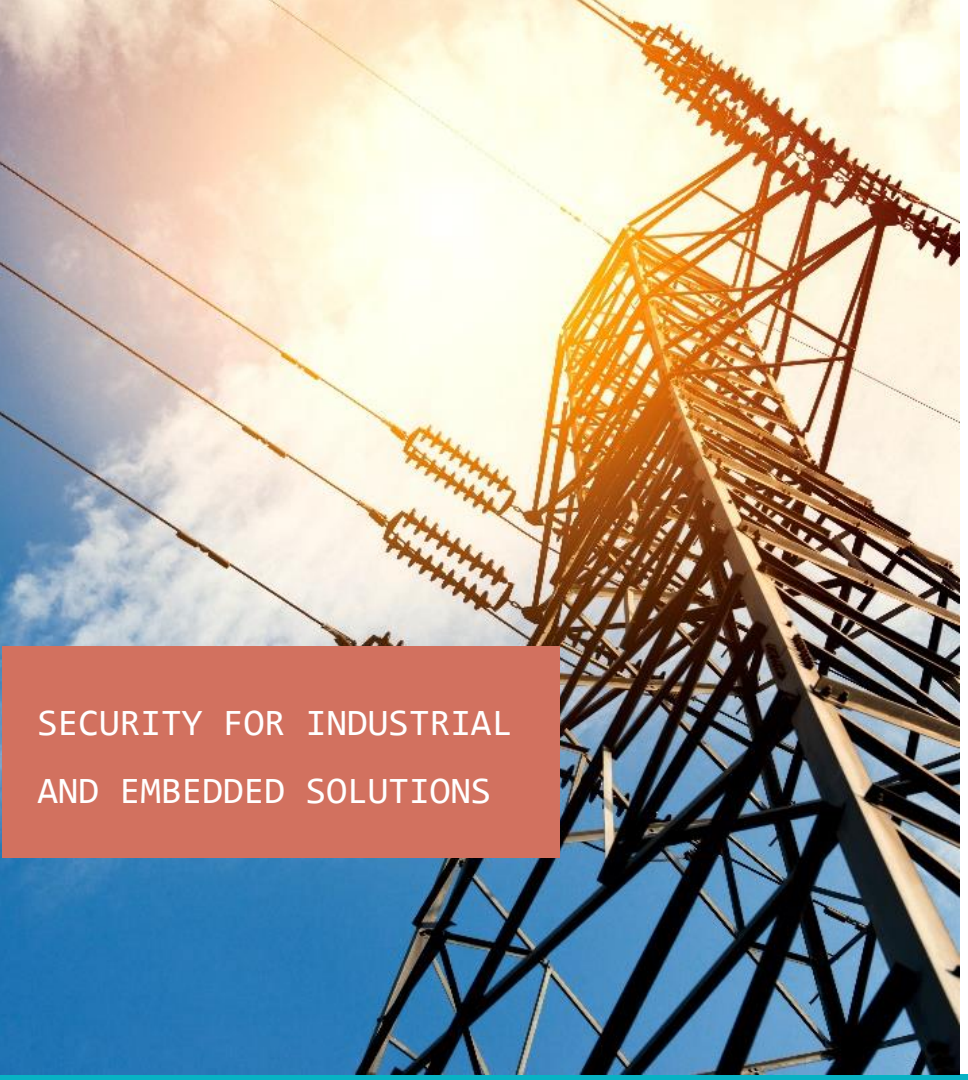
Крипточип ViPNet SIES Core Nano – встраиваемый СКЗИ для IIoT и ИСУЭ

Алексей Власенко
ведущий менеджер продуктов

Решение ViPNet SIES



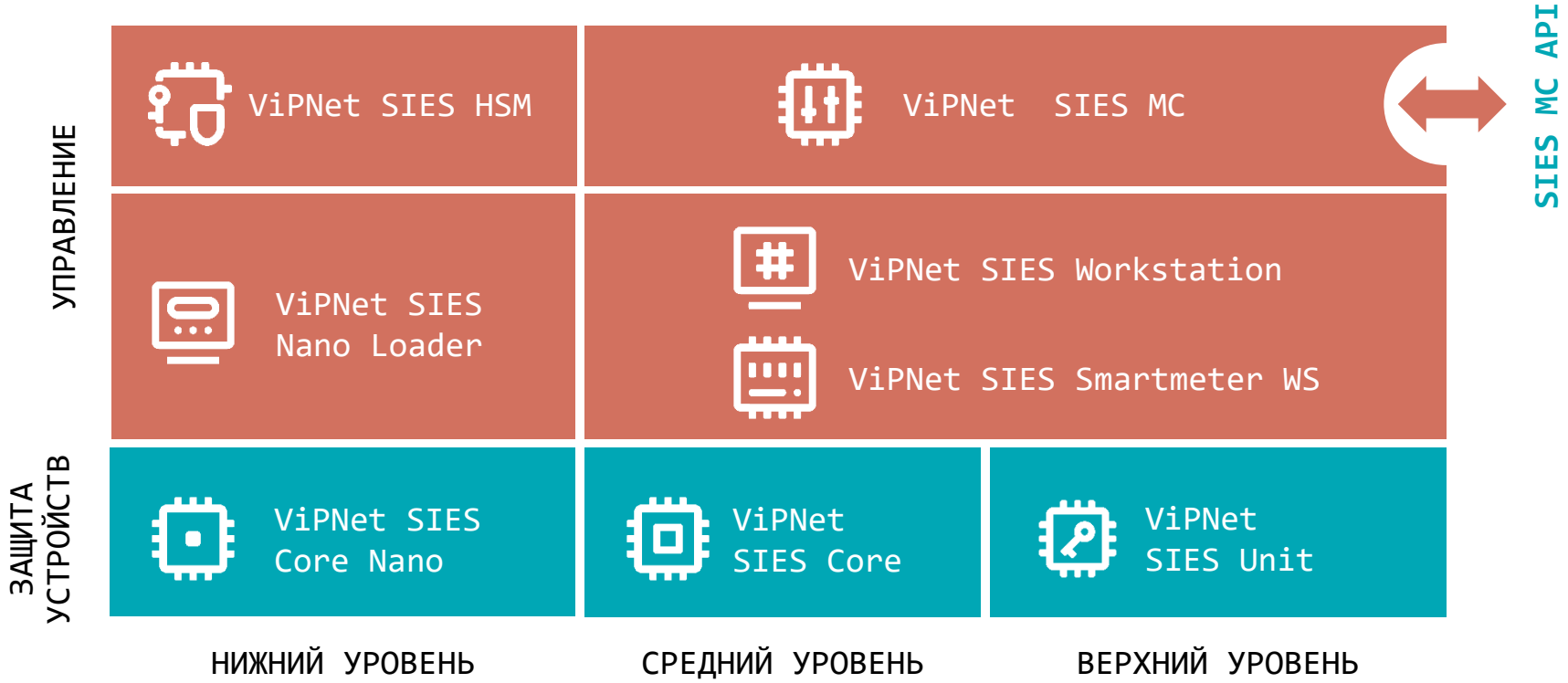
ТЕХНО infotecs 2023 ФЕСТ

Решение ViPNet SIES

Встраиваемые средства криптографической защиты информации:

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

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

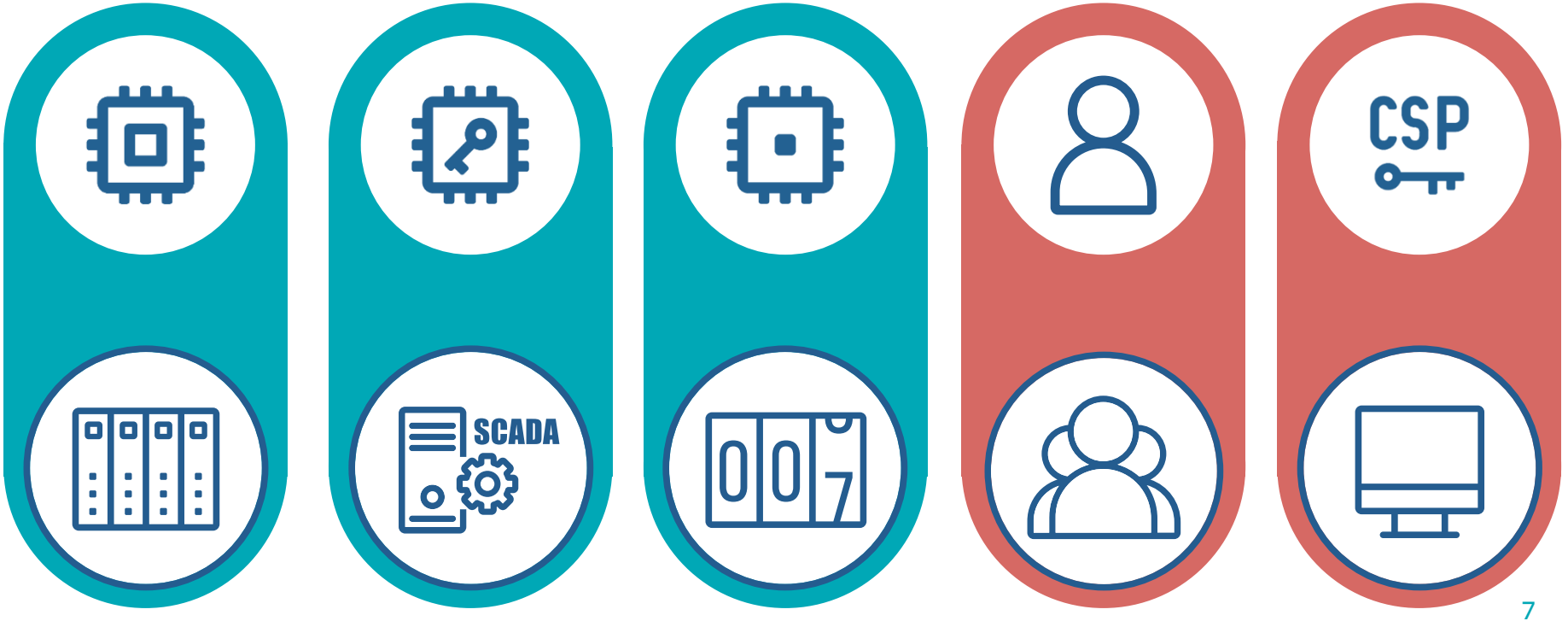
- Ключевой и Удостоверяющий центры
- Управление связями в системе
- Дистанционная смена ключевой информации
- Управление активами
- UI — Доступ к интерфейсу по WebUI
- API — API для подключения и управления сторонними СКЗИ
- Сертификат СКЗИ класса КС3 и КС1

SIES-узлы

СКЗИ, выполняющие прикладные криптографические операции с данными защищаемых устройств

