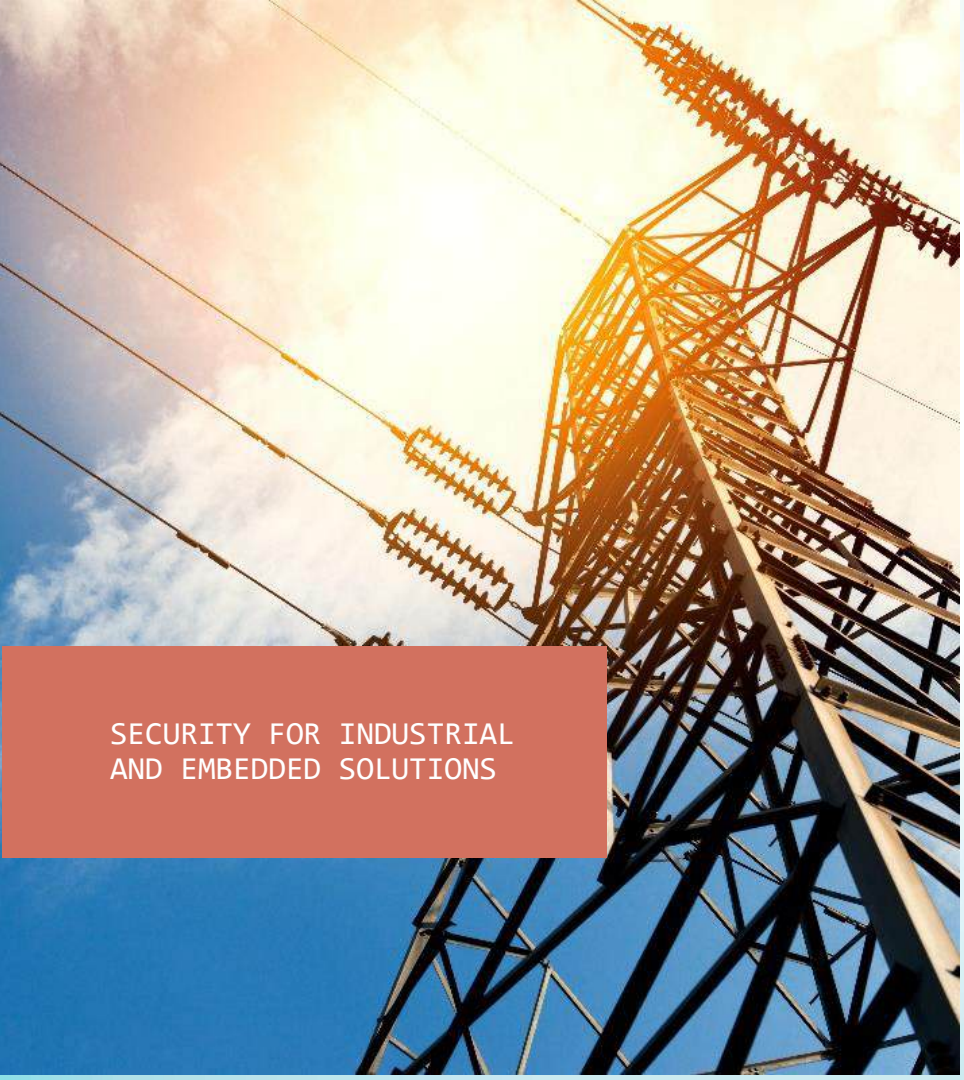
Решение ИнфоТеКС для защиты протоколов IIoT на примере LoRaWAN

Алексей Власенко
менеджер продуктов

infotecs



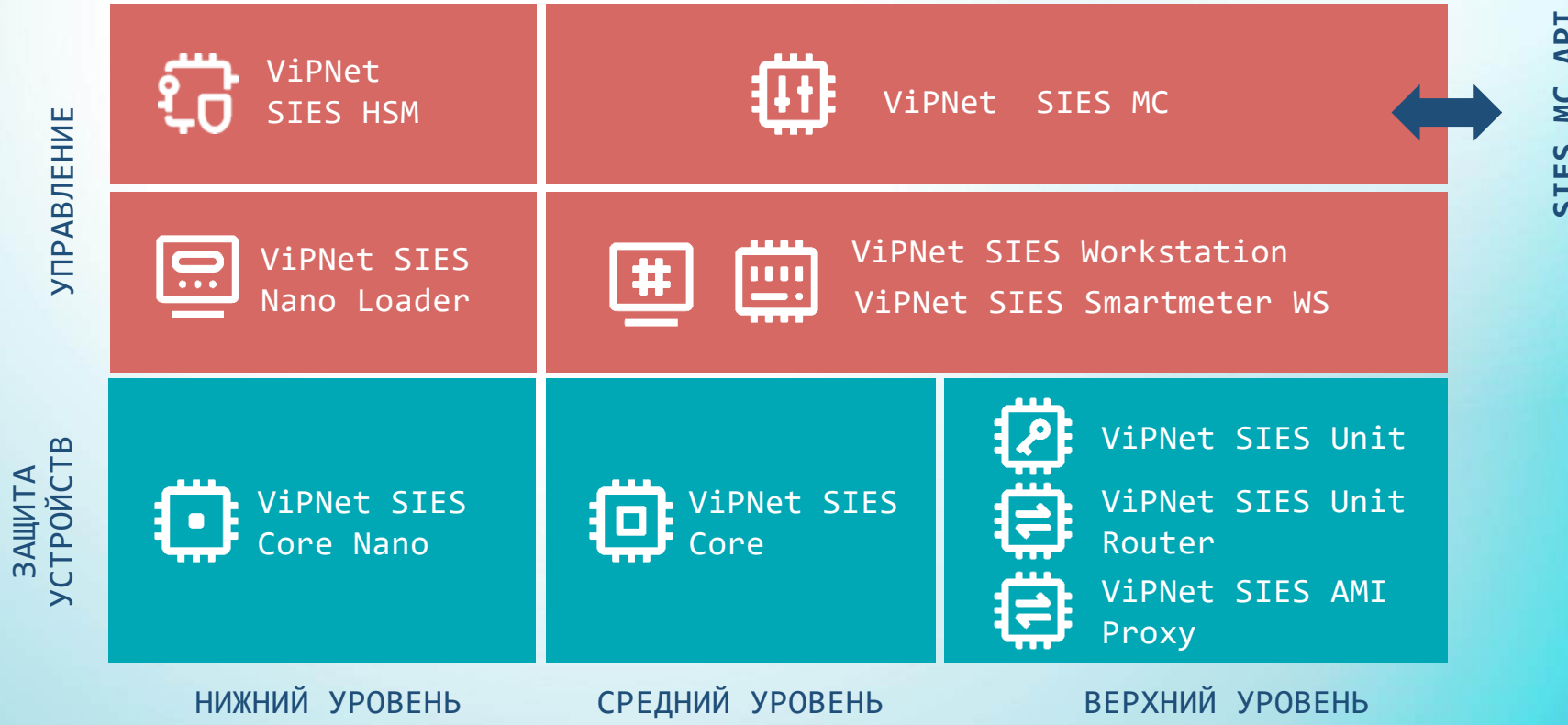
SECURITY FOR INDUSTRIAL
AND EMBEDDED SOLUTIONS

