aprotech Kaspersky IoT company

KasperskyOS Операционная система

Kaspersky IoT Secure Gateway

Кибериммунные шлюзы для подключения **НЕФТЕХИМИЧЕСКОГО ОБОРУДОВАНИЯ** к облакам и бизнес-системам

Сценарий №1

Шлюз как программный дата-диод (однонаправленная передача данных)

- **Безопасный и надежный транспорт** ранее недоступных для бизнеса данных;
- **Доверенные данные со шлюза помогают** строить цифровые сервисы по аналитике, прогнозированию работы оборудования;
- **Мониторинг** работы буровых установок для оптимизации нагрузки и прогностики сбоев;
- **Подключение и мониторинг** удаленных технологических площадок;
- **Сбор и передача параметров** для цифровизации нефтеналивного терминала.

Сценарий №2

Шлюз как роутер (двунаправленная передача данных)

- **Использование шлюзов** на объектах КИИ в режиме FW по сертификации ФСТЭК;
- **Отправка событий** безопасности по протоколу Syslog;
- **Безопасный** и надежный двунаправленный транспорт ранее недоступных для бизнеса данных;
- **Анализ промышленных протоколов (с функцией обнаружения и предотвращения вторжения)** для защиты от внешних угроз;
- **Кибер-защита промышленного оборудования,** РСУ, АСУТП и SCADA-систем от кибер-атак при подключении к ИТ-системам и сборе данных;
- **Сбор и передача данных** (КИП) от насосов и оборудования куста скважин/месторождения, для оптимизации энергопотребления и прогностики сбоев, передача данных в ДМЗ;
- **Комплексный сбор и защита данных** с перерабатывающего оборудования для создания цифрового двойника технологического процесса и оптимального правления системой;
- **Локальное хранение** всей собираемой информации (буферизация), аварийный буфер данных;
- **Защищенный сбор и передача данных** с промышленных устройств для передачи в РСУ.

Дополнительно:

- Создание экосистемы из продуктов Лаборатории Касперского: KISG+KUMA+KSRW+KICS+KSC для обеспечения безопасности на объекте и дальнейшей безопасной передачи данных в систему «ГосСОПКА»;
- Централизованное управление продуктами Kaspersky через Kaspersky Security Center.