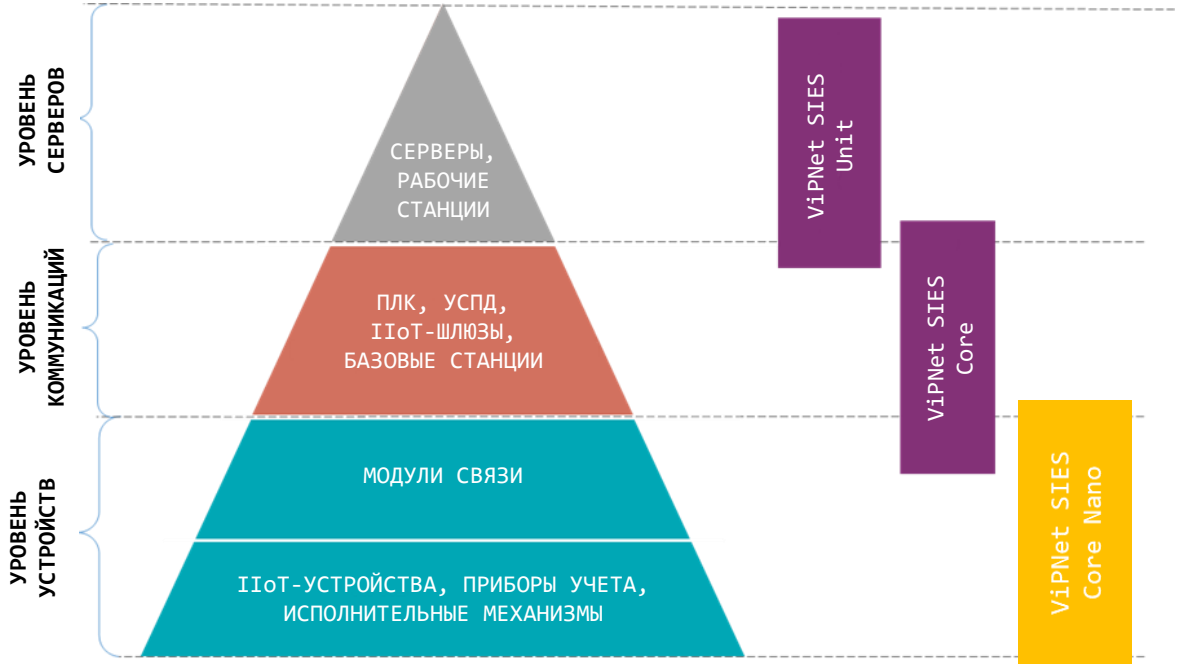
Защищаемые устройства

средства обработки информации, интегрированные с SIES-узлами

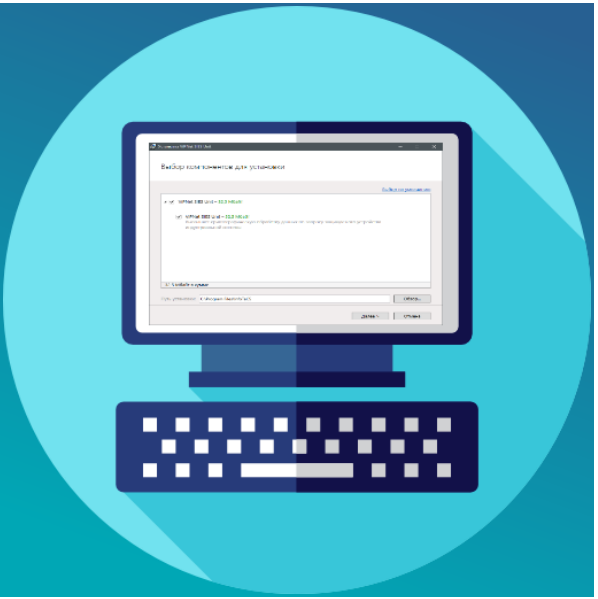


Защита данных от АСУ ТП до IIoT

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



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

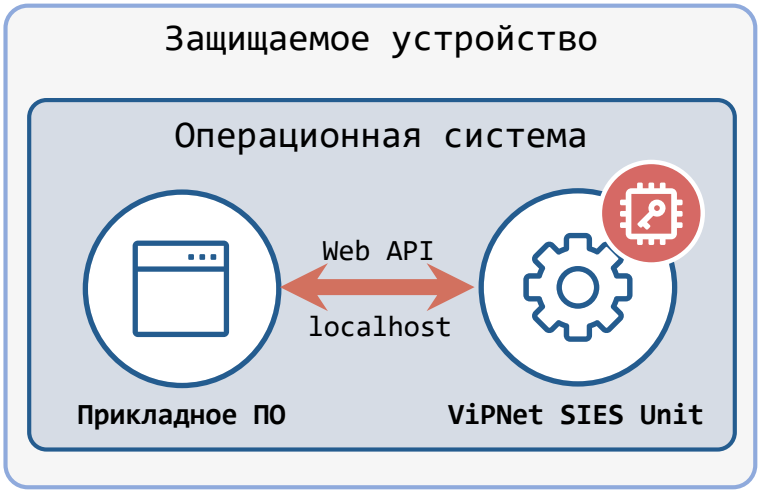
Функциональные особенности:

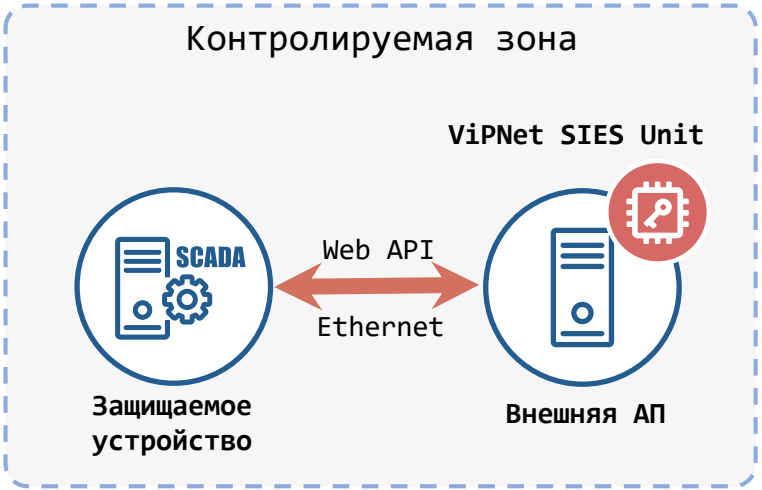
- Поддерживаемые архитектуры – x86-32, x86-64, ARM (armhf)
- Поддерживаемые ОС – Windows, Linux (Debian 9.8, 10 / Ubuntu 16, 18 / Astra Linux SE 1.6, 1.7 / Альт8СП)
- Установка на защищаемое устройство или выделенную платформу

Соответствие требованиям:

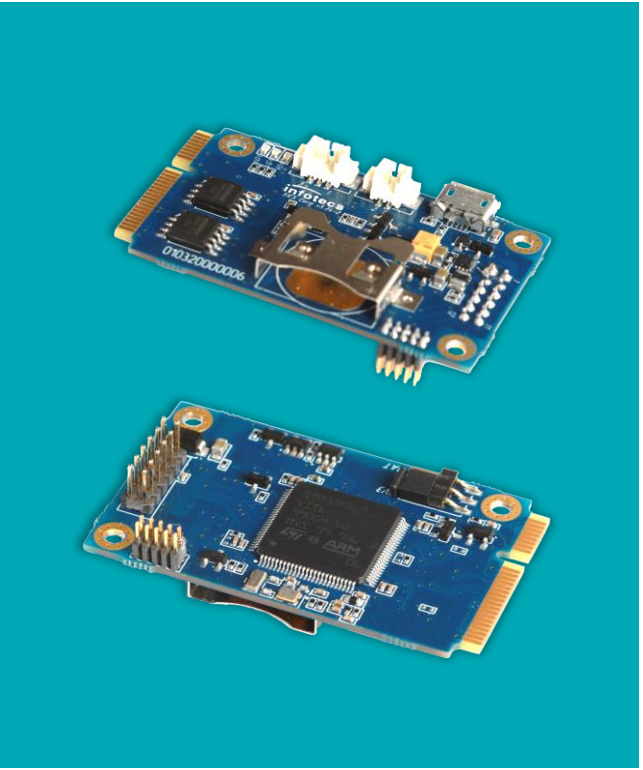
- СКЗИ класса КС1 и КС3

Интеграция ViPNet SIES Unit





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

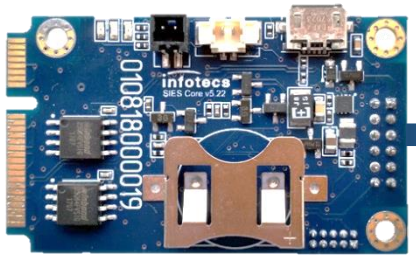
Функциональные особенности:

- 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^{0}C

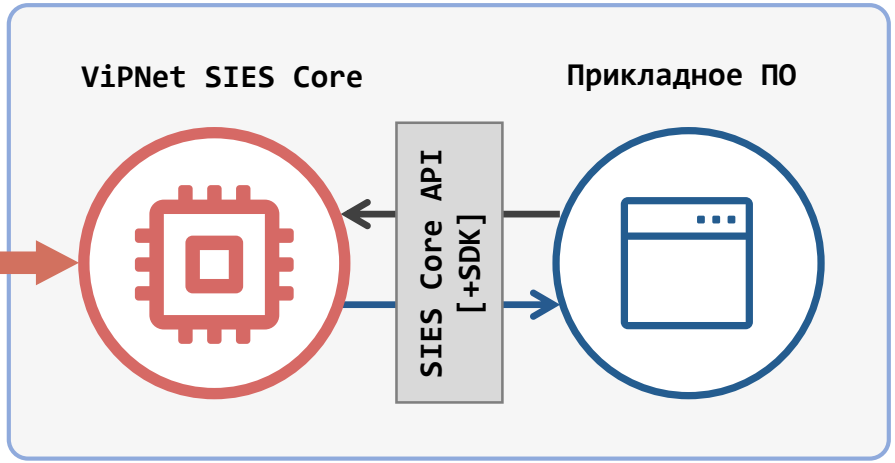
Соответствие требованиям:

