

Комплект разработчика ViPNet SIES Core Nano в теории и на практике

Алексей Власенко
ведущий менеджер продуктов

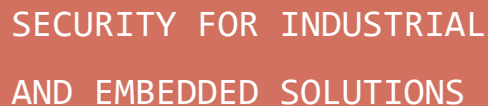
The logo for infotecs, featuring a stylized orange and red arc above the word "infotecs" in a bold, blue, sans-serif font.



Решение ViPNet SIES

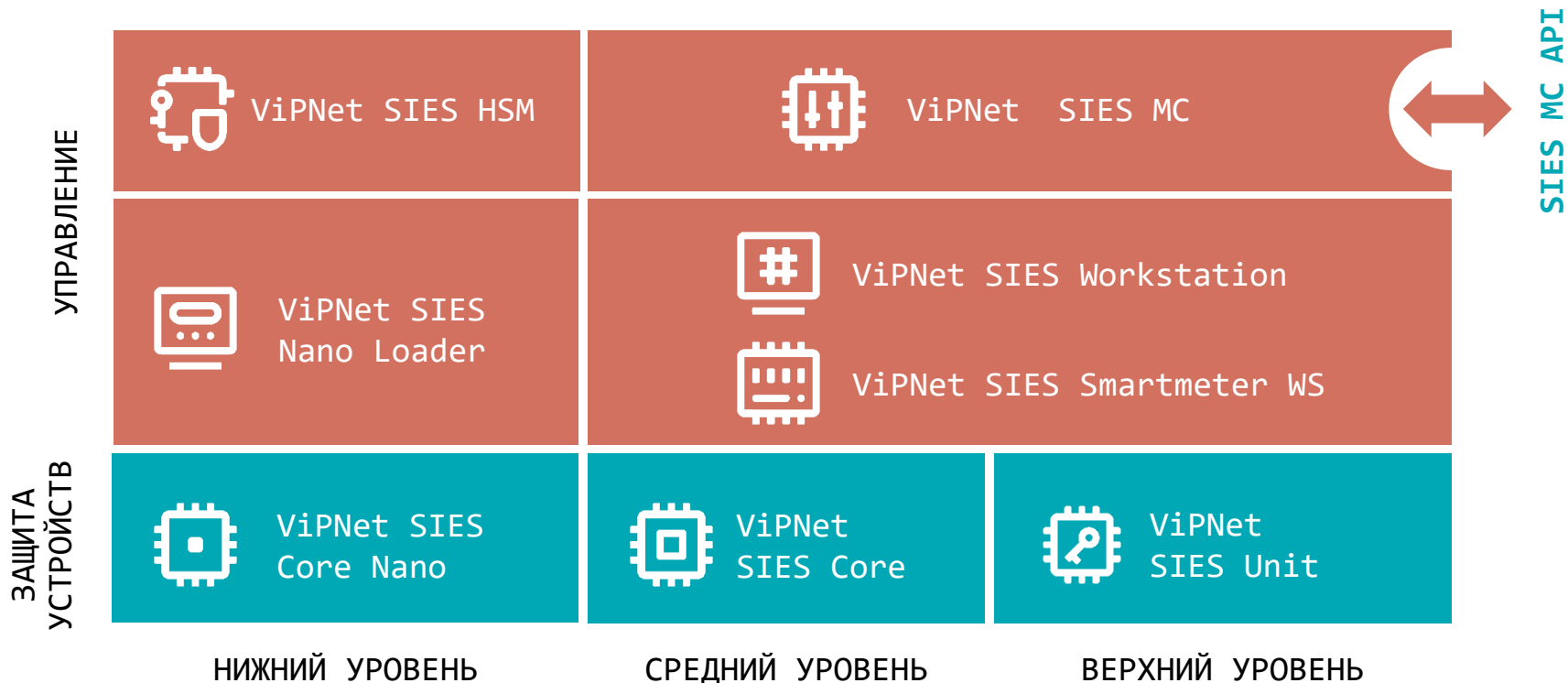
Встраиваемые криптографические средства защиты информации:

- для устройств автоматизации на всех уровнях АСУ
- для М2М-устройств
- для IIoT-устройств
- для ИСУЭ

A red rectangular box containing the text "SECURITY FOR INDUSTRIAL AND EMBEDDED SOLUTIONS" in white, uppercase, sans-serif font. The background of the slide is a low-angle photograph of a high-voltage power transmission tower against a bright, hazy sky with some clouds.

