aprotech Kaspersky IoT company KasperskyOS Операционная система

start@aprotech.ru
+7 495 970 71 17
www.aprotech.ru

Kaspersky IoT Secure Gateway

Разработан на базе операционной системы KasperskyOS и аппаратной платформы Kraftway Рубеж-Н

Кибериммунный шлюз данных нового поколения для организации безопасного канала связи между технологической и корпоративной сетями передачи данных и защиты систем промышленного интернета вещей (IIoT) от киберугроз

Основные области применения:

- Умные города/здания
- Транспорт и логистика
- Промышленность
- Нефтехимия
- Энергетика
- и 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:

«Роутер» - маршрутизатор с функциями межсетевого экрана, анализа и фильтрации промышленных протоколов (с функцией обнаружения и предотвращения вторжения) с предустановленным MQTT-брокером

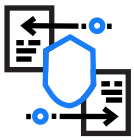
«Диод данных» - сбор данных по промышленным протоколам с последующей конвертацией и однонаправленной передачей в корпоративные и облачные системы. На данный момент уже реализовано подключение через IoT-протокол MQTT. В скором времени функционал будет расширен

aprotech Kaspersky IoT company

KasperskyOS Операционная система

Начнем киберимунную цифровизацию вместе!

Ключевые преимущества KISG

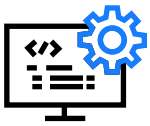


Безопасный транспорт данных

Кибериммунный шлюз обеспечивает надежный транспорт данных и защиту сетевой инфраструктуры от киберугроз. Дополнительные функции сетевой безопасности (firewall, анализ промышленных протоколов) 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.



Поддержка сторонних приложений

На новой платформе можно создавать собственные приложения под KasperskyOS, которые будут добавлены в общедоступный магазин приложений. Доставка на устройства осуществляется через консоль администрирования Kaspersky Security Center, что гарантирует аутентичность приложений и их безопасную установку.

Кибериммунитет

Кибериммунитет – это 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.

aprotech Kaspersky IoT company KasperskyOS Операционная система

Аппаратная платформа Рубеж-Н
Технические характеристики

Спецификации

Тип процессора	Intel Pentium N4200, 1,1 ГГц, 2МБ L2 Cache
Накопитель	SATA II SSD (32 ГБ)
Тип запоминающего устройства	DDR3L, 1600 МГц
ОЗУ	8ГБ
Интерфейсы	2x100/1000 Мбит/с Ethernet RJ45
Сотовая связь	3G/4G-модем (опционально)
Диапазон рабочих температур	От +5 до +35 °C
Диапазон температур хранения	От -40 до +85 °C
Относительная влажность воздуха	до 80% при 25 °C (без конденсации)
Входное напряжение питания	DC 12...48 В AC 110...220В (опционально)
Энергопотребление	20 Вт (макс.)
Крепление	DIN рейка, 19” RACK
Размеры	Длина 165 мм, ширина 220 мм, высота 44 мм
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), маскарадинг.
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	Возможность поддержки VPN
Интеграция с облачными сервисами	Работа с IoT платформами по протоколу MQTT

aprotech Kaspersky IoT company

KasperskyOS Операционная система

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*)	• 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)
Анализ промышленных протоколов (с функцией обнаружения и предотвращения вторжения)	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

Мониторинг

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.
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*	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 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

**Сертификация в 2025 г.*