Решение ViPNet SIES

Встраиваемые криптографические средства защиты информации:

- для устройств автоматизации на всех уровнях АСУ
- для M2M-устройств
- для АСКУЭ/ИСУЭ
- для IIoT-устройств

Состав решения ViPNet SIES



Центр управления ViPNet SIES MC

ПАК ViPNet SIES MC 10000
- До 1 млн устройств
- СКЗИ класса КС3

ПАК ViPNet SIES MC 3000
- До 3000 устройств
- СКЗИ класса КС3

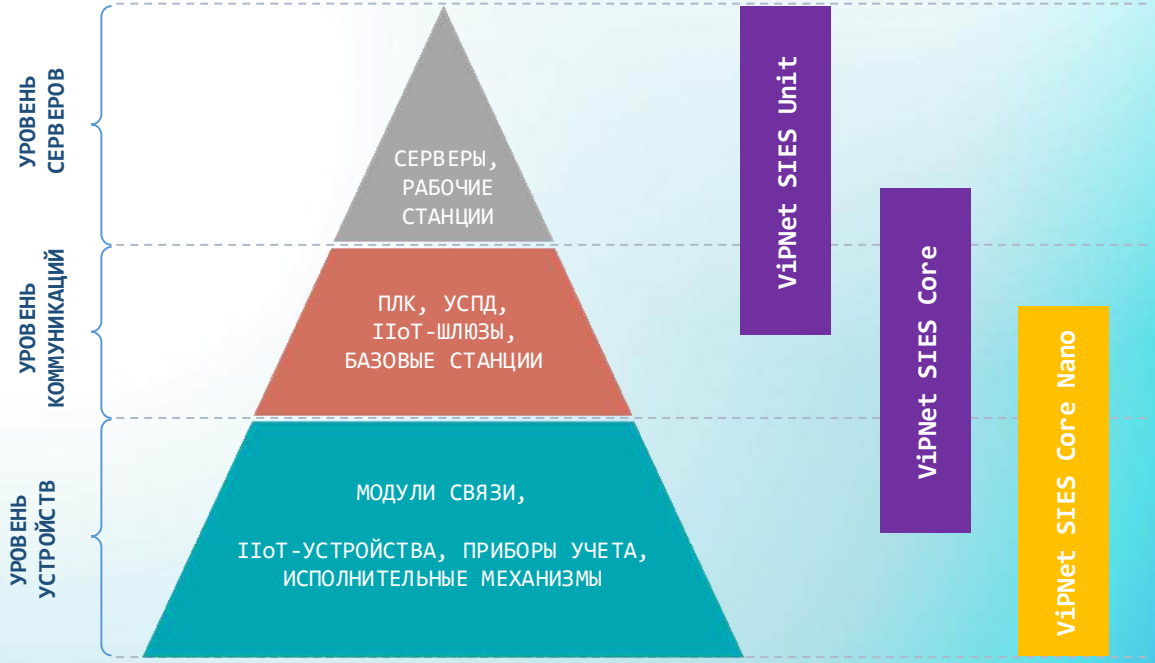
ПАК ViPNet SIES MC IoT
- До 2 млн устройств
- СКЗИ класса КС3

ViPNet SIES MC VA
- До 5000 устройств
- СКЗИ класса КС1

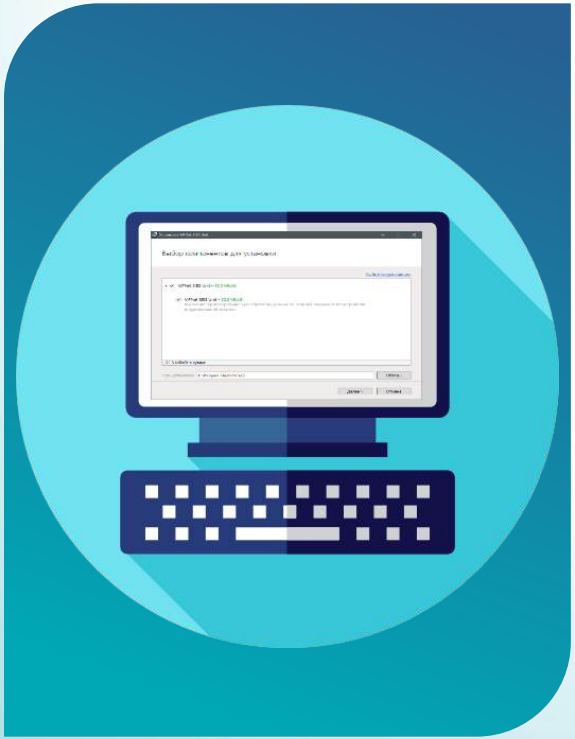
- Ключевой и Удостоверяющий центры
- Управление связями в системе
- Дистанционная смена ключевой информации
- Управление активами
- UI — Доступ к интерфейсу по WebUI
- API — API для подключения и управления сторонними СКЗИ
- Сертификат СКЗИ класса КС3 и КС1

Защита данных от АСУ ТП до IIoT

СКЗИ для всех уровней АСУ ТП, IIoT-систем и ИСУЭ



ViPNet SIES Unit



Встраивание:

- ПО устанавливается и работает как сервис ОС
- Интеграция на программном уровне – RESTfull API (HTTP/1.1), gRPC API (HTTP/2) или SDK

Криптографические функции:

- Зашифрование/расшифрование (CRISP)
- Вычисление/проверка имитовставки (CRISP)
- Зашифрование/расшифрование (CMS)
- Вычисление/проверка ЭП (CMS)
- Вычисление/проверка хэш-кода

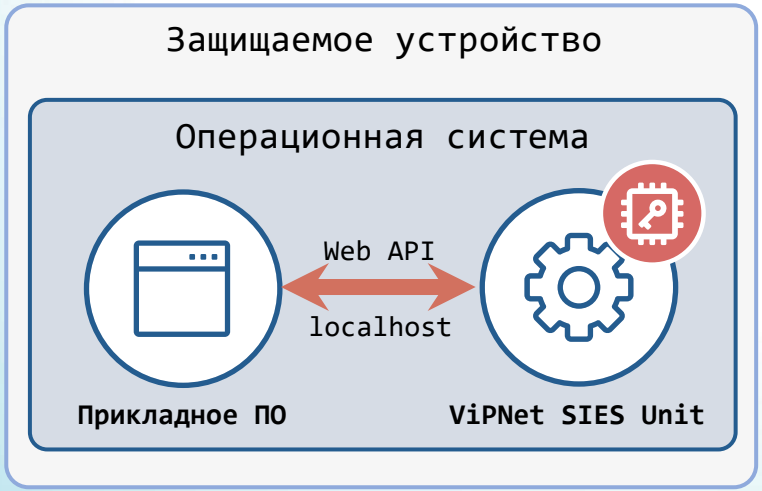
Функциональные особенности:

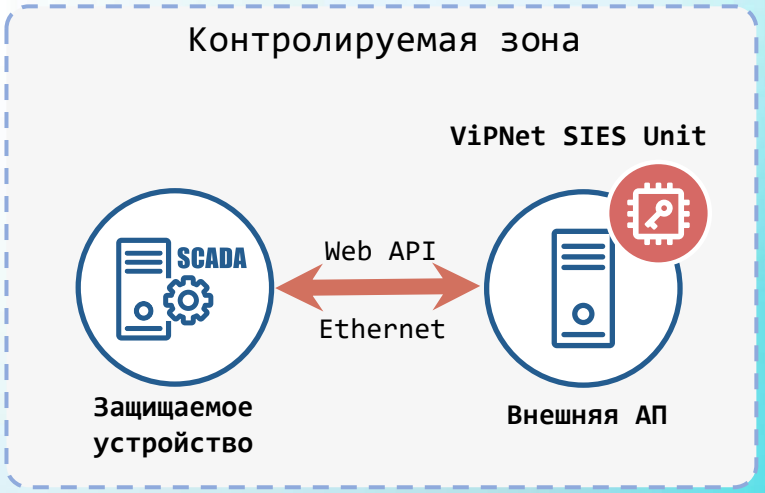
- Поддерживаемые архитектуры: x86-32, x86-64, ARM
- Поддерживаемые ОС: Windows, Linux, Astra Linux, Альт СП
- Установка на защищаемое устройство или выделенную платформу

Соответствие требованиям:

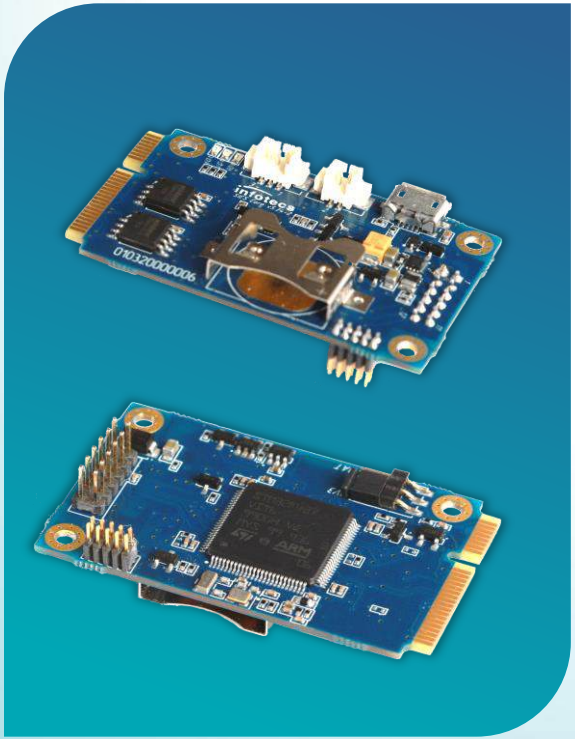
- СКЗИ класса КС1 и КС3

Интеграция ViPNet SIES Unit





ViPNet SIES Core



Встраивание:

- На аппаратном уровне – UART, USB, SPI
- На программном уровне – SIES Core API
  SDK для Linux (ARM, x86), Windows, RTOS

Криптографические функции:

- Зашифрование/расшифрование (CRISP)
- Вычисление/проверка имитовставки (CRISP)
- Зашифрование/расшифрование (CMS)
- Вычисление/проверка ЭП (CMS)
- Вычисление/проверка хэш-кода

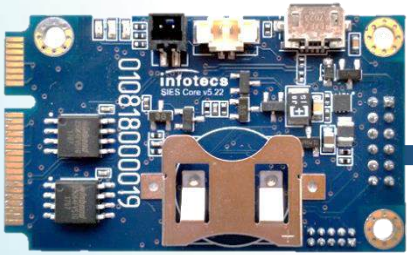
Функциональные особенности:

- Форм-фактор – плата PCI Express® Full-Mini Card
  (51 x 30 x 11,2 мм)
- Поддержка ДНСД для эксплуатации вне контролируемой зоны
- Рабочий диапазон температур -40…+70^{0}C

Соответствие требованиям:

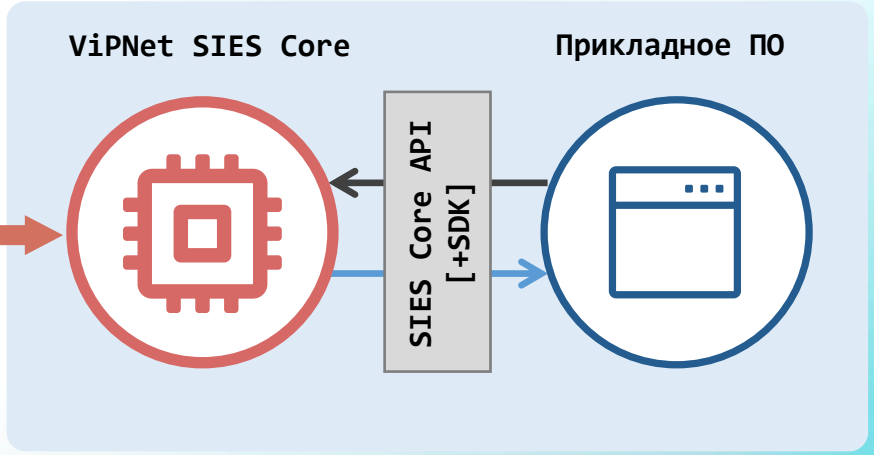
- СКЗИ класса КС3

Интеграция ViPNet SIES Core



ViPNet SIES Core

UART / USB / SPI



SIES Core SDK:

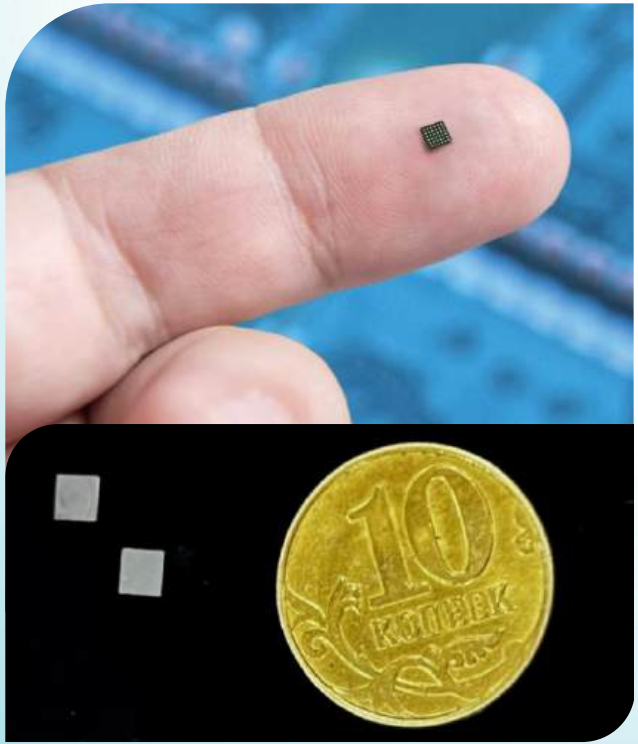
- x86-32/x86-64/ARM
- Windows
- Linux
- Baremetal (для устройств без ОС)

Защищаемое устройство
(УСПД, УСО, шлюз и т.п.)