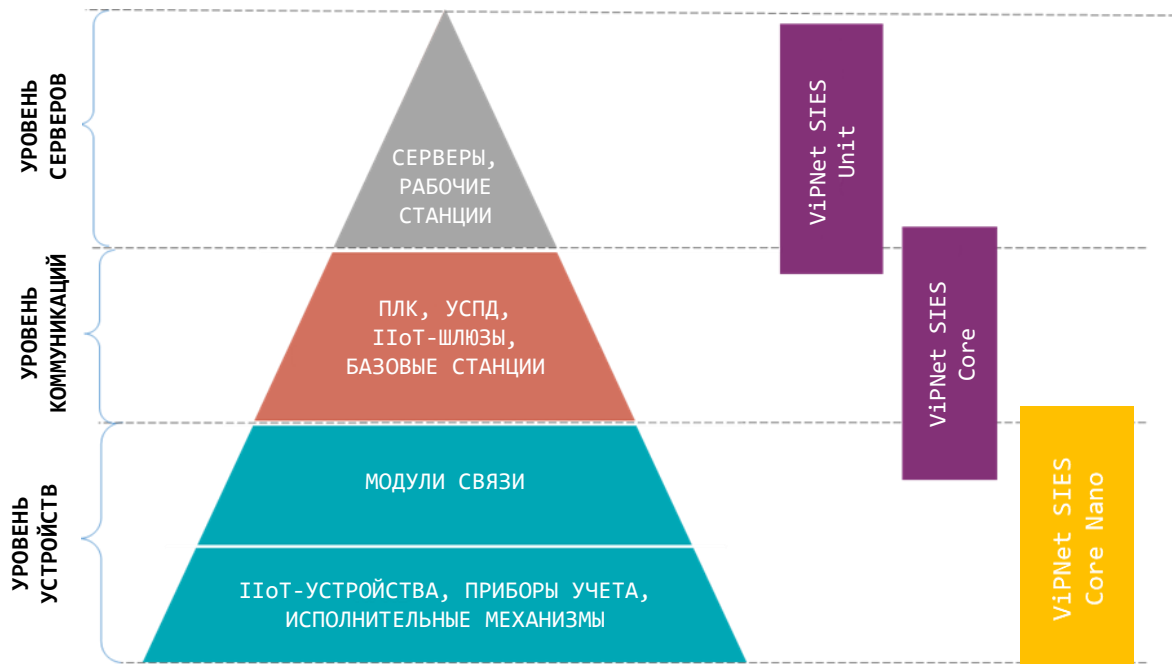
SECURITY FOR INDUSTRIAL
AND EMBEDDED SOLUTIONS

Состав решения ViPNet SIES



Защита данных от АСУ ТП до IIoT

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



Центр управления ViPNet SIES MC



- ПАК ViPNet SIES MC 10000
 - До 1 млн. устройств
 - СКЗИ класса КСЗ
- ПАК ViPNet SIES MC 3000
 - До 3000 устройств
 - СКЗИ класса КСЗ
- ПАК ViPNet SIES MC IoT
 - До 2 млн. устройств
 - СКЗИ класса КСЗ
- 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



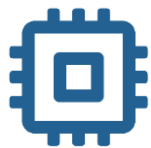
Сертификат СКЗИ класса КСЗ и КС1

SIES-узлы

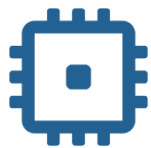
СКЗИ, выполняющие прикладные криптографические операции с данными защищаемых устройств



ПО
ViPNet
SIES Unit



ПАК
ViPNet
SIES Core



ПАК
ViPNet
SIES Core
Nano



СКЗИ
Пользова-
теля АСУ

Токены/смарт-карты
сервисного инженера,
инженера КИП и др.

