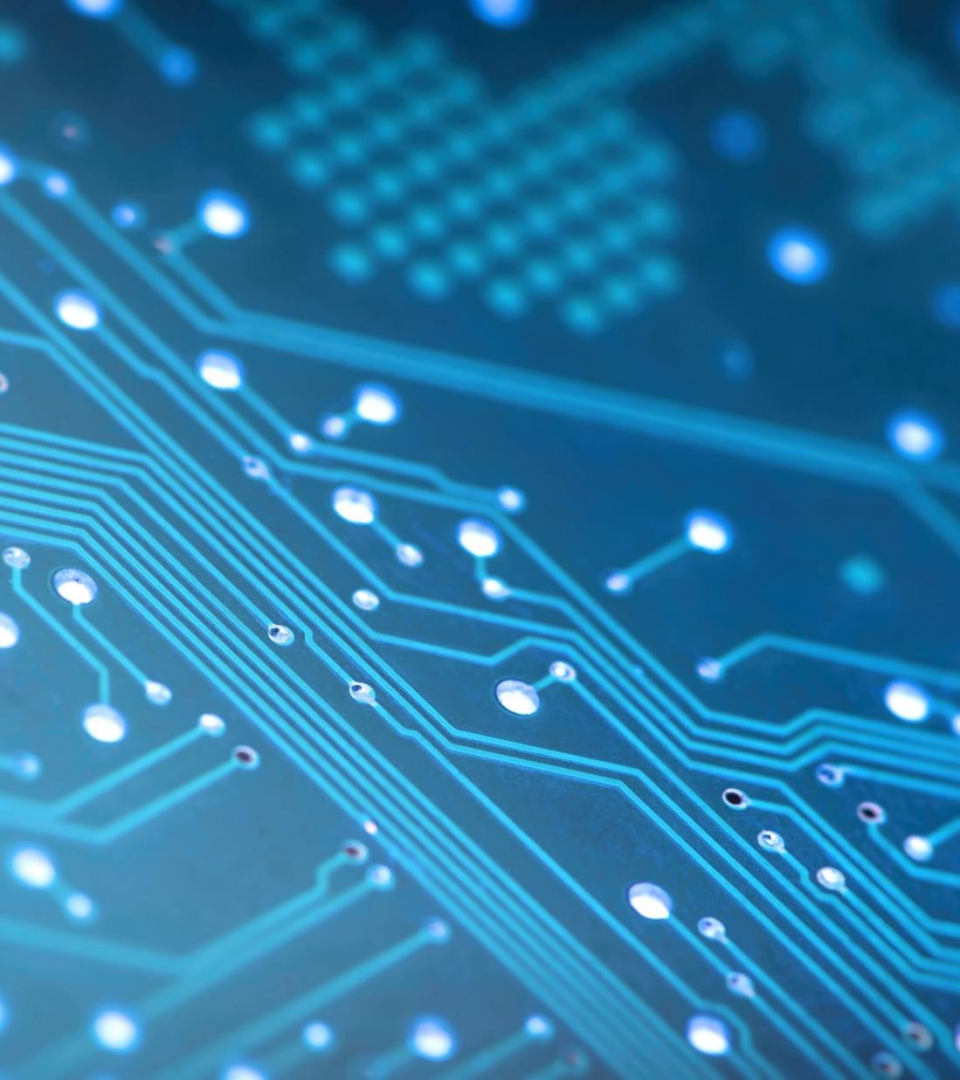


VIPNet SIES Core Nano – крипточип для IIoT-устройств и приборов учета

Алексей Власенко
ведущий менеджер продуктов


infotecs



The left side of the slide features a vertical background image of a glowing blue circuit board. The traces and components are illuminated with a bright blue light, creating a sense of depth and technology.

Решение **VIPNet SIES** встраиваемые СКЗИ

Решение ViPNet SIES для ИСУЭ

SIES MC API



УПРАВЛЕНИЕ

ЗАЩИТА
УСТРОЙСТВ

ViPNet SIES MC

ViPNet SIES Nano Loader

ViPNet SIES Workstation
ViPNet SIES Smartmeter WS

ViPNet SIES Core Nano

ViPNet SIES Core

ViPNet SIES Unit

НИЖНИЙ УРОВЕНЬ

СРЕДНИЙ УРОВЕНЬ

ВЕРХНИЙ УРОВЕНЬ

Решение ViPNet SIES – это комплекс продуктов для криптографической защиты IIoT-устройств и компонентов ИСУЭ:

- ПAK ViPNet SIES Core Nano - для встраивания в ПУ, IIoT-устройства, LPWAN модули связи
- ПAK ViPNet SIES Core - для встраивания в IIoT-шлюзы, УСПД, LPWAN базовые станции
- ПК ViPNet SIES Unit - для интеграции с серверами и рабочими станциями
- ПAK ViPNet SIES MC - для управления ключевой информацией решения
- ПК ViPNet SIES Workstation – для инициализации ViPNet SIES Core и SIES Unit
- SIES MC API – API для интеграции сторонних СКЗИ в решение ViPNet SIES

Центр управления ViPNet SIES MC



- ПAK ViPNet SIES MC 10000
 - До 1 млн. устройств
 - СКЗИ класса КС3
- ПAK ViPNet SIES MC 3000
 - До 3000 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



