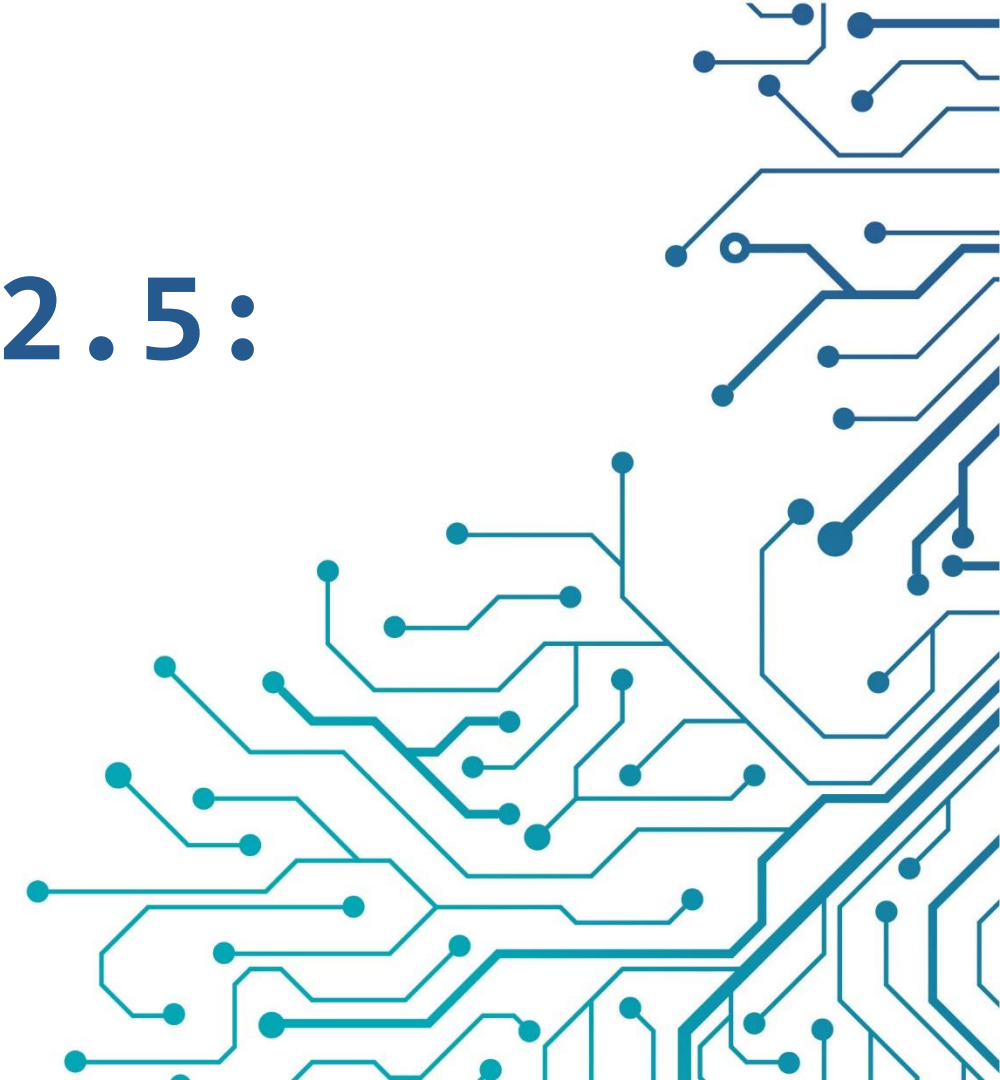