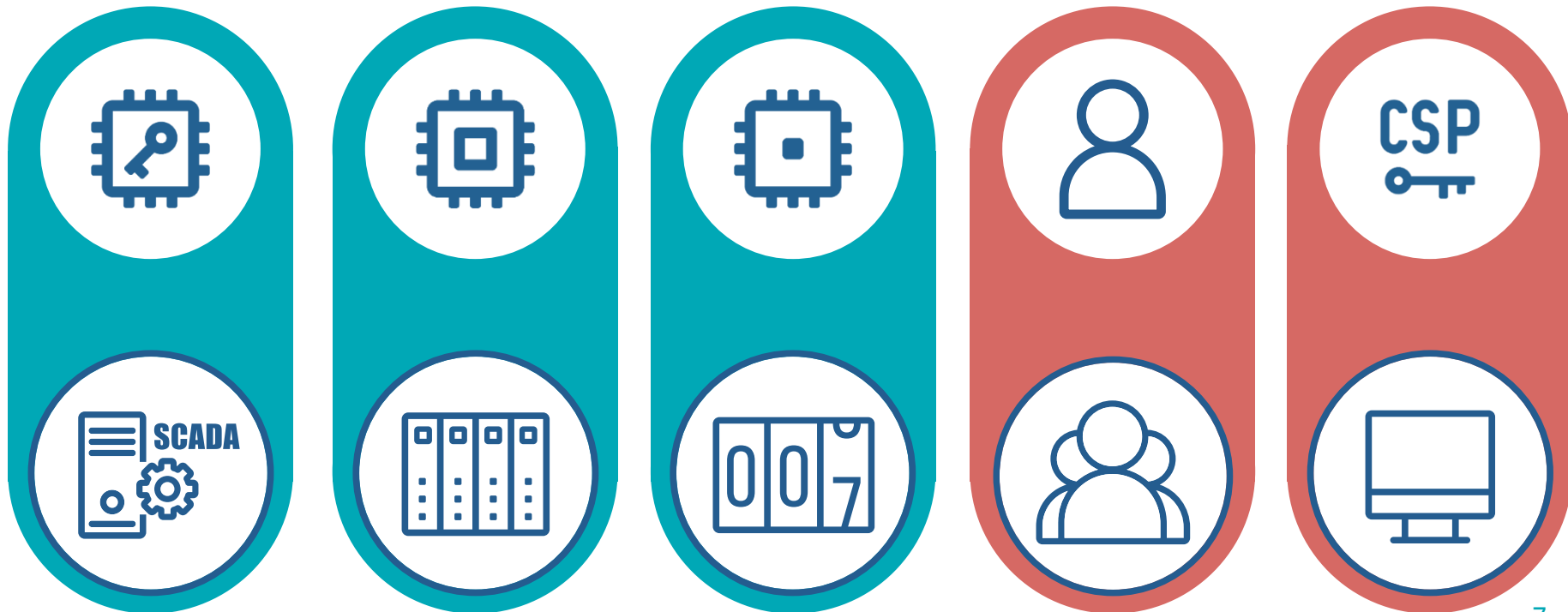


Другой
SIES-узел

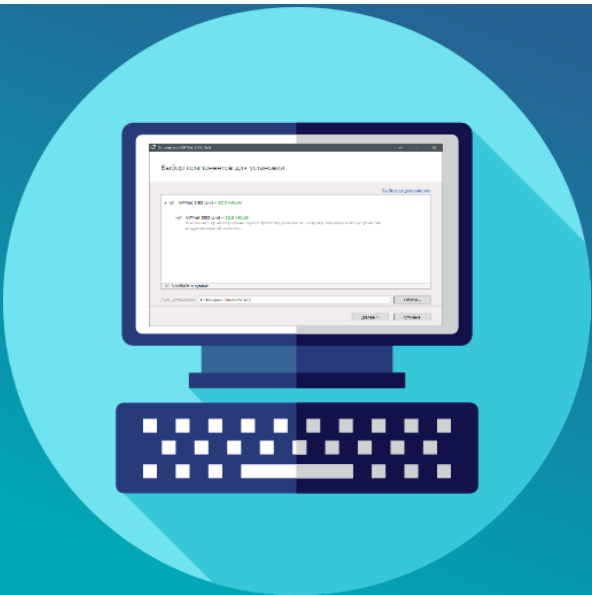
Криптопровайдеры,
прочие PKI-продукты,
библиотеки,
сторонние СКЗИ с
реализацией CRISP