- СКЗИ класса КС3

Интеграция ViPNet SIES Core



UART / USB / SPI



ViPNet SIES Core

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

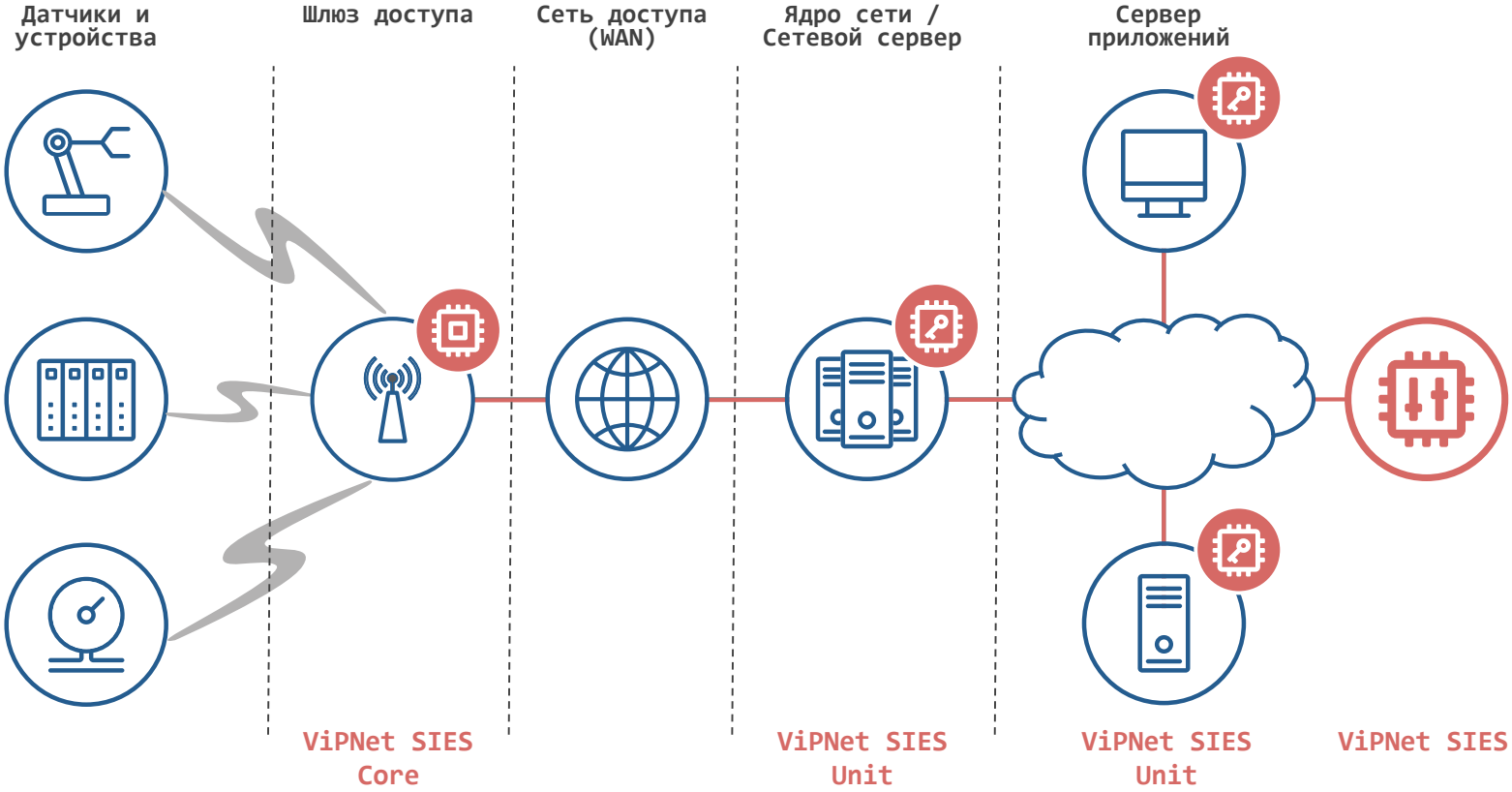
SIES Core SDK:

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

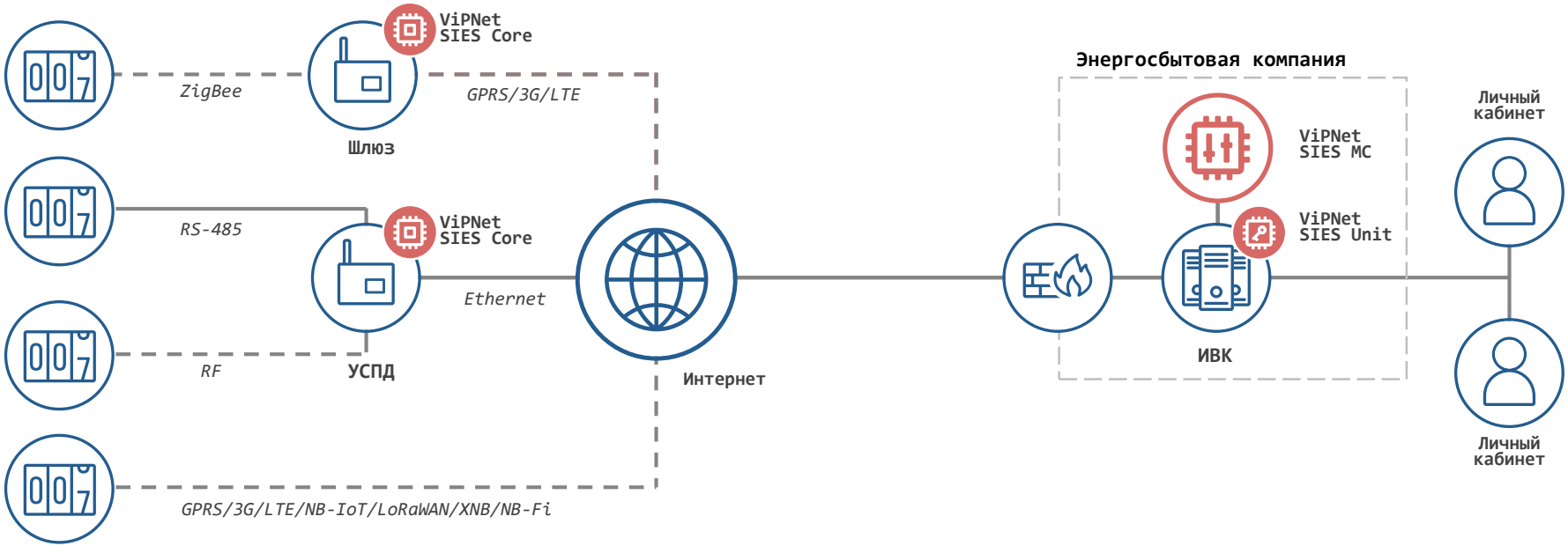
Данные

Защищенные данные

Защита данных в IIoT-системе



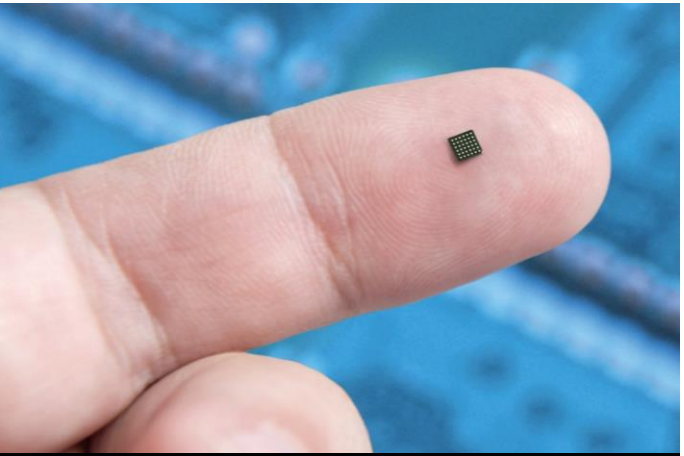
Защита данных в ИСУЭ



ТЕХНО 2023 infotecs ФЕСТ

ViPNet SIES Core Nano

ПАК ViPNet SIES Core Nano



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

Криптографический протокол CRISP:
- Зашифрование/расшифрование (CRISP)
- Вычисление/проверка имитовставки (CRISP)
- Вычисление/проверка хэш-кода

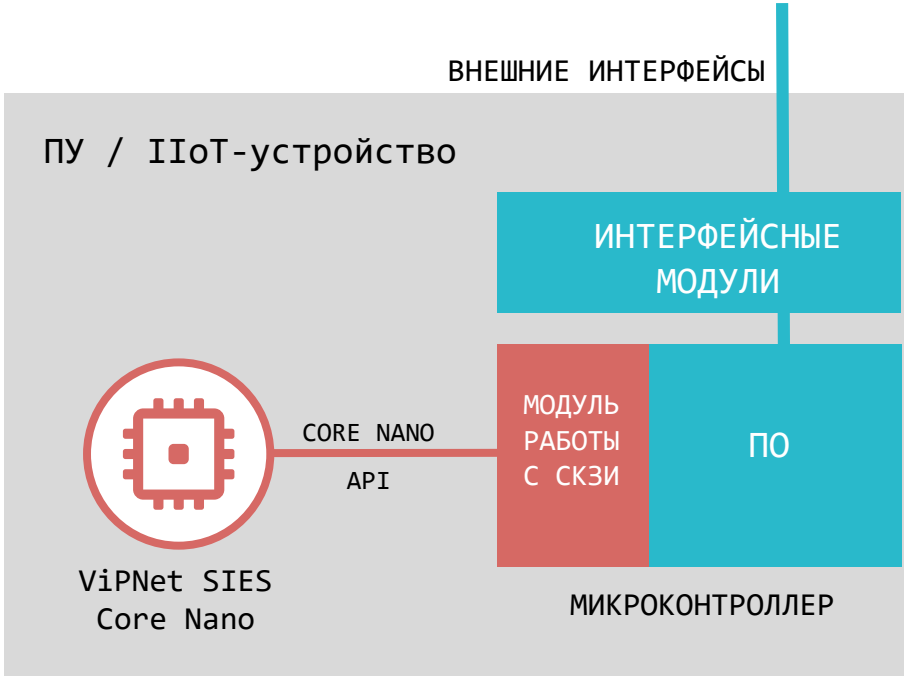
Функциональные особенности:
- 3 резервируемых ключа связи
- Хранение ключевой информации до 16 лет
- Рабочий диапазон температур -40…+85^{O}C
- Форм-фактор – микросхема BGA36 3x3x0,4 мм

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

Встраивание ViPNet SIES Core Nano в IIoT-устройства

Интеграция на аппаратном уровне – SPI

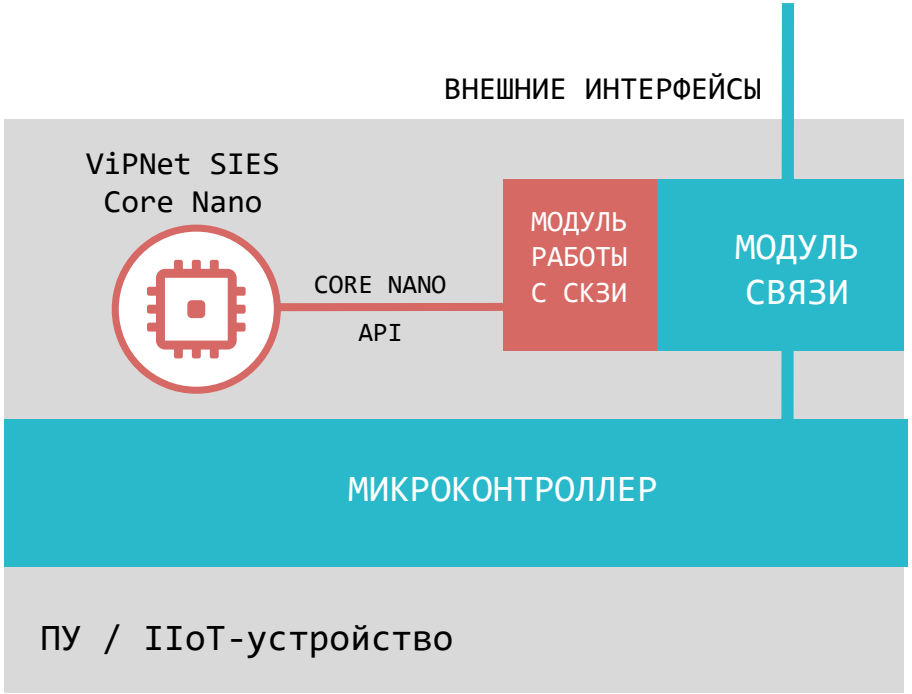
Интеграция на программном уровне – Core Nano API