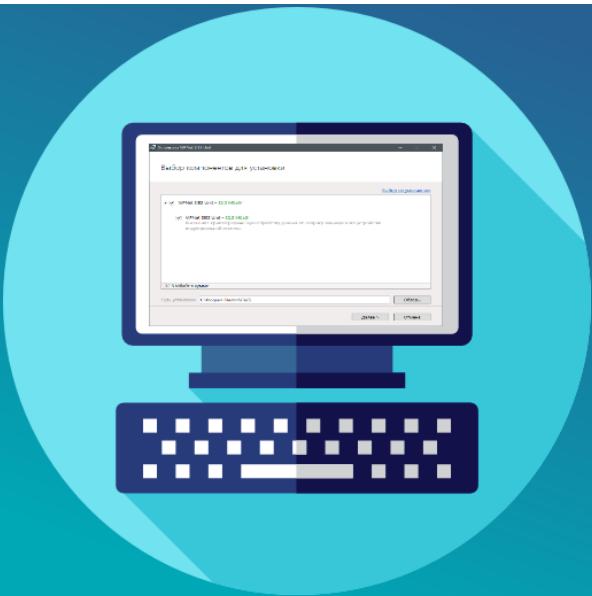
Доступ к интерфейсу по WebUI



API для подключения и управления сторонними СКЗИ



Сертификат СКЗИ класса КС3 и КС1



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

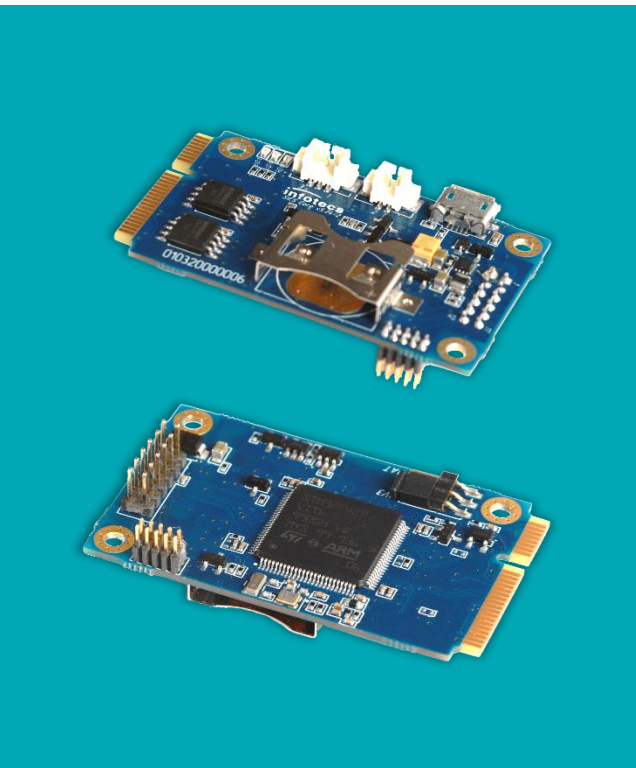
Функциональные особенности:

- Поддерживаемые архитектуры – x86-32, x86-64, ARM (armhf)
- Поддерживаемые ОС – Windows, Linux (Debian 9.8, 10/Ubuntu 16, 18/Astra Linux SE 1.6, 1.7 Смоленск)
- Установка на защищаемое устройство или выделенную платформу

Соответствие требованиям:

- СКЗИ класса КС1 и КС3

ПАК 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

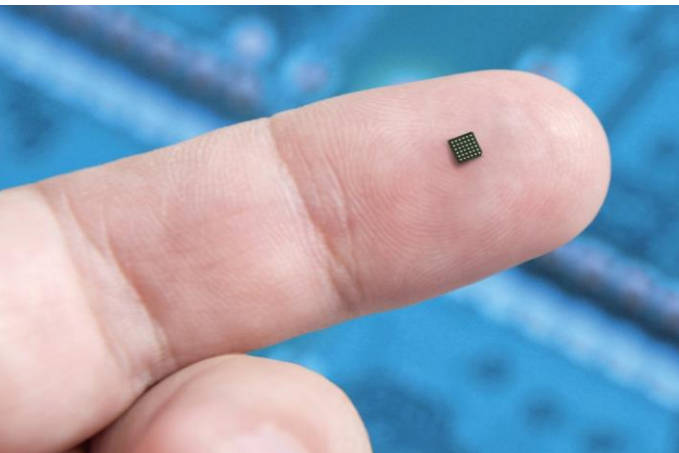
Функциональные особенности:

- 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°C

Соответствие требованиям:

- СКЗИ класса КСЗ

ПАК ViPNet SIES Core Nano



Встраивание:

- На аппаратном уровне – SPI
- На программном уровне – Core Nano API

Область применения:

- Защита данных IIoT-устройств
- Защита данных приборов учета
- Встраивание в модули связи LPWAN

Функциональные особенности:

- 3 резервируемых ключа связи
- Хранение ключевой информации до 16 лет
- Рабочий диапазон температур -40...+85°C
- Форм-фактор – микросхема BGA36 3x3x0,4 мм

Соответствие требованиям:

- СКЗИ класса КСЗ
- Защита от атак инженерного проникновения (СКЗИ-ИР)

СКЗИ ViPNet SIES Core Nano

Криптографические алгоритмы –
ГОСТ Р 34.12-2018, ГОСТ Р 34.13-2018,
ГОСТ Р 34.11-2018

Криптографический протокол –
Р 1323565.1.029-2019 (CRISP)
(наборы 3 и 4)

Соответствие требованиям:

- СКЗИ класса КСЗ*
- СКЗИ-НР в части защиты от атак инженерного проникновения*



Защита данных с помощью протокола CRISP

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

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



PLC



ZigBee®



RF

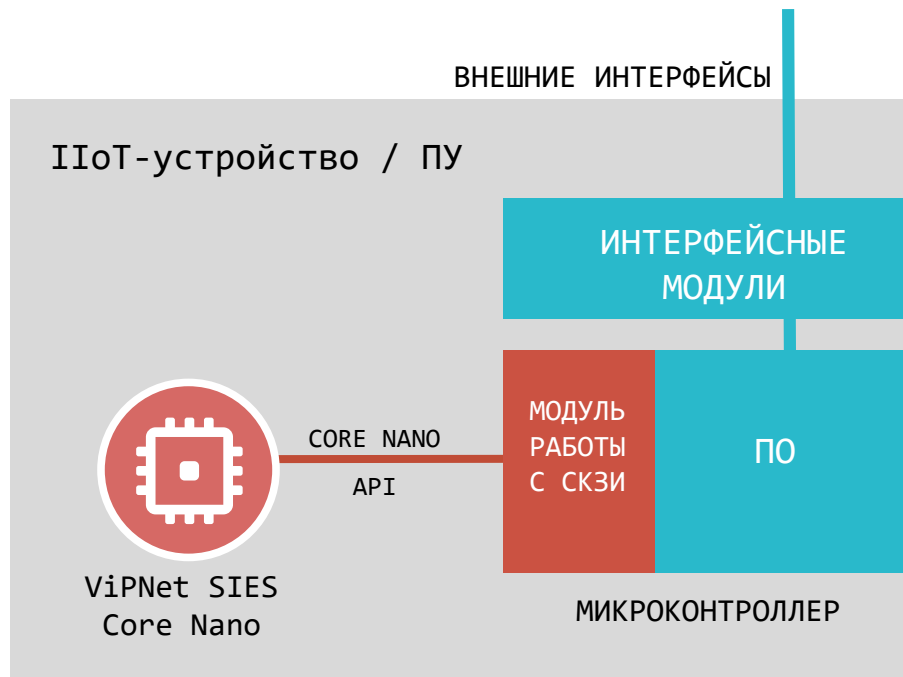


* Протокол CRISP (Р 1323565.1.029-2019) входит в перечень рекомендованных Минцифрой протоколов для ИСУЭ

Встраивание ViPNet SIES Core Nano в IIoT-устройства и приборы учета

Интеграция на аппаратном уровне – SPI

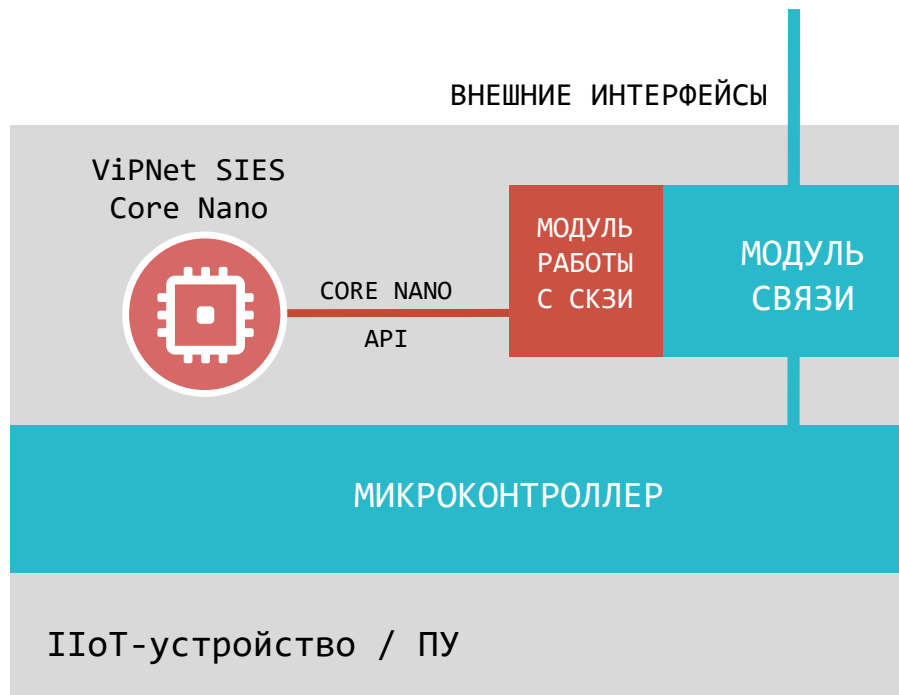
Интеграция на программном уровне – Core Nano API



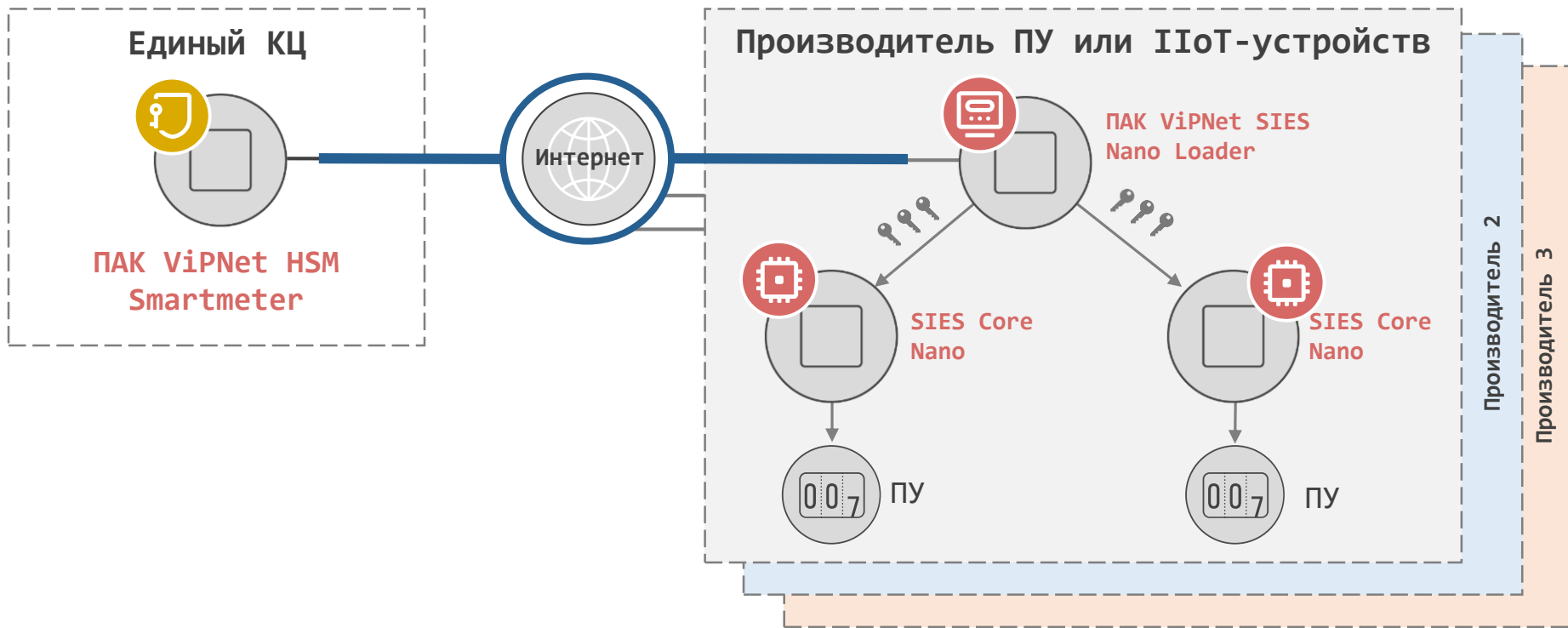
Встраивание ViPNet SIES Core Nano в модули связи устройств