Защищаемые устройства

средства обработки информации, интегрированные с SIES-узлами



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

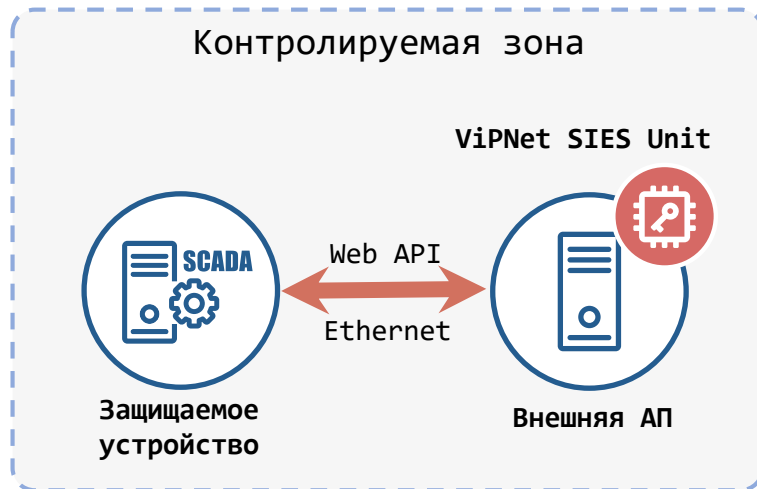
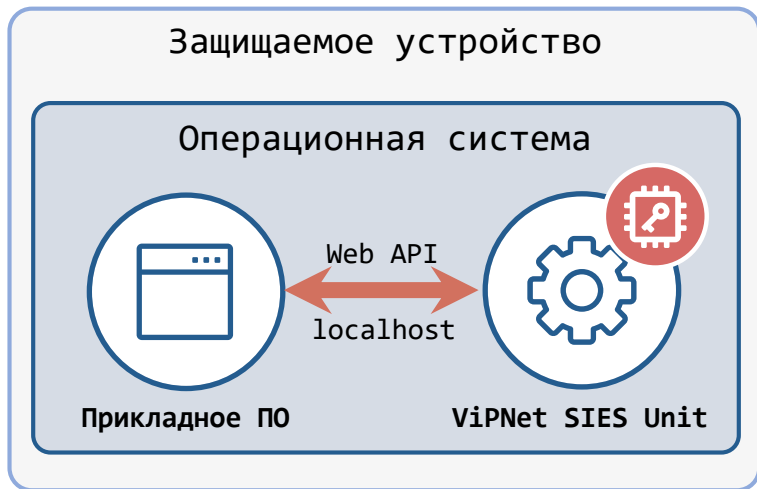
Функциональные особенности:

- 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

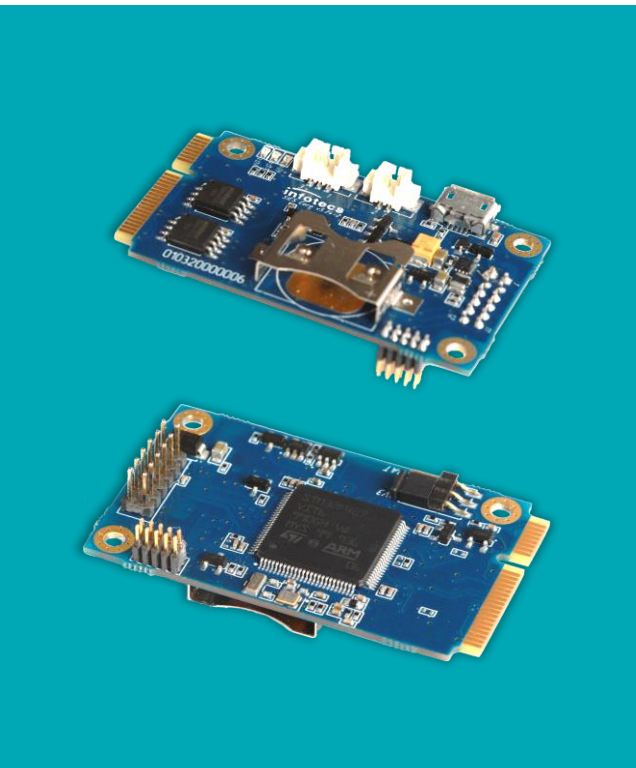
Соответствие требованиям:

- 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

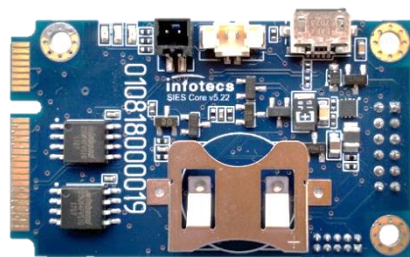
Функциональные особенности:

- 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°C

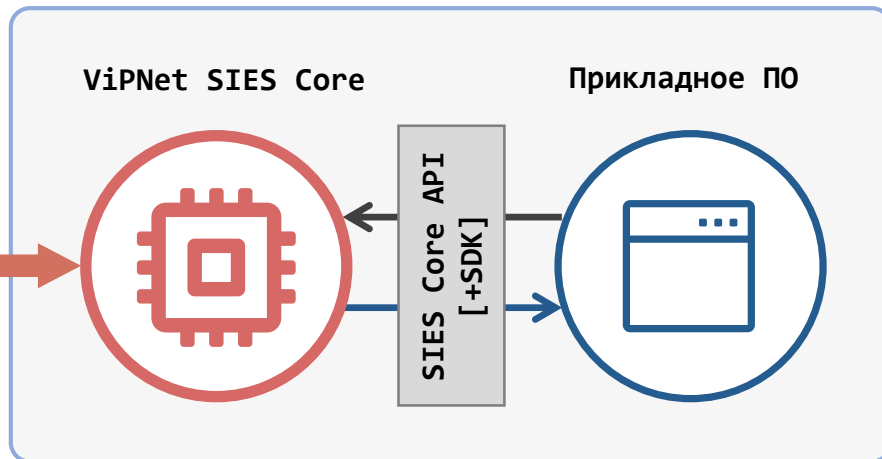
Соответствие требованиям:

- СКЗИ класса КСЗ

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)

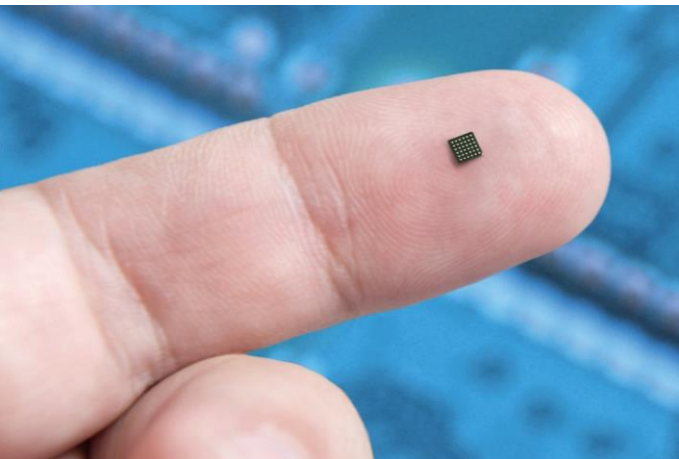


Данные



Защищенные данные

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 $-40...+85^{\circ}\text{C}$
- Форм-фактор – микросхема BGA36 $3\times 3\times 0,4$ мм

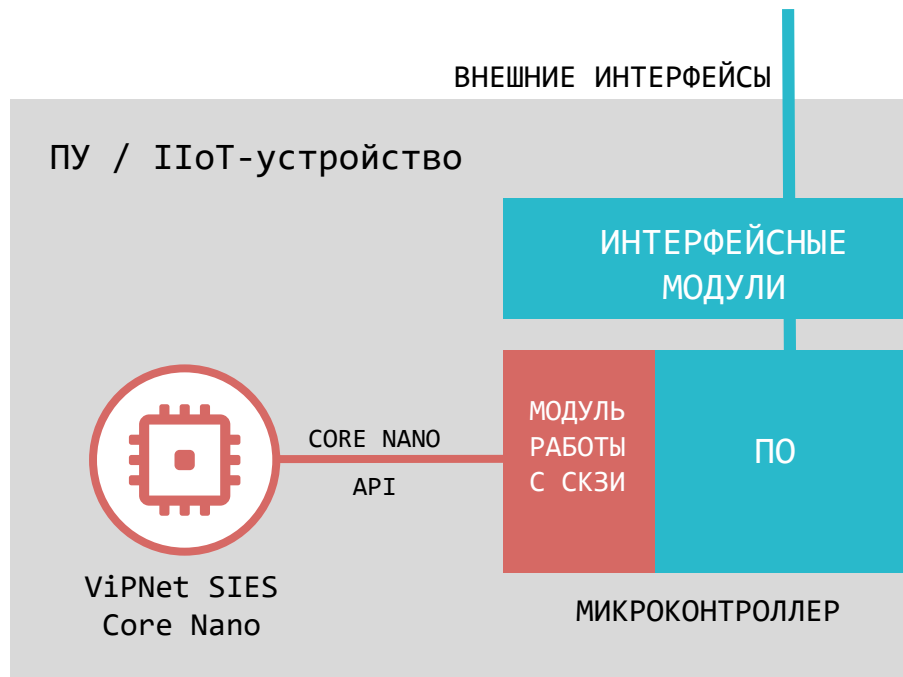
Соответствие требованиям:

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

Встраивание ViPNet SIES Core Nano в IIoT-устройства

Интеграция на
аппаратном уровне – SPI

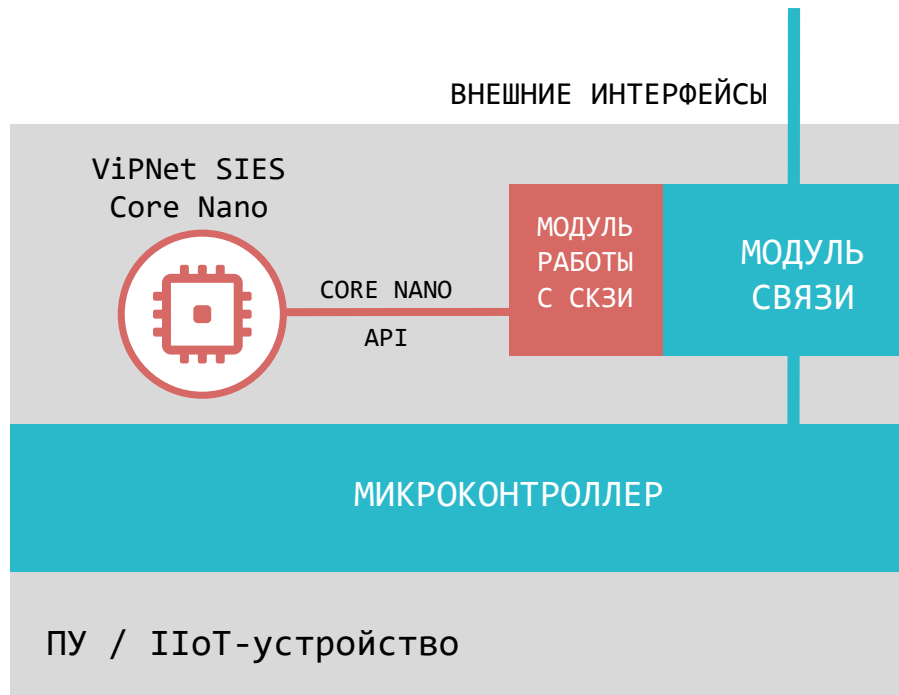
Интеграция на
программном уровне –
Core Nano API



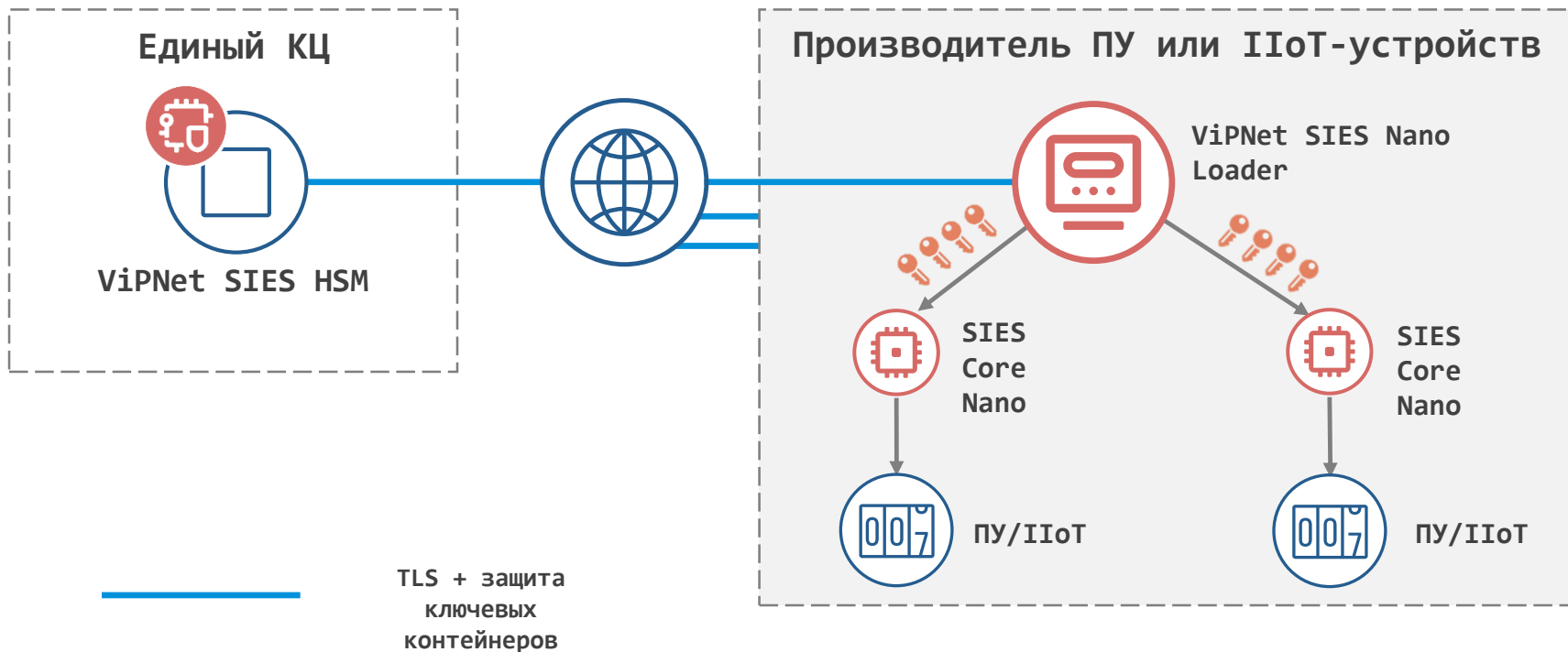
Встраивание ViPNet SIES Core Nano в модули связи устройств