Встраивание ViPNet SIES Core Nano в модули связи устройств

Интеграция на аппаратном уровне – SPI

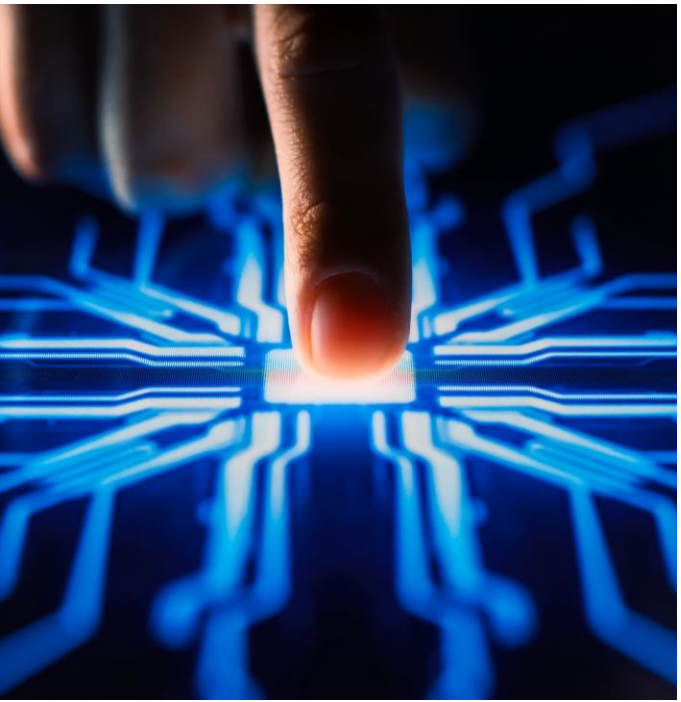
Интеграция на программном уровне – Core Nano API



Этапы встраивания СКЗИ

- Подготовка к встраиванию СКЗИ
- Встраивание СКЗИ в защищаемое устройство
- Проведение испытаний защищаемого устройства с встроенным СКЗИ
- Оценка влияния защищаемого устройства на СКЗИ
- Обеспечение требований и условий работы с СКЗИ
- Производство

Оценка влияния

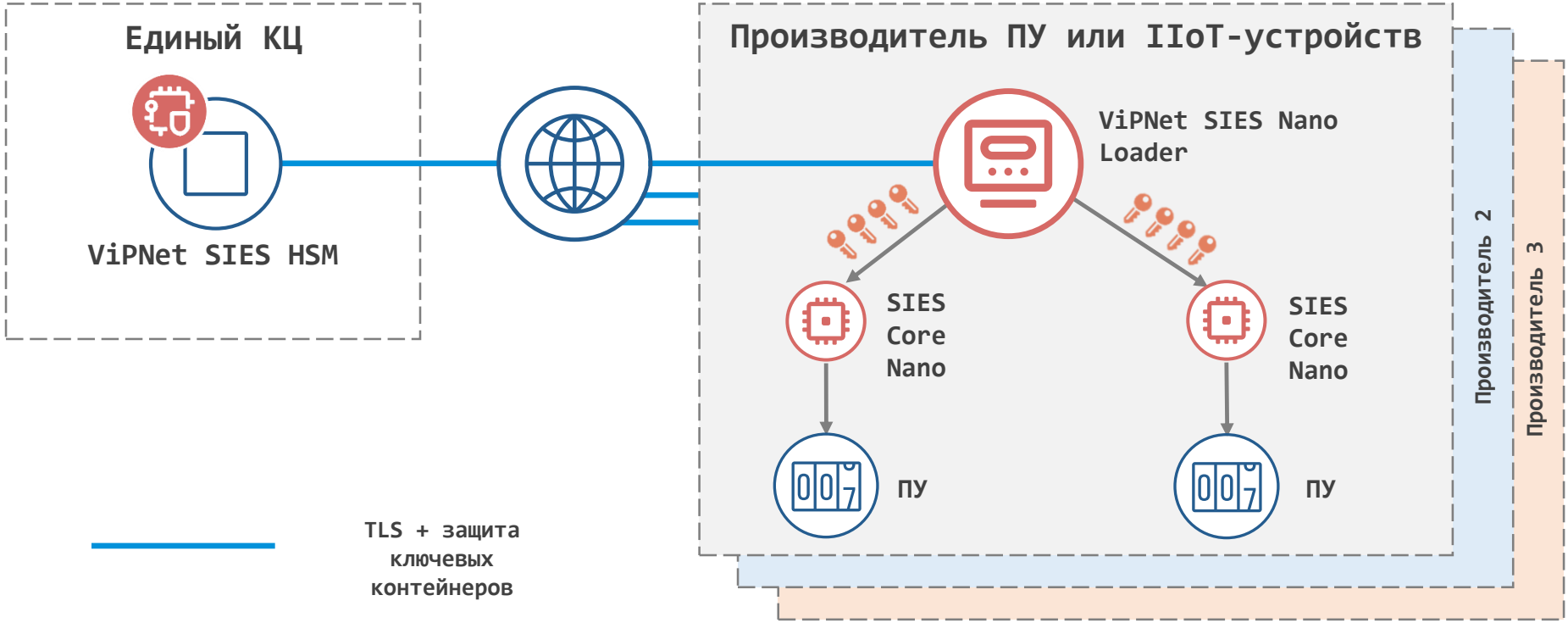


- Подготовка ТЗ на оценку влияния
- Согласование ТЗ на оценку влияния с испытательной лабораторией
- Согласование ТЗ на оценку влияния с ФСБ России
- Передача материалов и стенда в исследовательскую лабораторию для проведения работ по оценке влияния
- Направление исследовательской лабораторией результатов исследований на экспертизу в ФСБ России
- Получение результатов экспертизы в ФСБ России