Данные

Защищенные данные

ViPNet SIES Core Nano



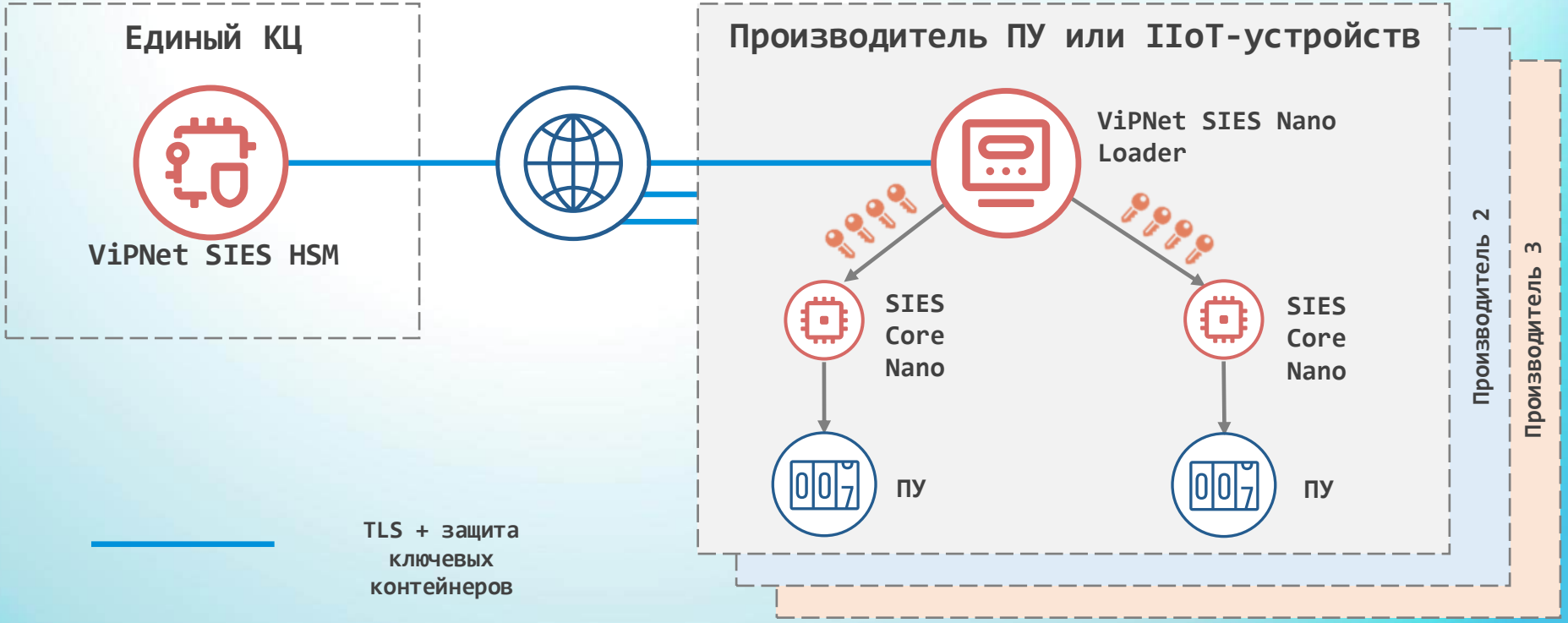
Встраивание:
- На аппаратном уровне – SPI
- На программном уровне – SIES Core Nano API

Криптографические функции:
- Зашифрование/расшифрование (CRISP)
- Вычисление/проверка имитовставки (CRISP)
- Вычисление/проверка хэш-кода

Функциональные особенности:
- 3 резервируемых ключа связи
- Хранение ключевой информации до 16 лет
- Рабочий диапазон температур -40^{0}C…+85^{0}C
- Форм-фактор – микросхема BGA36 / QFN40
- Эксплуатация вне контролируемой зоны

Соответствие требованиям:
- СКЗИ класса КС3
- Защита от атак инженерного проникновения(СКЗИ-НР)

Загрузка ключевой информации в ViPNet SIES Core Nano



ViPNet SIES Core Nano: несменные долговременные ключи сроком действия 16 лет

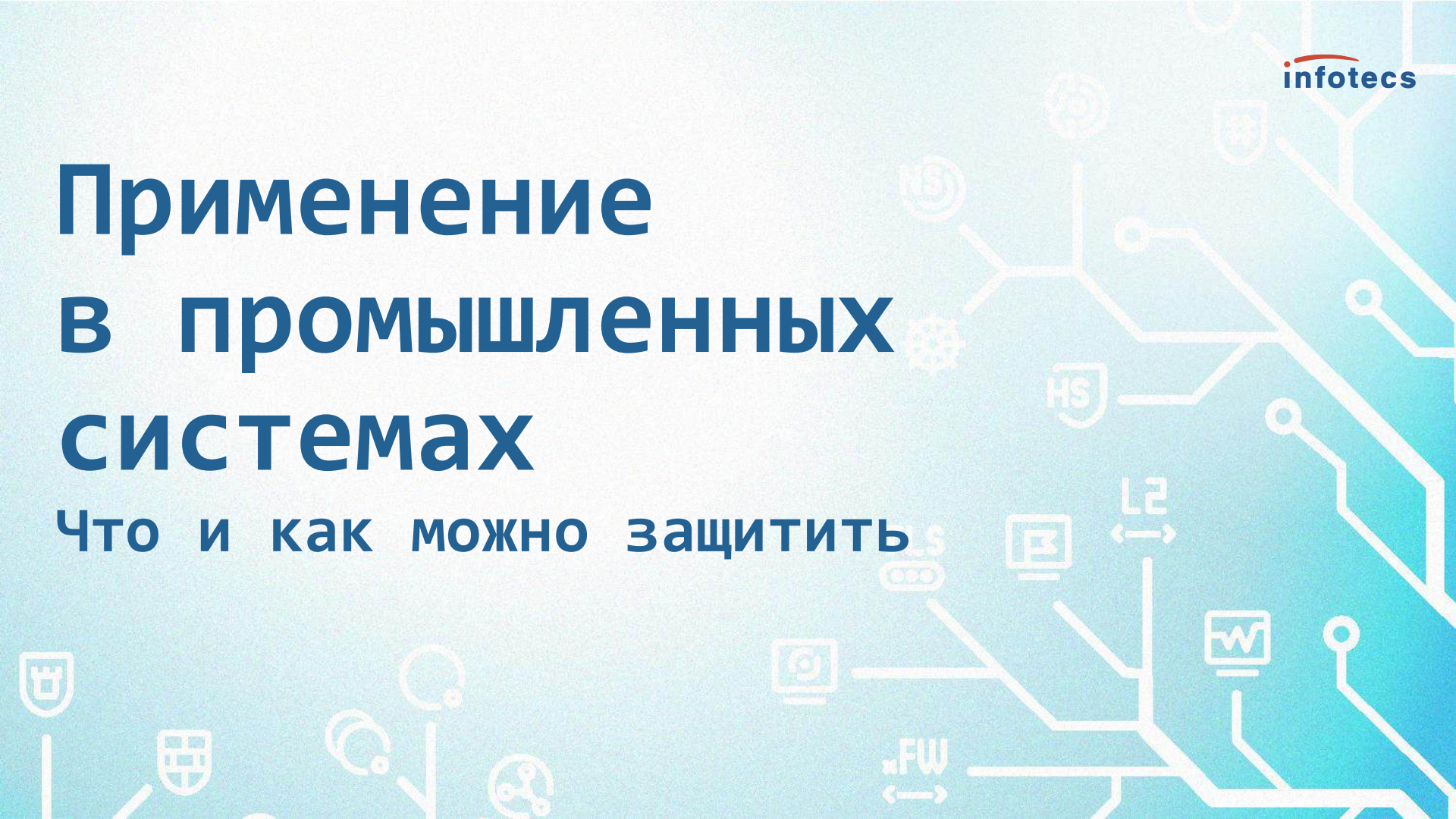
КЛЮЧИ ЗАГРУЖАЮТСЯ НА ЗАВОДЕ, ИЗГОТАВЛИВАЮЩЕМ УСТРОЙСТВО, С ПОМОЩЬЮ SIES NANO LOADER