Интеграция на
аппаратном уровне – SPI

Интеграция на
программном уровне –
Core Nano API



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

● 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®

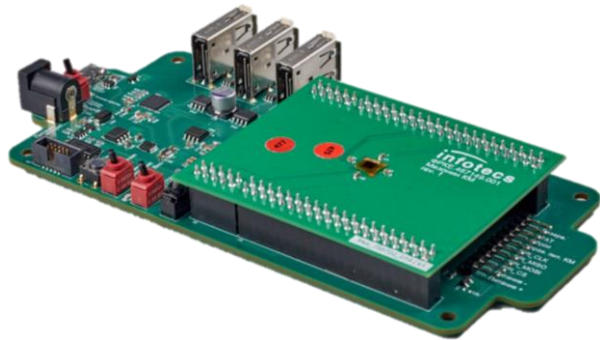


RF



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

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



* В ViPNet SIES Core Nano, установленный в комплекте разработчика, уже загружена вся ключевая информация из ViPNet SIES HSM ИнфоТекС

ViPNet SIES Development kit

варианты исполнения

Исполнение 1	Исполнение 2	Исполнение 3	Исполнение 4
ViPNet SIES Core (2 модуля)	ViPNet PKI Client с TLS Unit	ViPNet SIES Core (2 модуля)	ViPNet PKI Client с TLS Unit
ViPNet SIES Core SDK	ViPNet SIES Unit	ViPNet SIES Core SDK	ViPNet SIES Unit
ViPNet SIES Workstation	ViPNet SIES MC VA	ViPNet SIES Workstation	Подключение к ViPNet SIES MC ИнфоТеКс
ViPNet SIES Unit		ViPNet SIES Unit	
ViPNet PKI Client с TLS Unit		ViPNet PKI Client с TLS Unit	
ViPNet SIES MC VA		Подключение к ViPNet SIES MC ИнфоТеКс	<i>* Может быть предоставлен при заказе комплекта разработчика ViPNet SIES Core Nano</i>