ТЕХНО 2023 infotecs ФЕСТ

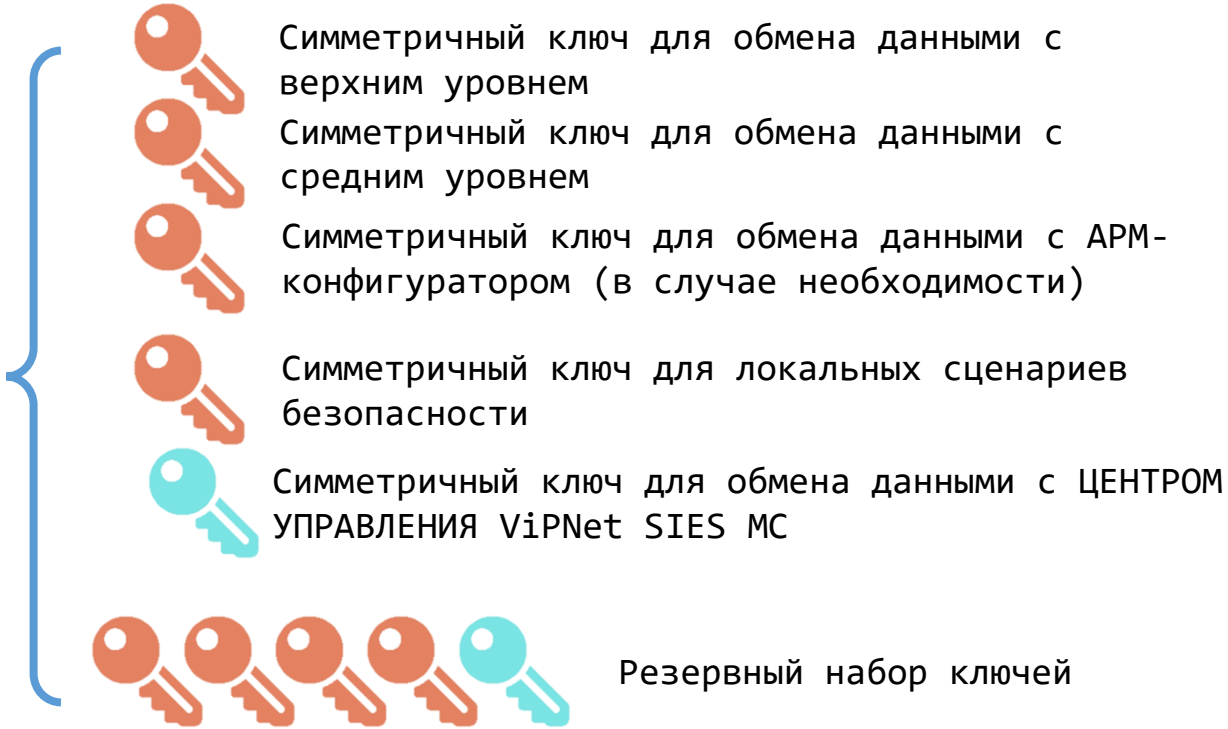
Применение ViPNet SIES Core Nano

Загрузка ключевой информации в ViPNet SIES Core Nano



Ключевая информация ViPNet SIES Core Nano

СРОК СЛУЖБЫ 16 ЛЕТ



- Симметричный ключ для обмена данными с верхним уровнем
- Симметричный ключ для обмена данными с средним уровнем
- Симметричный ключ для обмена данными с АРМ-конфигуратором (в случае необходимости)
- Симметричный ключ для локальных сценариев безопасности
- Симметричный ключ для обмена данными с ЦЕНТРОМ УПРАВЛЕНИЯ ViPNet SIES MC
- Резервный набор ключей

Защита данных с помощью протокола CRISP

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

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

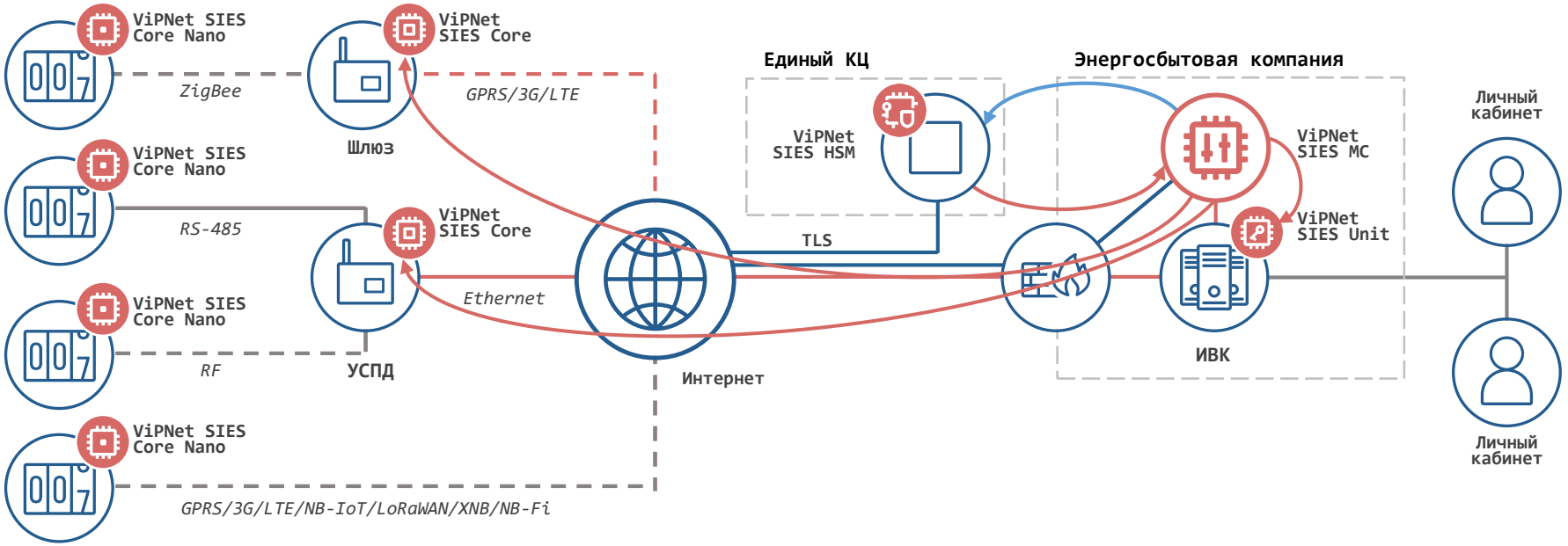
Защита адресных и групповых сообщений

Бессесионный криптографический протокол

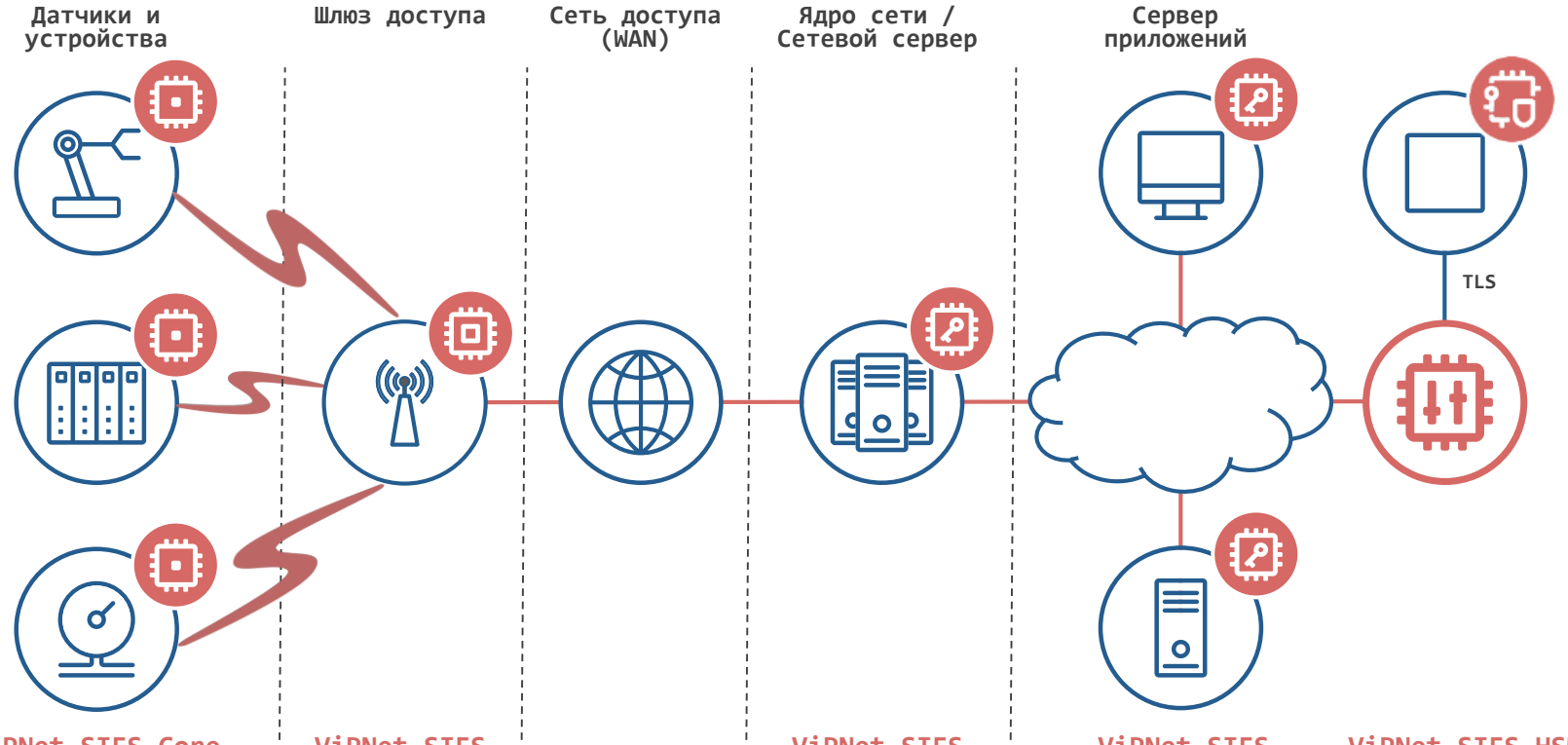
Минимальные накладные расходы (overhead)и минимальная нагрузка на сеть