СРЕДСТВО ГЕНЕРАЦИИ КЛЮЧЕЙ – SIES HSM

- К 1: симметричный ключ для обмена данными с устройством верхнего уровня (парная связь)
- К 2: симметричный ключ для обмена данными с устройством среднего уровня (парная связь)
- К 3: симметричный ключ для обмена данными с устройством (парная связь)
- К 4: симметричный ключ для собственных нужд ViPNet SIES Core Nano
- К 5: симметричный ключ для резервированной связи с устройствами верхнего или среднего уровня
- Служебный симметричный ключ для обмена данными с **центром управления** ViPNet SIES MC
- Резервный набор ключей

Применение в промышленных системах

Что и как можно защитить

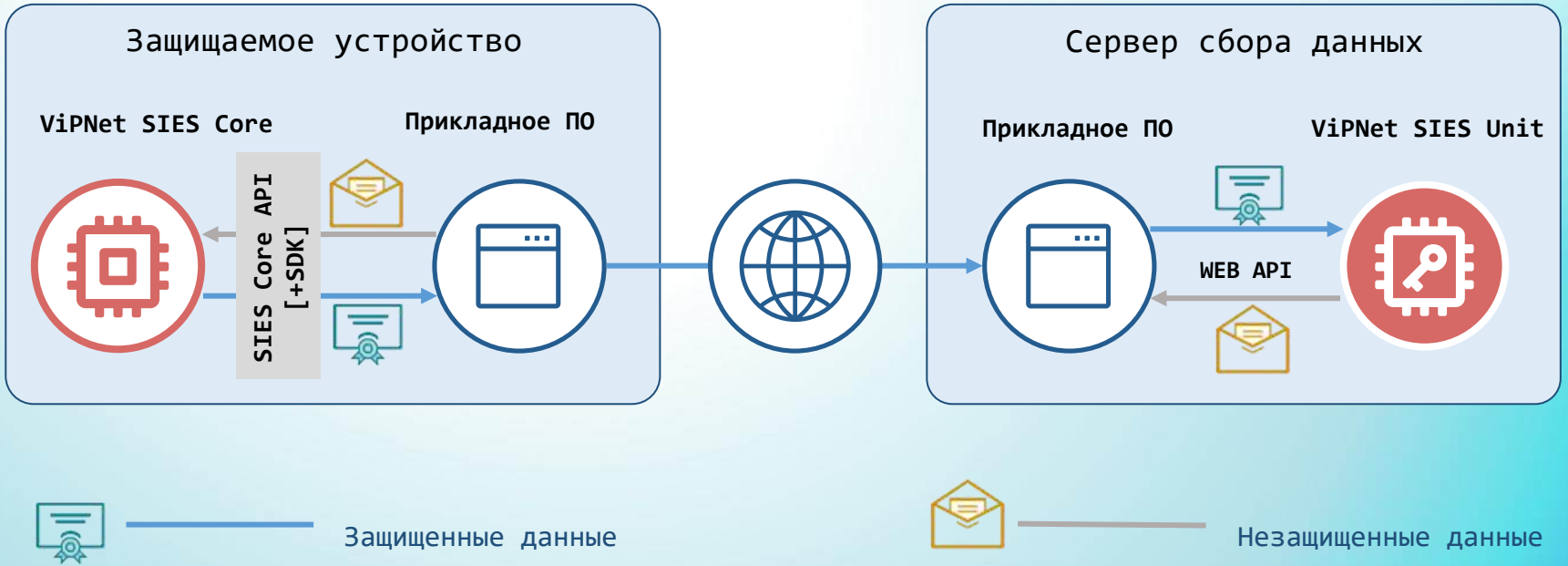


Криптографические сервисы для защищаемых устройств

Компоненты решения ViPNet SIES позволяют реализовывать следующие сценарии обеспечения информационной безопасности защищаемых устройств:

- Защита данных при передаче по каналам связи вне зависимости от типа сети
- Доверенное обновление защищаемого устройства
- Доверенное локальное и дистанционное конфигурирование защищаемого устройства
- Локальная и дистанционная аутентификация пользователей защищаемого устройства