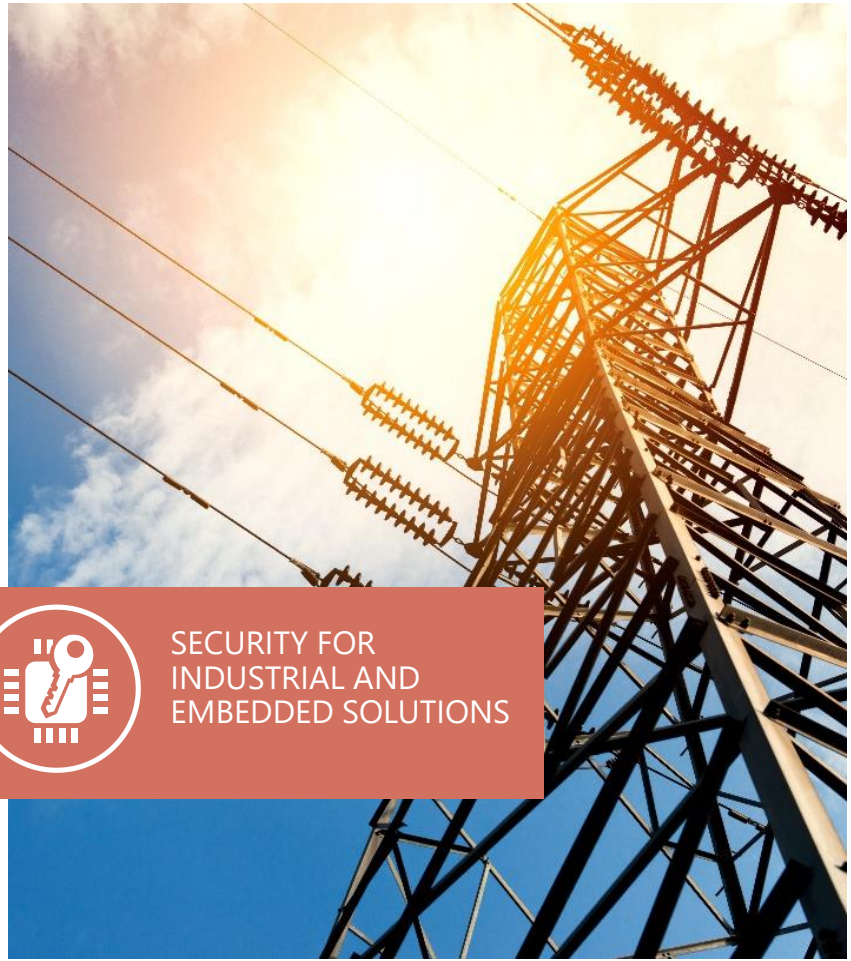
ViPNet SIES 2.5: что нового?