Универсальный стандартизированный протокол защиты любых протоколов ИСУЭ

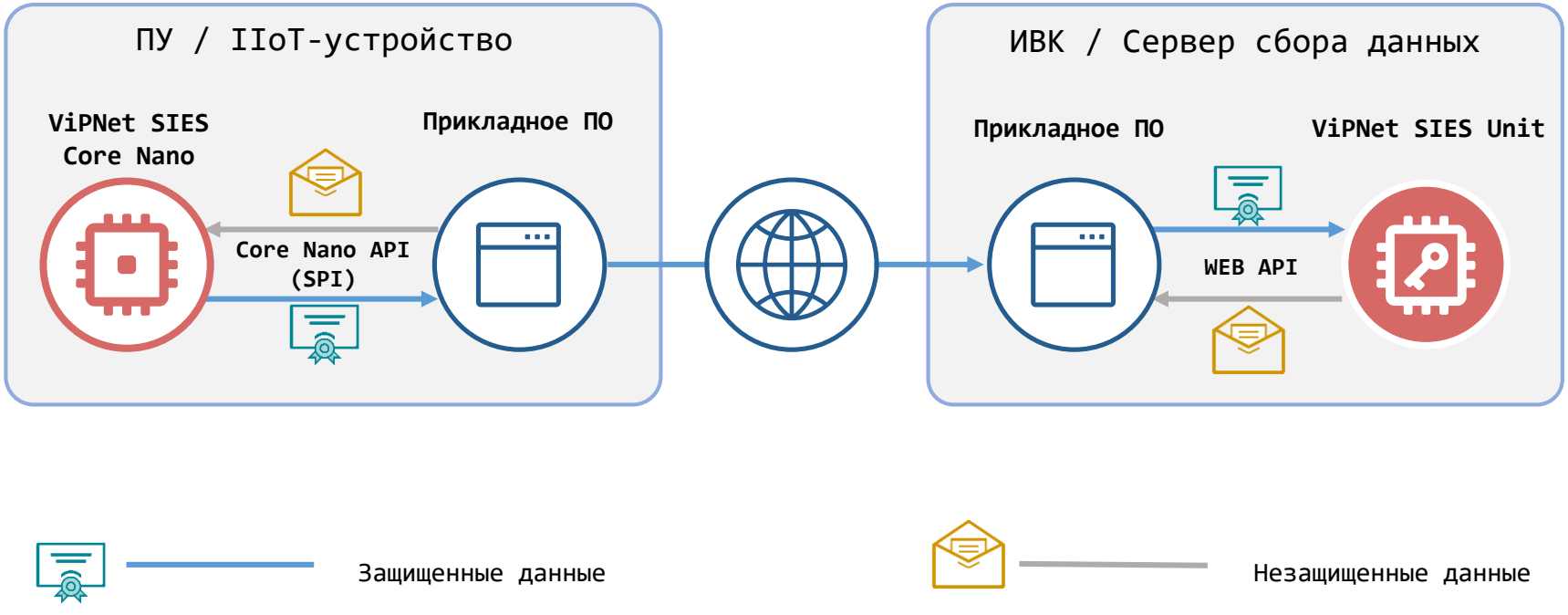
Защита данных в ИСУЭ до уровня ПУ



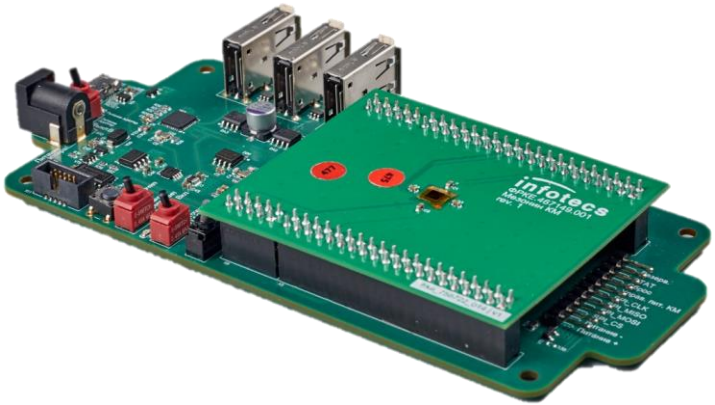
Защита данных в IIoT-системе



Защита коммуникаций с помощью ViPNet SIES



Комплект разработчика ViPNet SIES Core Nano DevKit



Предназначен для разработчиков защищаемых устройств, ведущих работы по встраиванию ViPNet SIES Core Nano

Состоит из:

- модуля SIES Core Nano Adapter;
- мезонинной платы с распаянным SIES Core Nano

Комплект разработчика позволяет:

- ознакомиться с возможностями продукта ViPNet SIES Core Nano;
- разработать и отладить ПО защищаемого устройства для взаимодействия с ViPNet SIES Core Nano;
- реализовать сценарии защиты информации защищаемого устройства;
- подготовить стенд для проверки реализованных сценариев защиты информации;
- разработать конструкторскую, доработать пользовательскую и эксплуатационную документацию с учётом использования СКЗИ

ТЕХНО 2023 infotecs ФЕСТ

Спасибо за внимание!

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363