Защита коммуникаций с помощью ViPNet SIES



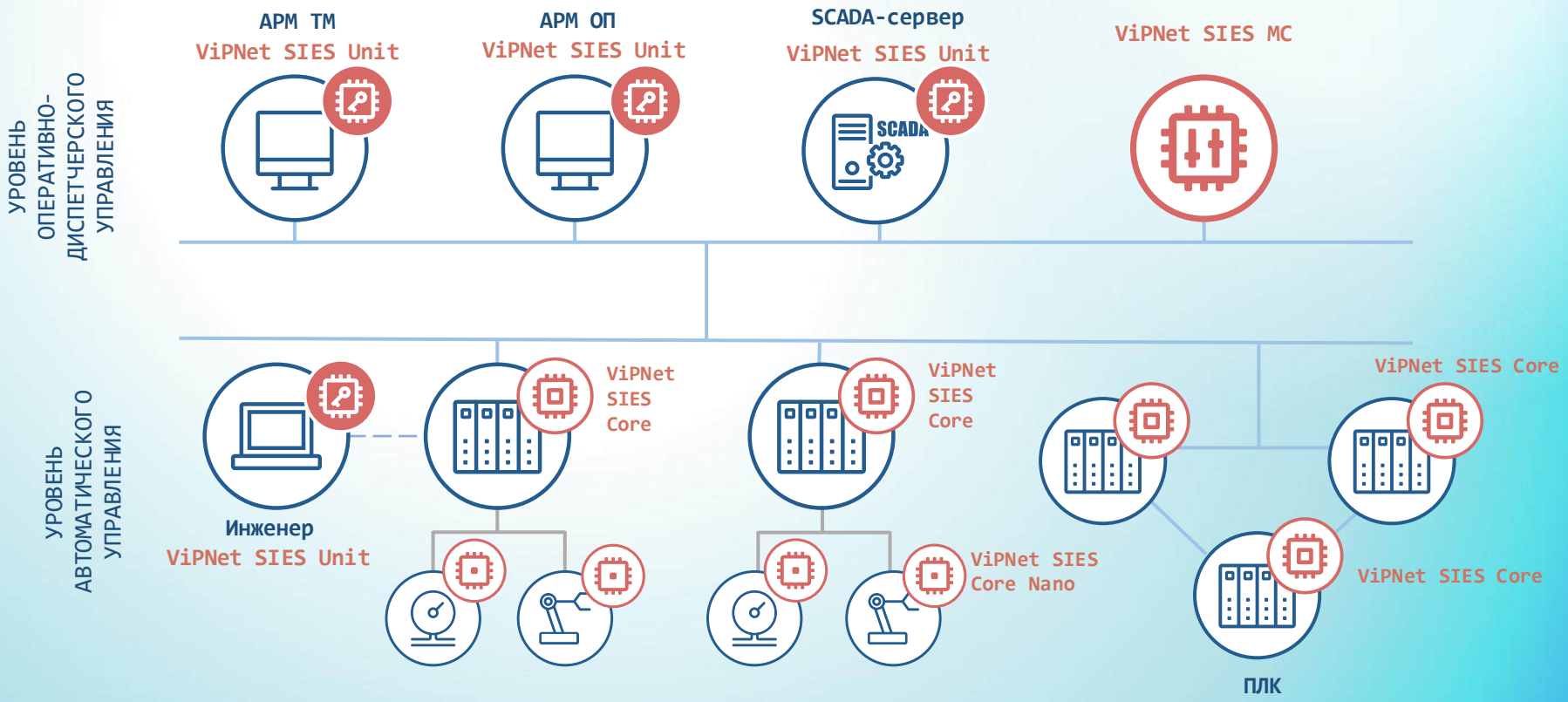
Защита данных с помощью протокола CRISP

- Целостность
- Конфиденциальность (опционально)
- Защита от навязывания повторных сообщений
- Аутентификация источника сообщений

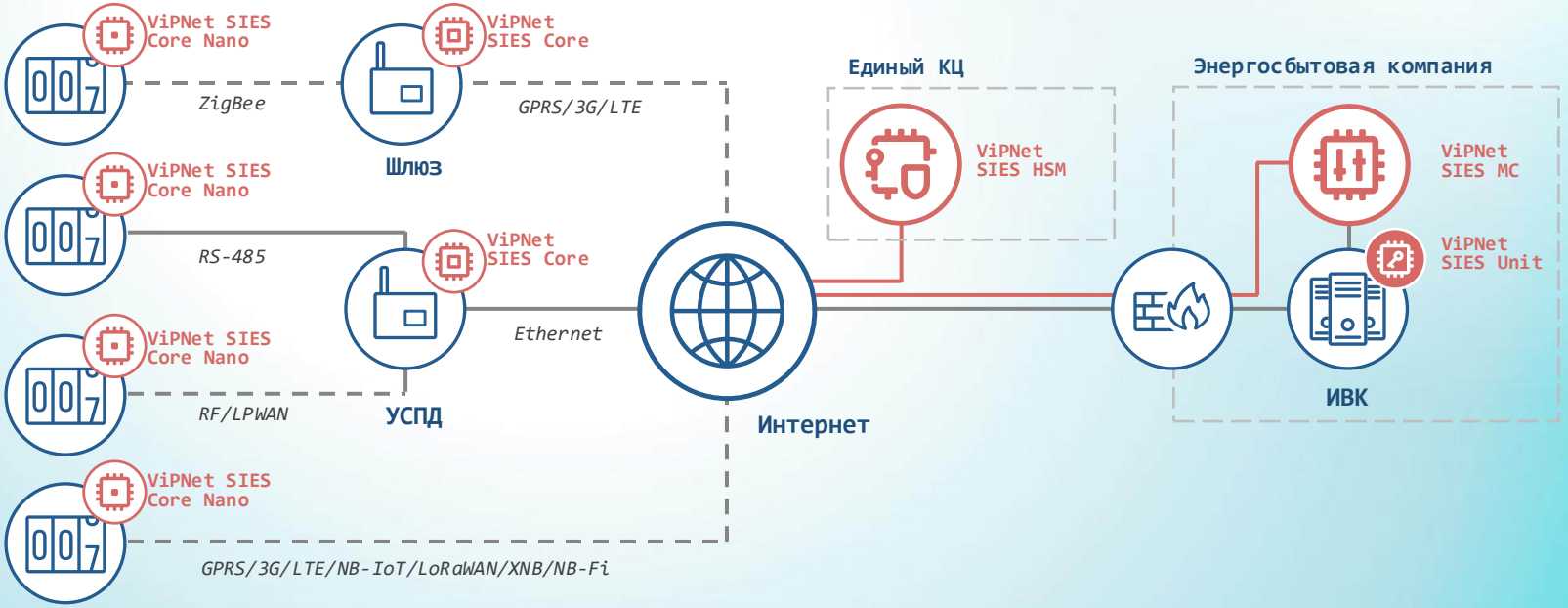
* Протокол CRISP (ГОСТ Р 71252-2024) входит в перечень рекомендованных Минцифры России протоколов для ИСУЭ и IIoT

- Защита адресных и групповых сообщений
- Бессесионный криптографический протокол
- Минимальные накладные расходы (overhead)и минимальная нагрузка на сеть
- Универсальный стандартизированный протокол защиты любых протоколов ИСУЭ

Защищенная АСУ ТП



Защита данных в ИСУЭ



ViPNet SIES AMI Proxy

Функции:

- Обеспечение криптографической защиты данных для протоколов СПОДЭС/СПОДУС
- Автоматическое наложение и снятие криптографической защиты данных при помощи ViPNet SIES Unit
- Обеспечивает единую точку подключения к ИВК ИСУЭ по протоколам СПОДЭС/СПОДУС
- Обеспечивает совместимость продуктов ViPNet SIES с ИВК различных производителей, поддерживающих СПОДЭС/СПОДУС

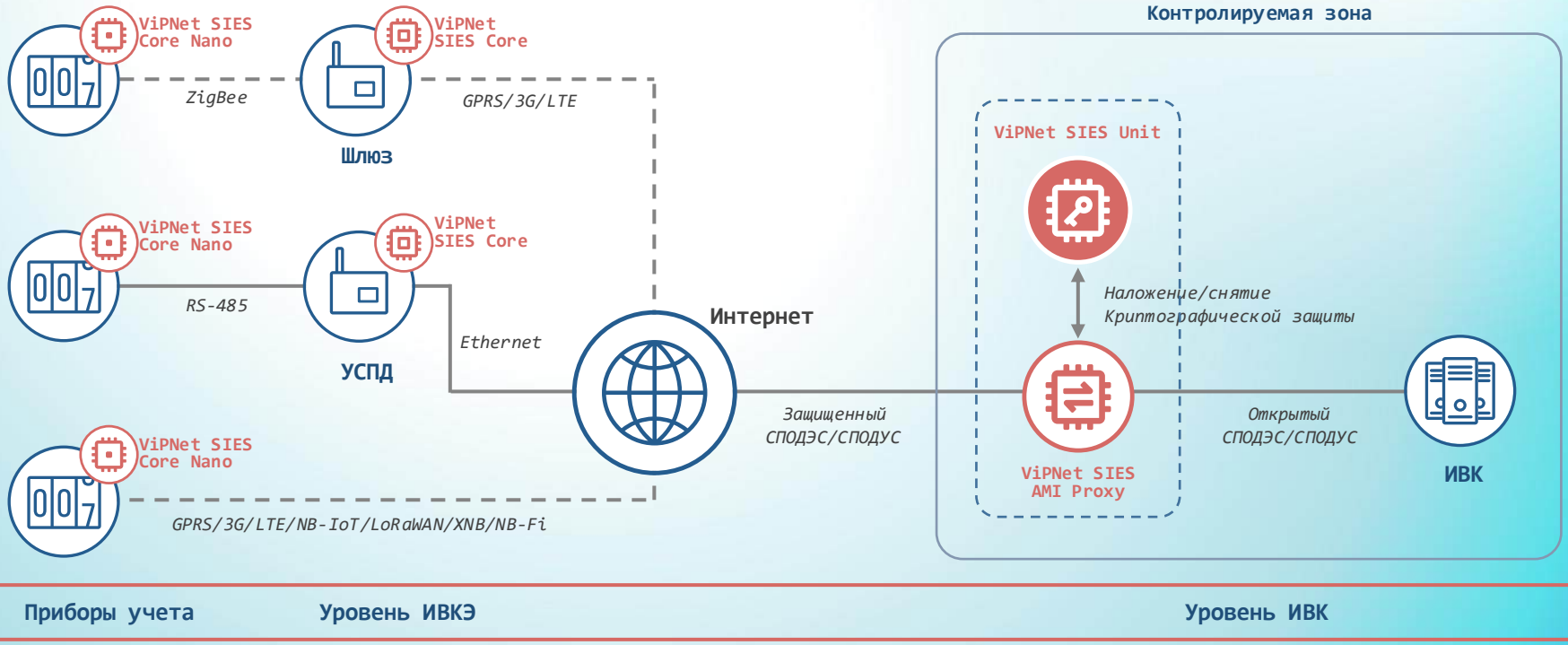
Функциональные особенности:

- Программный комплекс работает как служба ОС
- Стоит в разрыв связи перед ИВК ИСУЭ, перехватывая данные
- Прозрачный режим при взаимодействии ИВК с ИВКЭ и ПУ
- Поддерживаемые архитектуры: x86-64
- Поддерживаемые ОС: Astra Linux, Альт СП, Debian

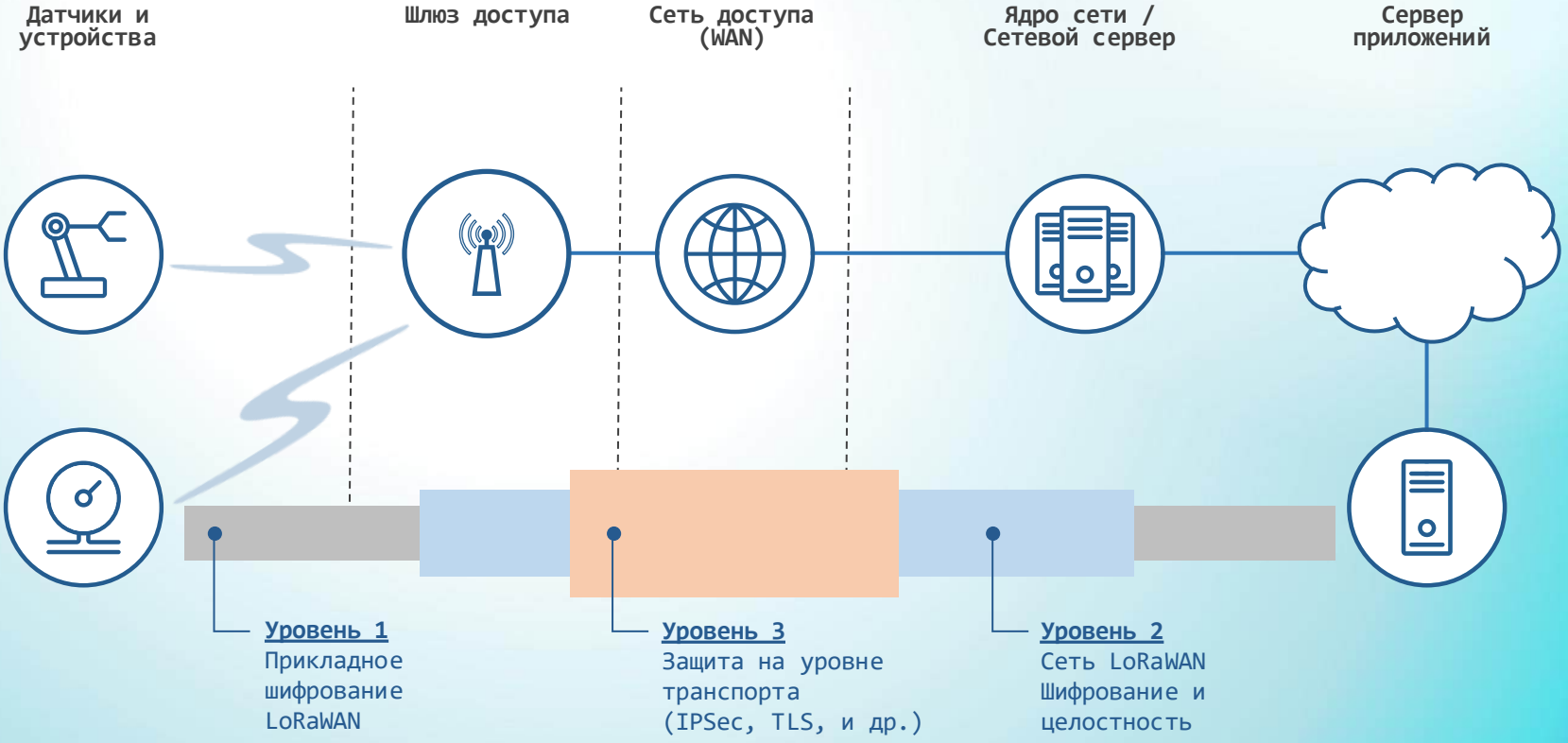
Соответствие требованиям:

- Не является СКЗИ и не подлежит сертификации

Защита данных в ИСУЭ



Защита данных в LoRaWAN



Защита данных в LoRaWAN RU

ViPNet SIES Unit Router

Функции:

- Повышение производительности ViPNet SIES Unit
- Распределение запросов на выполнение криптографических операций между несколькими ViPNet SIES Unit
- Обеспечивает единую точку входа для подключения множества защищаемых устройств к нескольким ViPNet SIES Unit
- Автоматическая генерация таблицы маршрутизации запросов
- Резервирование ViPNet SIES Unit

