуры, без необходимости в наложенных средствах безопасности.

Отличительные особенности операционной системы KasperskyOS:

- Все компоненты (домены) ОС строго изолированы друг от друга и взаимодействуют только через микроядро.
- Микроядро KasperskyOS отвечает за функции, которые могут выполняться только в привилегированном режиме. Вся остальная функциональность ОС, включая драйверы, файловые системы и сетевые стеки, вынесена в режим пользователя.
- Все межпроцессные коммуникации проходят через строгий контроль в Kaspersky Security Module и проверяются на соответствие политикам безопасности. Согласно принципу Default Deny все, что явно не разрешено политиками безопасности — запрещено.

Технические характеристики и функции KISG

Спецификация аппаратной платформы Kraftway «Рубеж Н»

Тип процессора	Intel Pentium N4200, 1,1 ГГц, 2 МБ L2 Cache
Накопитель	SATA II SSD (32 ГБ)
Тип запоминающего устройства	DDR3L, 1600 МГц
ОЗУ	8 ГБ
Интерфейсы	2x100/1000 Мбит/с Ethernet RJ45
Сотовая связь	3G/4G-модем (опционально)
Диапазон рабочих температур	От +5 до +35 °С
Диапазон температур хранения	От -40 до +85 °С
Относительная влажность воздуха	до 80% при 25 °С (без конденсации)
Входное напряжение питания	DC 12...48 В AC 110...220В (опционально)
Энергопотребление	20 Вт (макс.)
Крепление	DIN-рейка, 19" RACK
Размеры	165 x 220 x 44 мм (Д x Ш x В)
Вес	1,2 кг

Сетевые функции

Ethernet	Два интерфейса для подключения к различным сегментам сети по витой паре (LAN и WAN)
3G/LTE	Возможность использовать мобильную сеть передачи данных в качестве основного или резервного канала связи
Маршрутизация и NAT	Настройка статической маршрутизации. Переадресация портов (Destination NAT), маскардинг.
VRRP	Объединение нескольких шлюзов в отказоустойчивый сетевой кластер. Виртуальный шлюз на интерфейсе LAN.
DHCP-сервер	Автоматическое распространение параметров сетевой конфигурации на устройства, расположенные в локальной сети
MQTT-брокер	MQTT брокер Mosquitto позволяет осуществлять централизованный сбор данных с IoT-устройств
TLS	Поддержка распространенных механизмов криптографической защиты данных, передаваемых по протоколам MQTT и Syslog
VPN	Поддержка VPN Client в режиме диода данных
Интеграция с облачными сервисами	Работа с IoT-платформами по протоколу MQTT. Возможно расширение функциональности при помощи приложений Kaspersky Appcenter,



Защита сетевой инфраструктуры

Межсетевой экран	Межсетевой экран работает по принципу Default Deny («запрет по умолчанию»). Администратор может быть уверен, что через шлюз будут проходить только разрешенные сетевые взаимодействия.
Межсетевой экран уровня промышленной сети (класс защиты 4 тип «Д» согласно ФСТЭК)	<ul style="list-style-type: none">• Контроль и фильтрация промышленных протоколов передачи данных: MQTT, Modbus, BACnet, DNP3, MMS, OMRON-FINS, ENIP/CIP, TriStation, S7comm• Проверка трафика протоколов MQTT и Modbus на аномалии (отклонения)
IDS/IPS	Модуль обнаружения и предотвращения вторжений блокирует зловредные и подозрительные сетевые активности, а также направляет уведомление об инциденте в Kaspersky Security Center и SIEM-систему
DPI	Фильтрация (блокирование) трафика прикладных протоколов: FTP, HTTP, MQTT, Modbus, SMTP, IMAP, POP3
Отчеты и уведомления (MQTT, Syslog, KSC)	Администратор может получать события безопасности KISG в единой консоли управления безопасностью предприятия — Kaspersky Security Center, а также передавать события в сторонние системы (SIEM, облачные платформы и т.п.) по протоколам Syslog и MQTT

Гибкое управление шлюзом

Веб-интерфейс	Информативный дэшборд, который позволяет быстро и оперативно получить все необходимые сведения. Удобная настройка и мониторинг IoT-сети, видимость и прозрачность благодаря WebGUI.
Централизованная система управления	Консоль администрирования Kaspersky Security Center позволяет работать с событиями, получаемыми со всех KISG, развернутых в инфраструктуре организации. Также с помощью нее можно отслеживать состояние шлюзов и управлять их конфигурацией.
Управление приложениями	Вне зависимости от подхода к управлению устройством функциональность Kaspersky Appcenter позволяет находить, устанавливать, обновлять и удалять приложения в любом интерфейсе.
RBAC	Управление доступом на основе ролей
Резервное копирование	Возможность восстанавливать конфигурацию системы из сохраненной ранее резервной копии

Защита шлюза от кибератак

Кибериммунитет (Secure by Design). ОС типа «А» четвертого класса защиты (Сертификация в 2024 г.)	Операционная система KasperskyOS исключает возможность компрометации устройства и помогает защитить инфраструктуру предприятия от кибератак
Безопасная загрузка (Secure boot)	Верификация целостности и подлинности прошивки шлюза с использованием криптографических методов перед загрузкой образа. Несанкционированно измененная 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

 — приложение доступно в Kaspersky Appcenter