Интеграция на
аппаратном уровне – SPI

Интеграция на
программном уровне –
Core Nano API

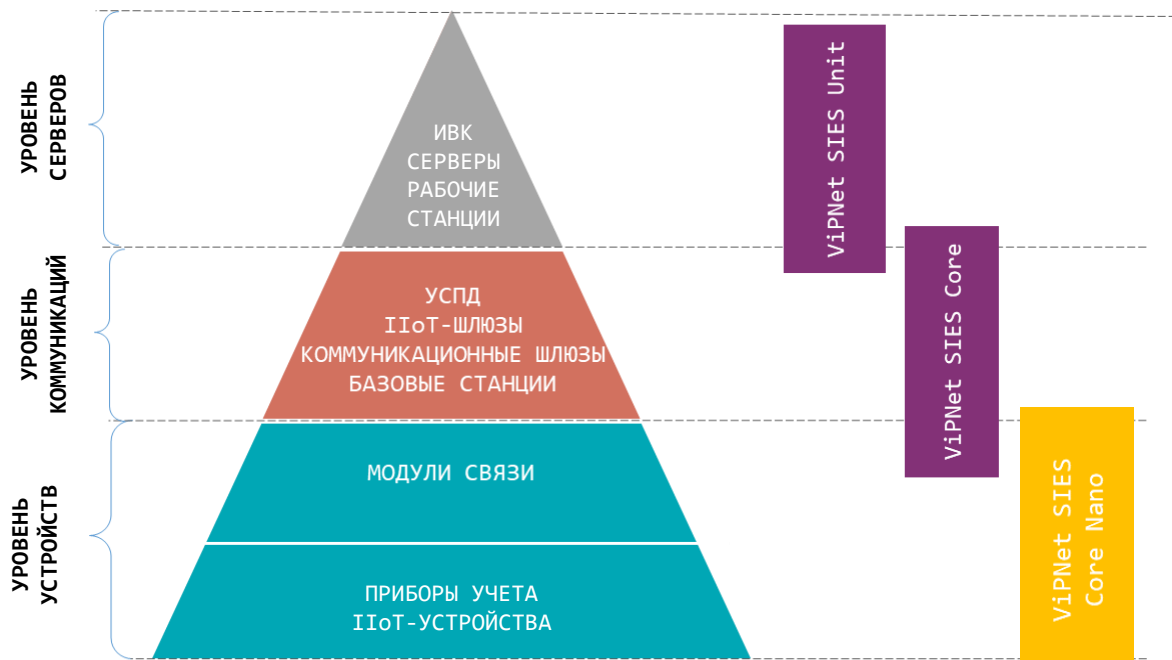


Загрузка ключевой информации в ViPNet SIES Core Nano

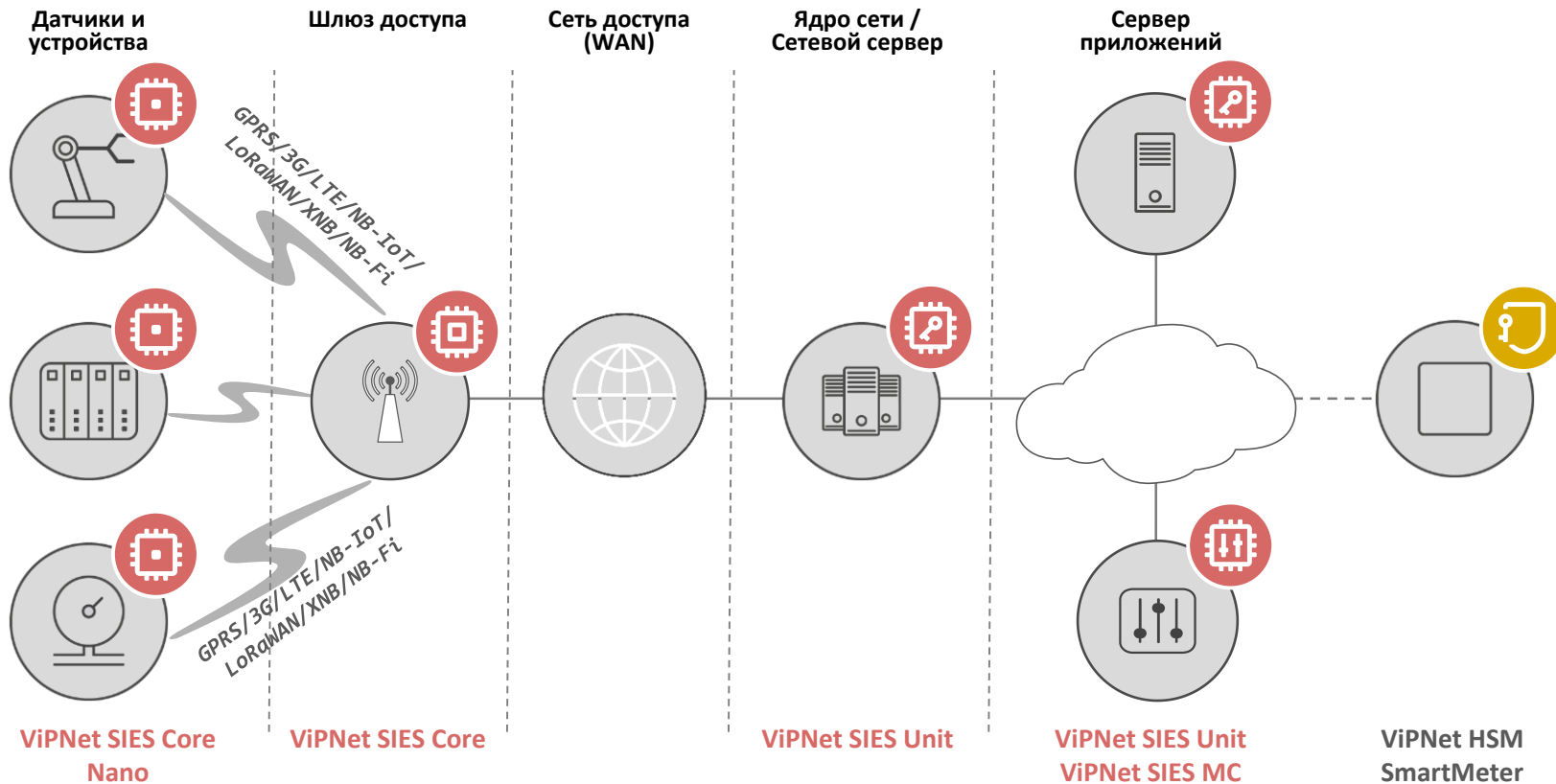