Паспорт, комплект пользовательской и эксплуатационной документации

Разработка сквозных сценариев с помощью КР ViPNet SIES Core Nano

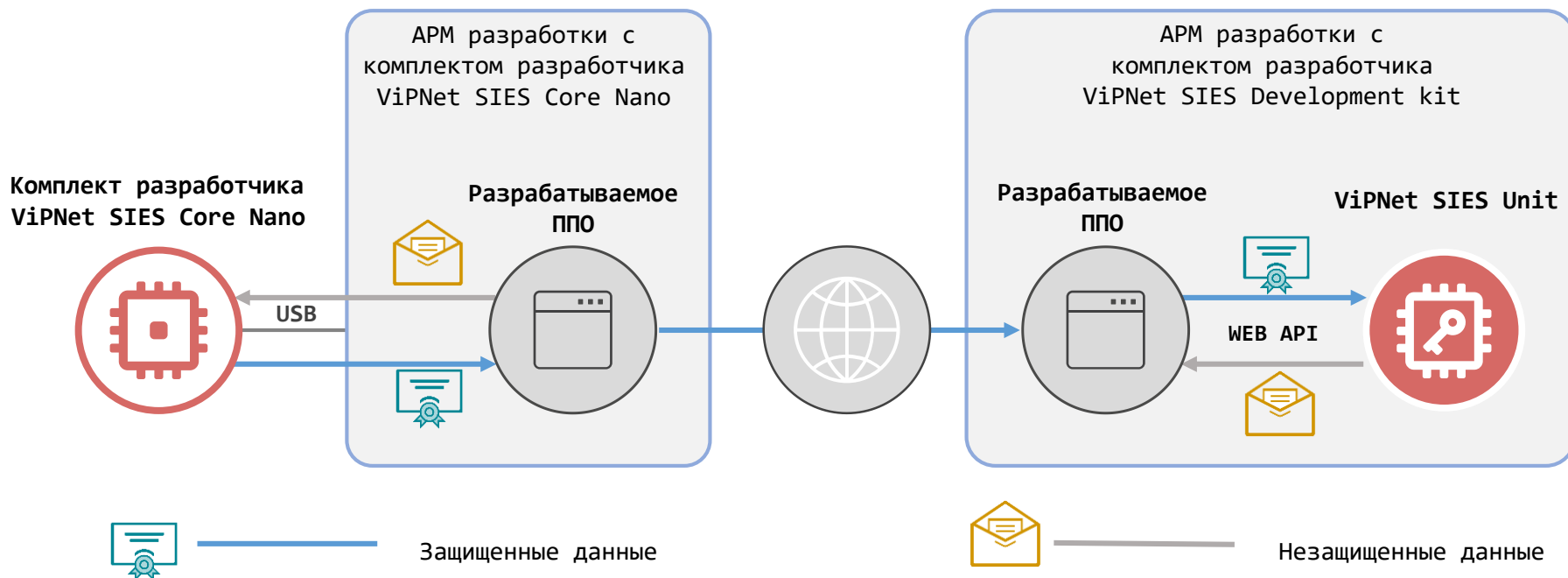
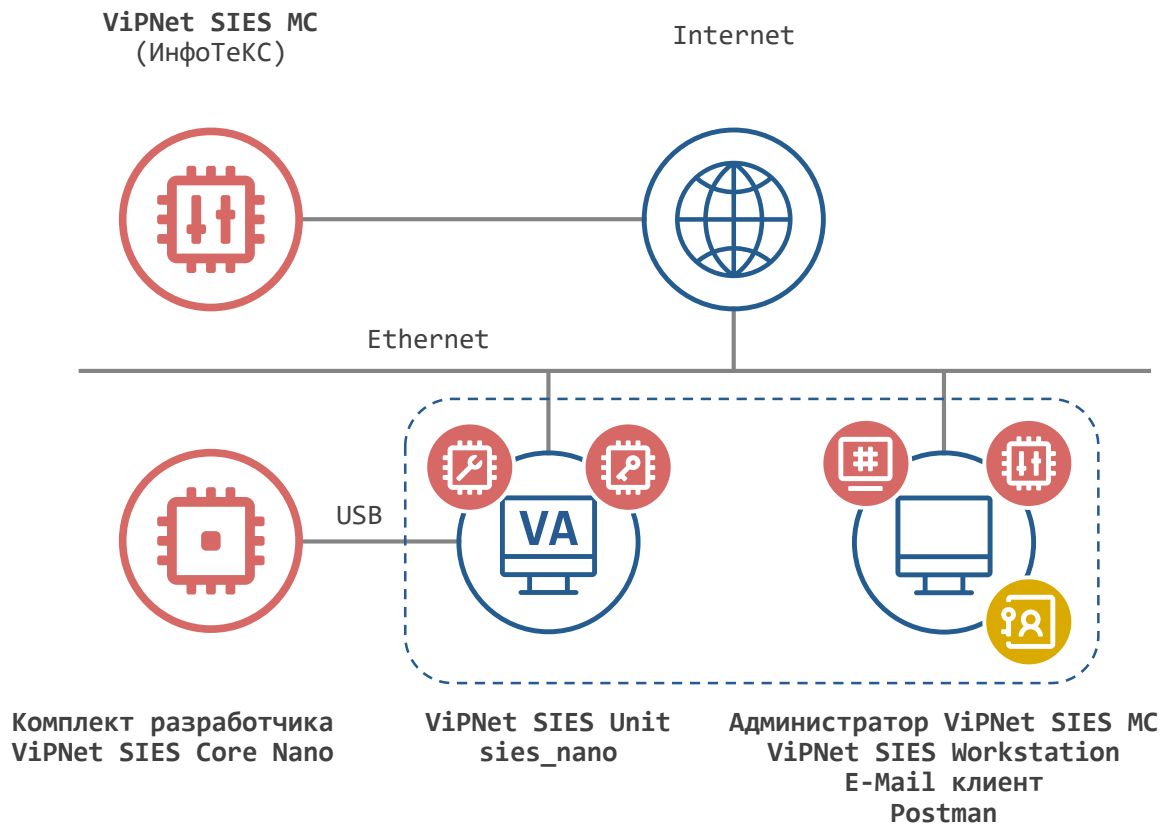


Схема взаимодействия





infotecs

Спасибо
за внимание!

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363