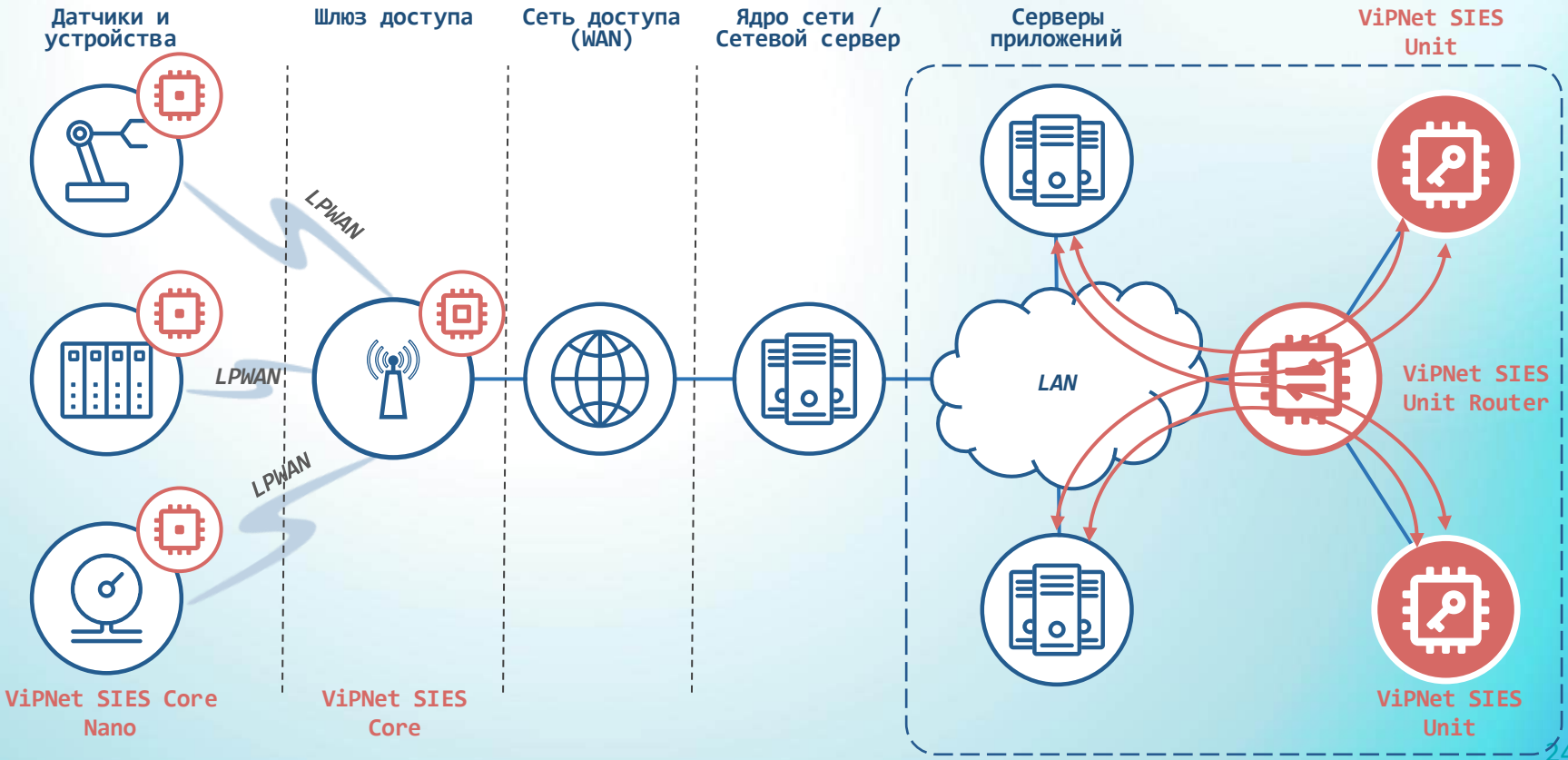
Функциональные особенности:

- Программный комплекс работает как служба ОС
- Поддержка резервирования (кластер ViPNet SIES Unit Router)
- Поддерживаемые архитектуры: x86-64
- Поддерживаемые ОС: Astra Linux, Альт СП

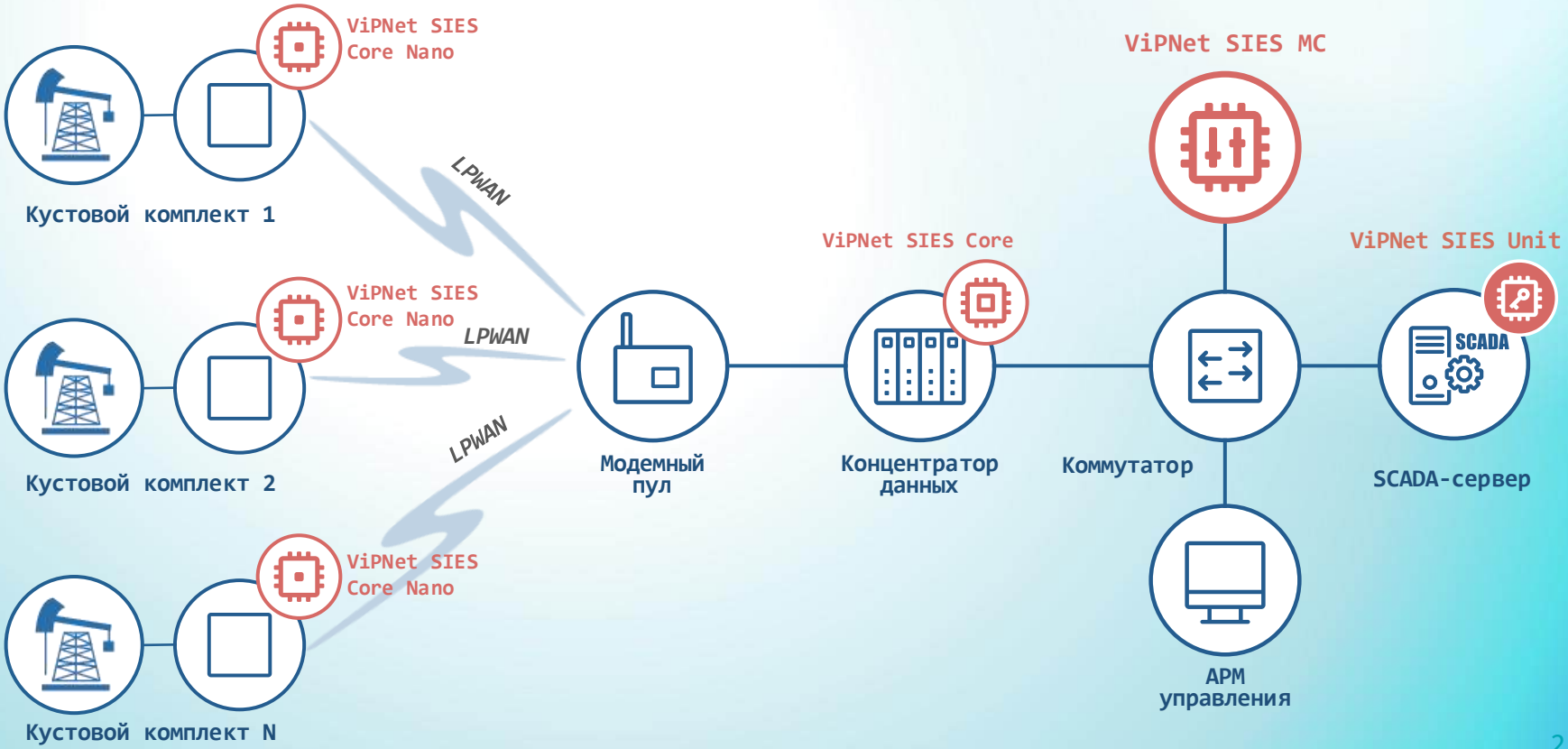
Соответствие требованиям:

- Не является СКЗИ и не подлежит сертификации

Защита данных в IIoT-системе



Защита данных в АССД



Подписывайтесь
на наши соцсети,
там много интересного

infotecs