Защита данных до уровня IIoT-устройств и приборов учета

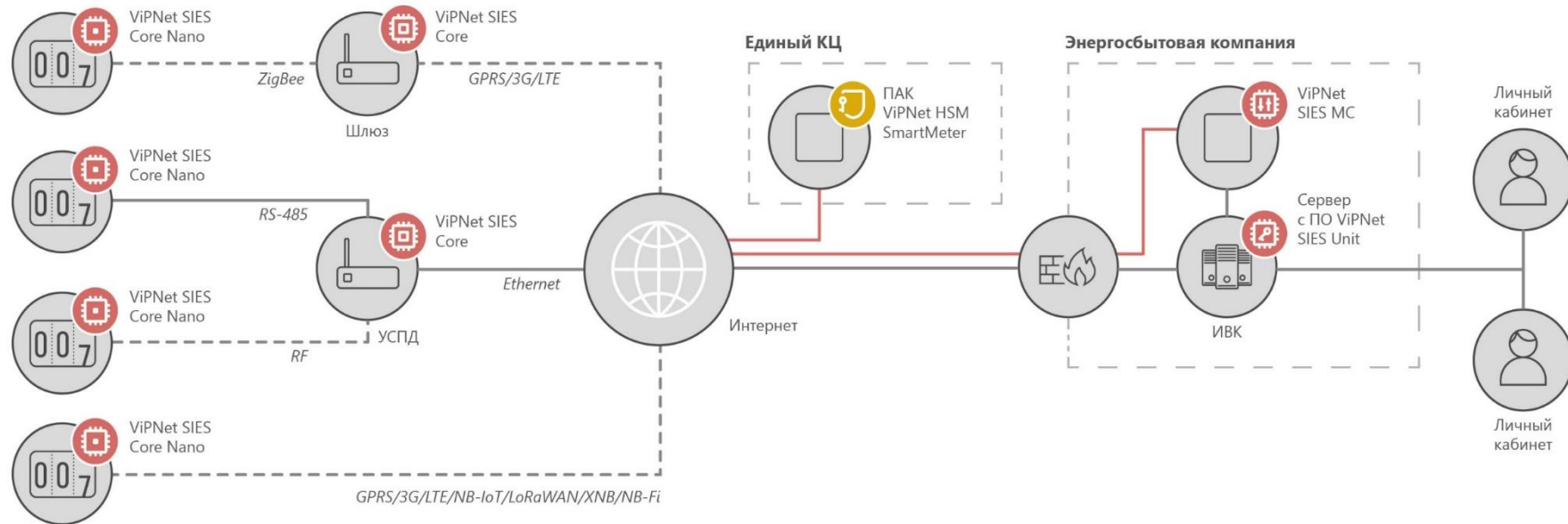
СКЗИ для всех уровней ИСУЭ и IIoT-системы



Защита данных в IIoT-системе



Защита данных в ИСУЭ

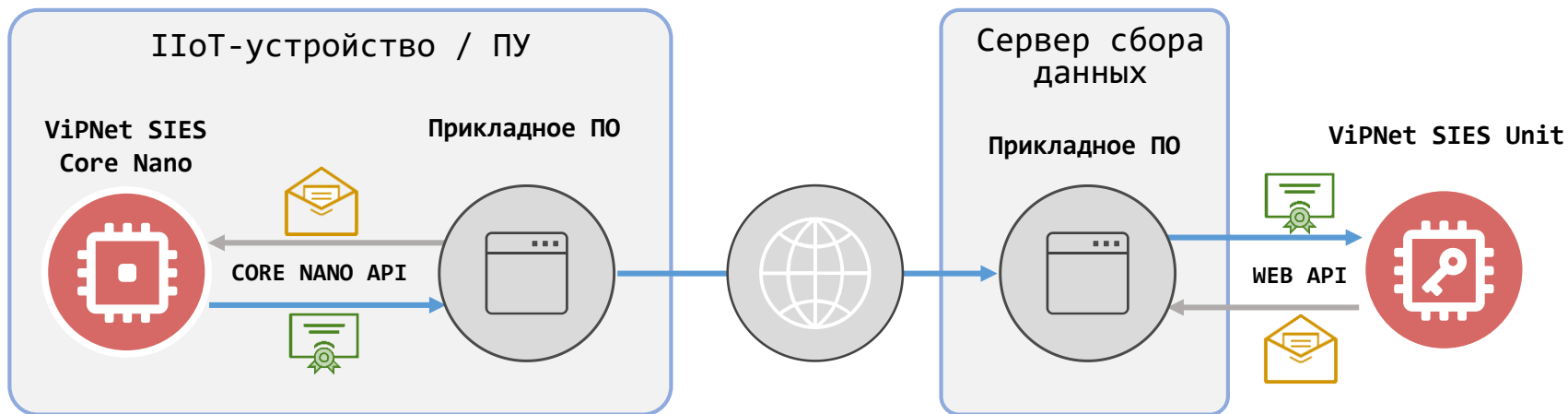


Приборы учета (ПУ)