Марина Сорокина

infotecs





Решение ViPNet SIES

Встраиваемые криптографические средства защиты информации:

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

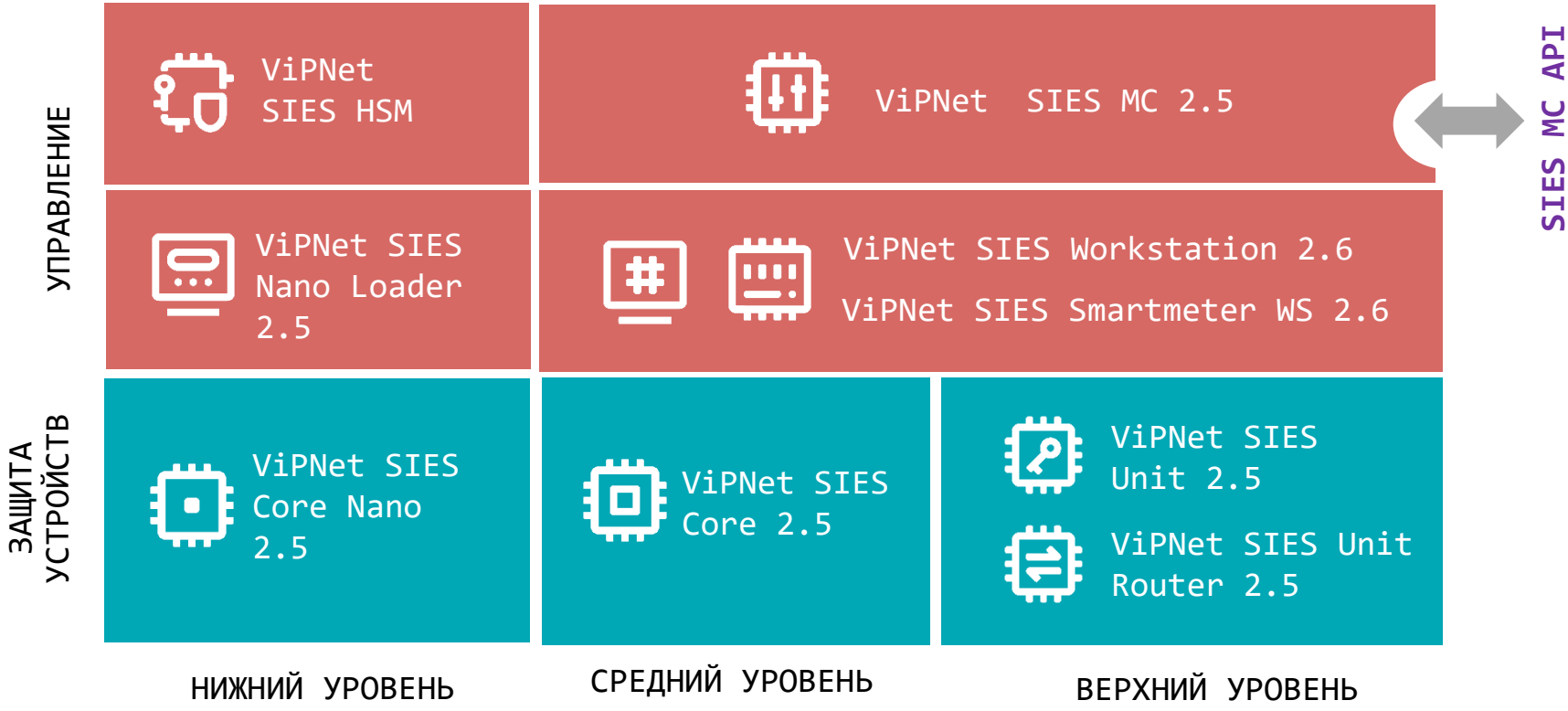
План вебинара

- Состав: продукты решения ViPNet SIES
- Сертификация
- Крипточип ViPNet SIES Core Nano и новые продукты ViPNet SIES, обеспечивающие его функционирование
- Криптомодуль ViPNet SIES Core 2.5
- ViPNet SIES Unit 2.5 & ViPNet SIES Unit Router 2.5
- ViPNet SIES MC 2.5
- ViPNet SIES Workstation & ViPNet SIES Smartmeter WS

Сертификация продуктов решения ViPNet SIES 2.4 завершена

Продукт	ViPNet SIES Core 2.4	ViPNet SIES MC 2.4				ViPNet SIES Unit 2.4			
Исполнение	На АП Core I2 и АП Core I4	SIES MC10000 Q1	SIES MC IoT Q1	SIES MC3000 Q1	SIES MC VA	Windows		Linux	
Форм-фактор	ПАК	ПАК	ПАК	ПАК	Virtual appliance	ПО			
Класс СКЗИ	СКЗИ КС3	СКЗИ КС3	СКЗИ КС3	СКЗИ КС3	СКЗИ КС1	СКЗИ КС1	СКЗИ КС3	СКЗИ КС1	СКЗИ КС3

