aprotech Kaspersky IoT company KasperskyOS Активируем кибериммунитет ADVANTECH

Kaspersky IoT

Secure Gateway 1000

Кибериммунный шлюз данных для защищенного, прозрачного и функционального интернета вещей. Ключевой инструмент построения надежных сквозных цифровых сервисов.

Разработан на базе операционной системы KasperskyOS и аппаратной платформы Advantech UTX-3117.

Кибериммунитет + защита сети

Исходная защищенность на уровне архитектуры ОС и функции межсетевого экрана. Устройство будет выполнять критичные функции даже в условиях агрессивной среды, а также обнаружит и предотвратит вторжения в сеть организации.

Безопасный транспорт данных

Шлюз собирает данные с IoT-устройств и безопасно передает их на цифровые платформы. Может применяться в промышленности, умных домах, системах видеонаблюдения и в других областях.

Централизованное управление и веб-интерфейс

Консоль администрирования Kaspersky Security Center (KSC) обеспечивает управление устройствами и позволяет отслеживать события безопасности KISG 1000. Настройка шлюза также возможна через веб-интерфейс.

Операционная система KasperskyOS	• Все компоненты (домены) ОС строго изолированы и не могут влиять друг на друга • Проприетарное микроядро по умолчанию блокирует неразрешенные взаимодействия на основании вердиктов безопасности • Вердикты выносит движок Kaspersky Security System в соответствии с политиками безопасности, которые позволяет гибко задавать
Протокол	• Безопасное подключение по TLS и защищенная передача данных между шлюзом и облачной платформой
Подключение к облачной платформе	• Работа с любыми IoT платформами по протоколу MQTT

Операционная система KasperskyOS открыта для разработки. При необходимости компоненты KISG 1000 можно дополнять новыми.

Начнем кибериммунную цифровизацию вместе!

start@aprotech.ru
+7 495 970 71 17

www.aprotech.ru

aprotech Kaspersky IoT company KasperskyOS Активируем киберимунитет ADVANTECH

Аппаратная платформа

Технические характеристики Advantech UTX-3117

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	4ГБ
Интерфейсы	2x100/1000 Мбит/с Ethernet RJ45
Дополнительное устройство связи	3G/4G-модем (опционально)
Диапазон рабочих температур	От 0 до +55 °C
Диапазон температур хранения	От -40 до +85 °C
Относительная влажность воздуха	Эксплуатация до 95% при 40 °C (без конденсации)
Входное напряжение питания	12...24 В постоянного тока
Среднее энергопотребление	12 В * 0,35 (А), 4,2 Вт
Максимальное энергопотребление	12 В * 0,61 (А), 7,32 Вт
Размеры	Длина 128 мм, ширина 152 мм, высота 37 мм
Подключение	
Ethernet	Два интерфейса для подключения к различным сегментам сети по витой паре (LAN и WAN)
3G/4G	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 параметров сетевой конфигурации на IoT и другие устройства, расположенные в локальной сети
MQTT-брокер	MQTT-брокер на базе Mosquitto позволяет осуществлять централизованный сбор данных с IoT-устройств
OpenSSL/TLS	Поддержка распространенных механизмов криптографической защиты данных, передаваемых по протоколам MQTT и Syslog
Интеграция с облачными сервисами	Работа с любыми IoT платформами 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, включая неавторизованные
Отчеты и уведомления (MQTT, Syslog, KSC)	Администратор может получать события безопасности KISG 1000 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 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	Консоль KSC позволяет работать с событиями, получаемыми со всех KISG 1000, развернутых в инфраструктуре организации. Также она позволяет отслеживать состояние шлюзов и управлять их конфигурацией
Защита шлюза от кибератак	
Кибериммунитет (Secure by design)	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