Уровень ИСКЭ

Уровень ИСК

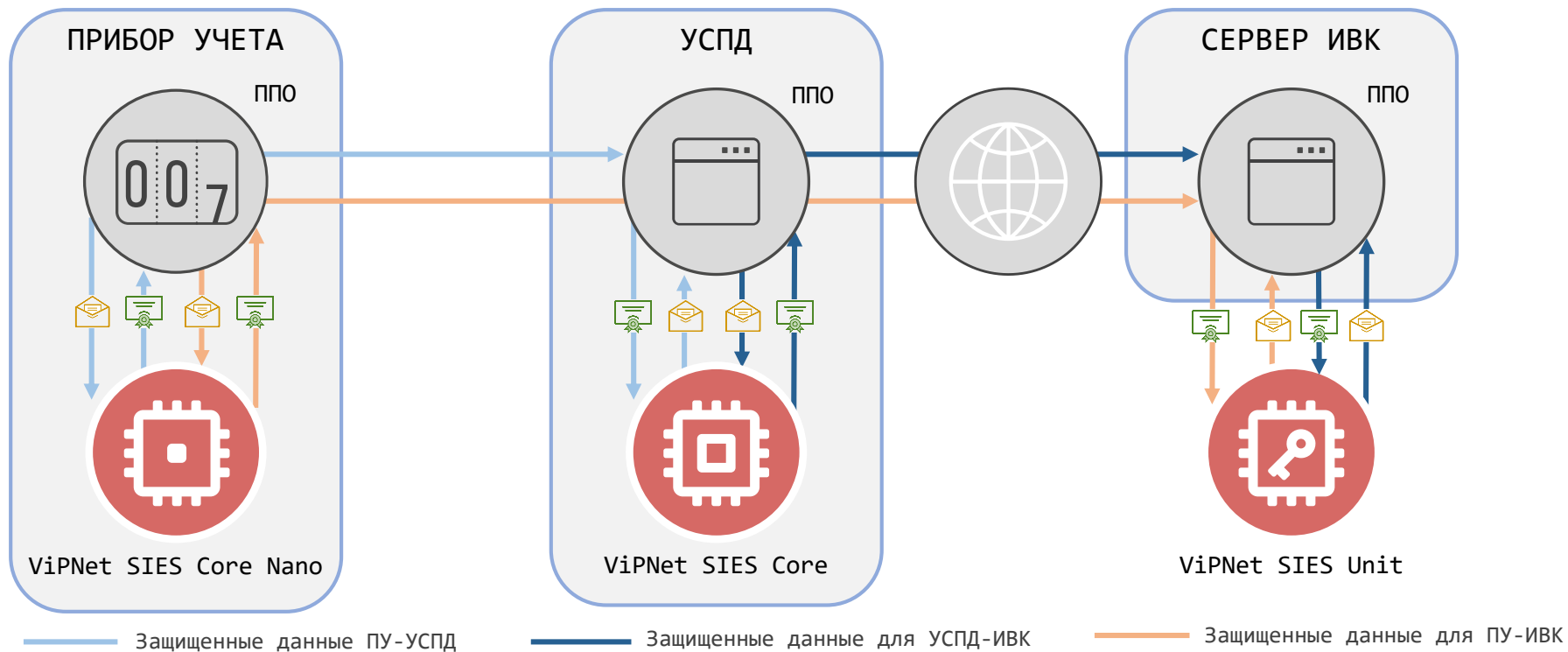
Защита данных ПУ с помощью ViPNet SIES (двухзвенная схема)



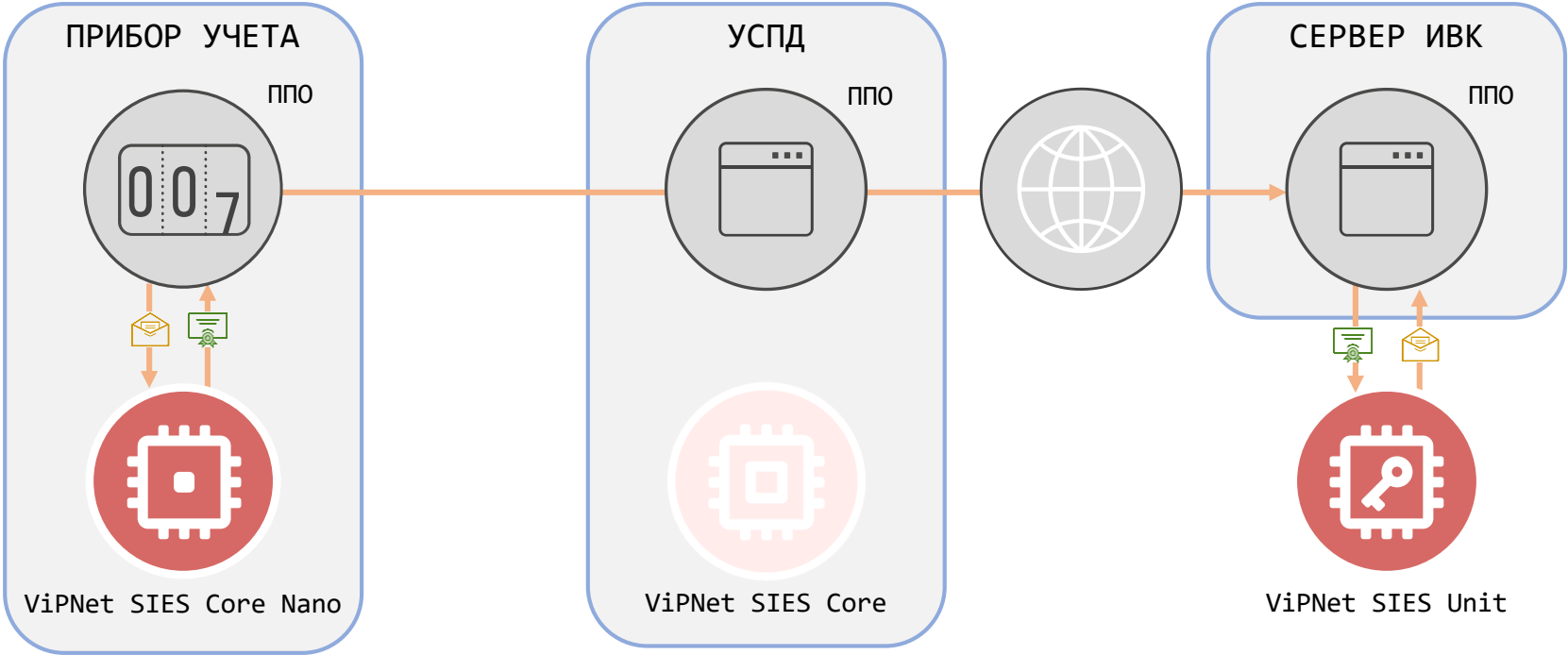
 Защищенные данные

 Незащищенные данные

Защита данных ПУ с помощью ViPNet SIES (трехзвенная схема)

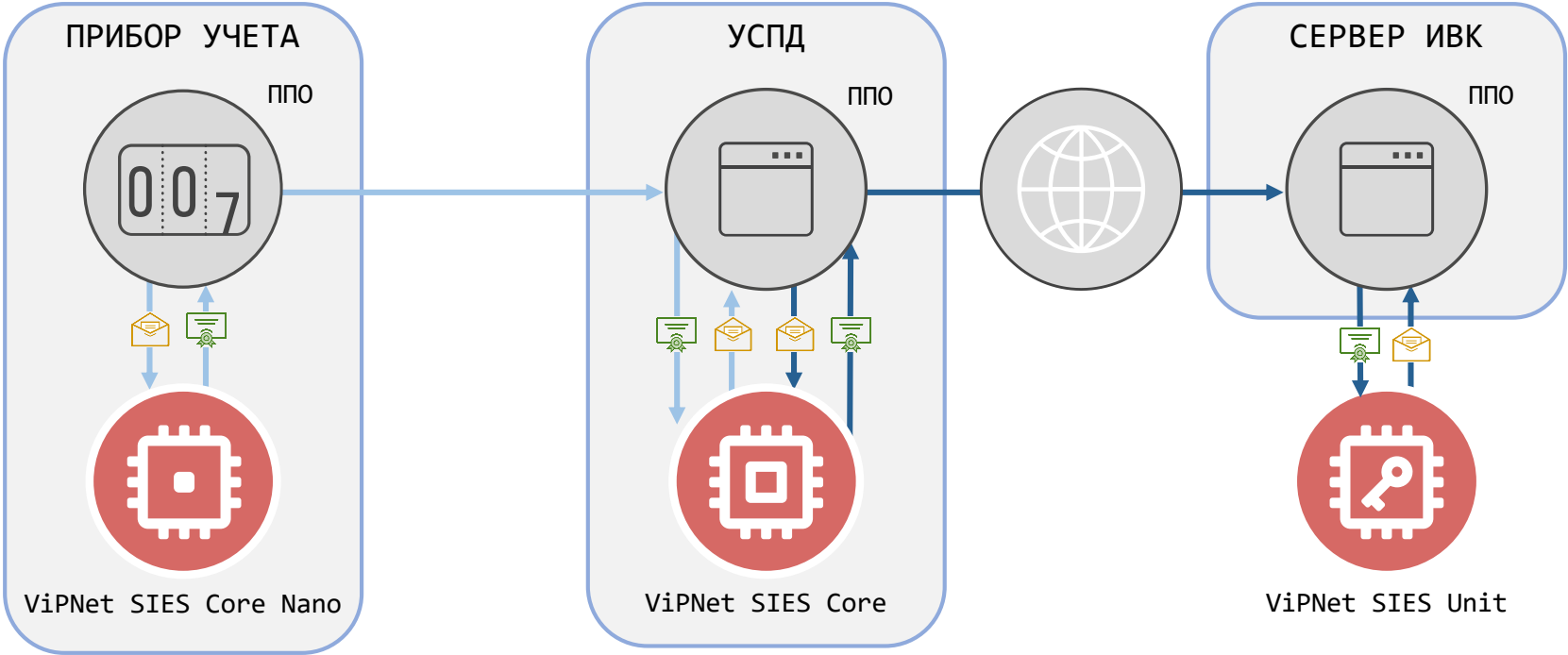


Защита данных ПУ-ИВК (трехзвенная схема)



— Защищенные данные для ПУ-ИВК

Защита данных ПУ-ИВКЭ-ИВК (трехзвенная схема)

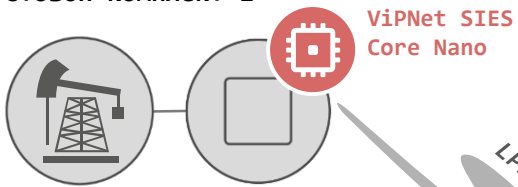


— Защищенные данные ПУ-УСПД

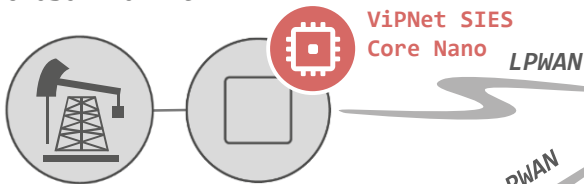
— Защищенные данные для УСПД-ИВК

Защита данных в АССД

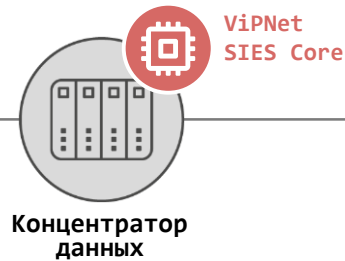
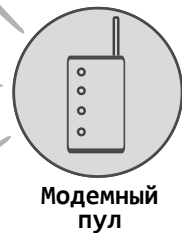
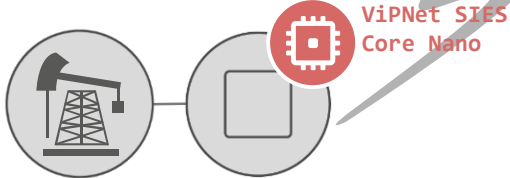
Кустовой комплект 1



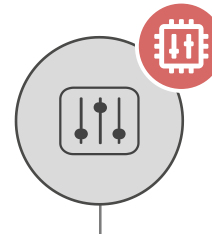
Кустовой комплект 2



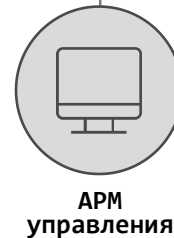
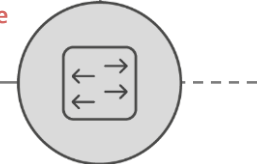
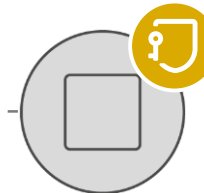
Кустовой комплект N



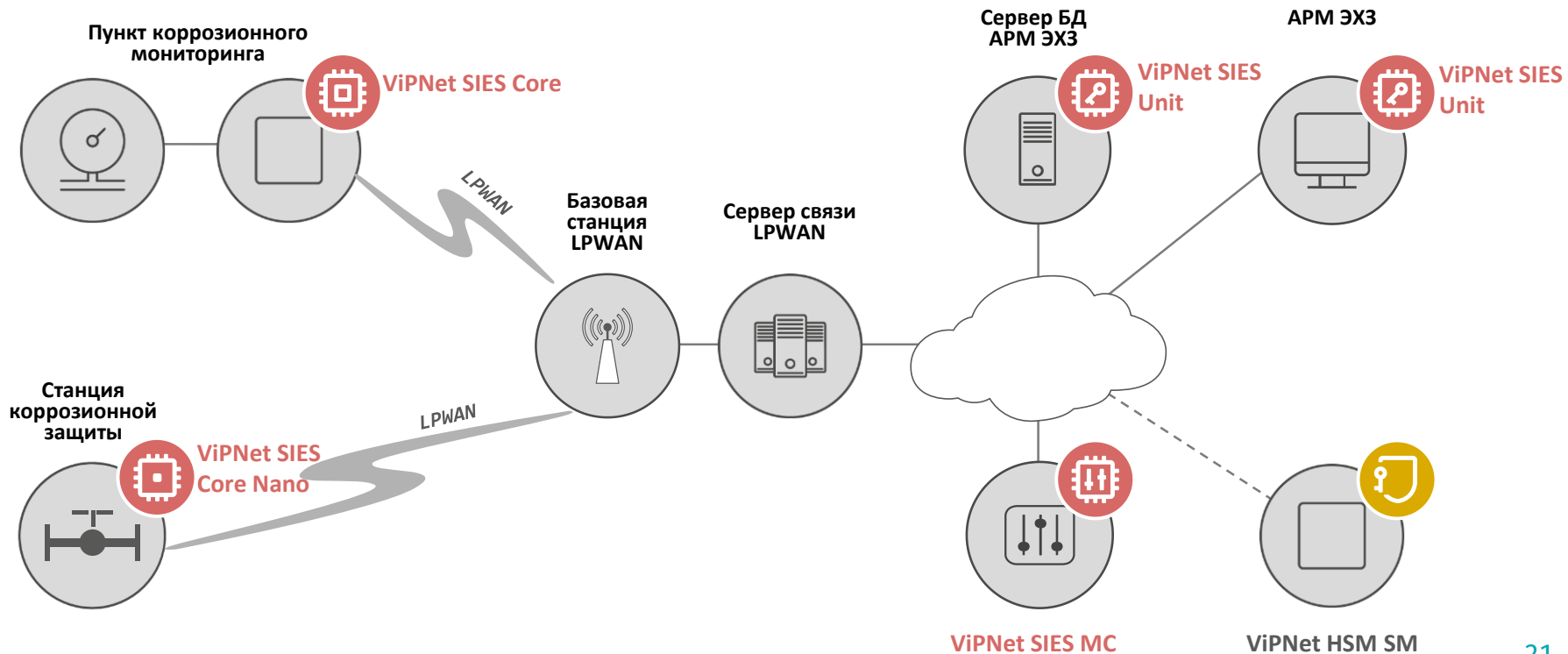
ViPNet SIES MC



ViPNet HSM SM



Защита данных в системе коррозионного мониторинга



VIPNet SIES Core Nano



низкое
энергопотребление



не требует
обслуживания



высокий класс
защиты



эксплуатация вне
контролируемой зоны



не требует смены
ключей в течение
всего срока службы
изделия



протокол CRISP,
подходящий для защиты
данных в большинстве
известных IoT-протоколов



централизованное
управление из
VIPNet SIES MC



полностью
русская
разработка



Спасибо за внимание!

Алексей Власенко

Менеджер отдела развития продуктов

e-mail: Aleksey.Vlasenko@infotecs.ru

Подписывайтесь на наши соцсети



vk.com/infotecs_news



t.me/infotecs_news



rutube.ru/channel/24686363