Продукты ViPNet SIES 2.5

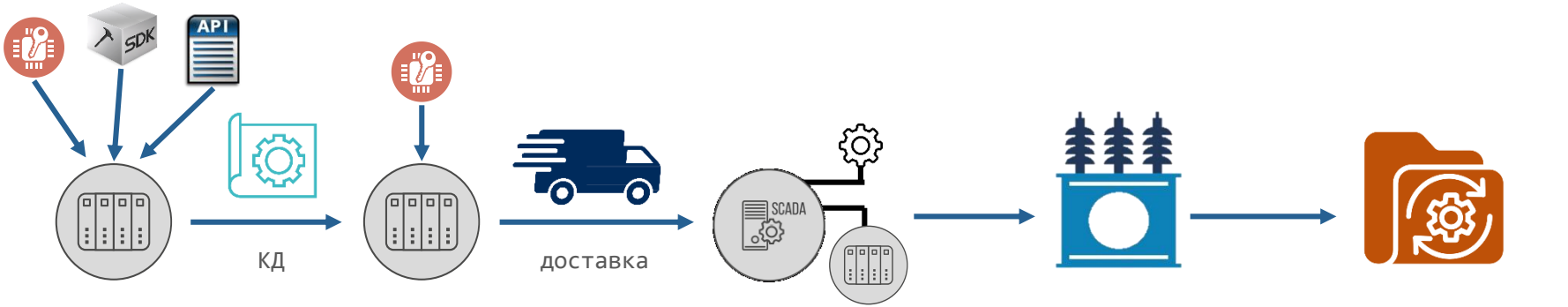


Продукты ViPNet SIES 2.5

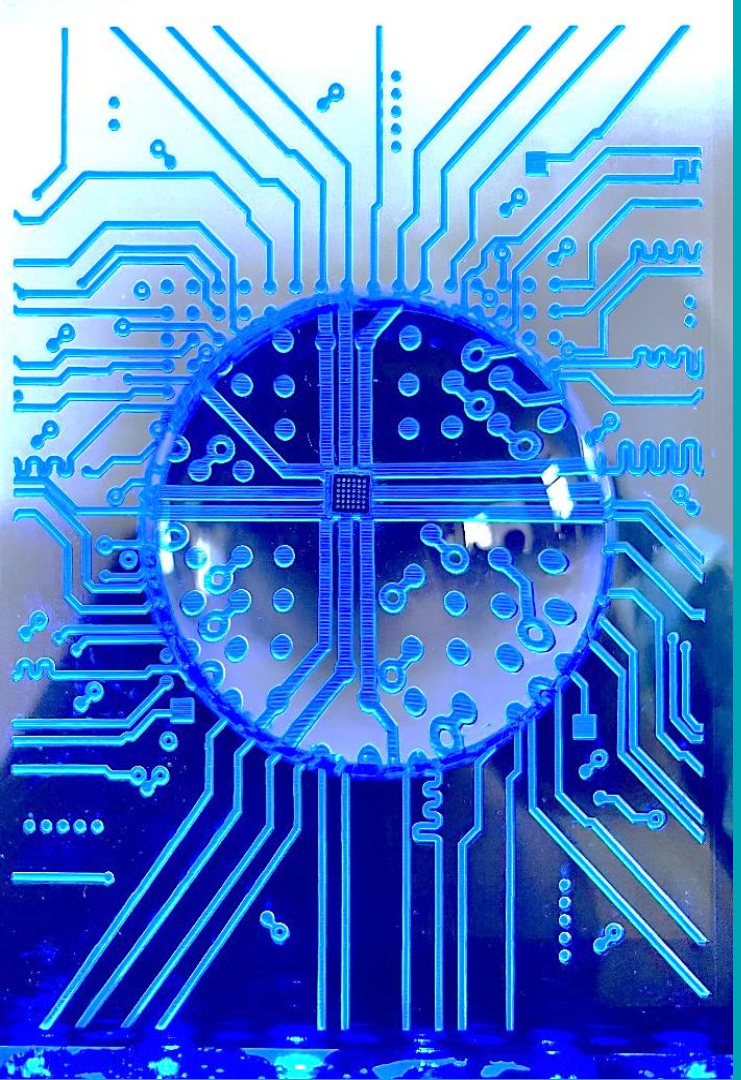
ViPNet SIES – комплекс продуктов для криптографической защиты информации компонентов АСУ ТП и IIoT-устройств:

- ПАК ViPNet SIES Core Nano – СКЗИ для встраивания в датчики, IIoT-устройства, приборы учета
- ПАК ViPNet SIES Core - СКЗИ для встраивания в концентраторы данных, IIoT-шлюзы, ПЛК, УСПД
- ПК ViPNet SIES Unit - СКЗИ для интеграции с серверами и рабочими станциями
- ПК ViPNet SIES Unit Router – маршрутизатор для организации масштабирования ViPNet SIES Unit
- ПАК ViPNet SIES MC – центр управления, удостоверяющий и ключевой центры СКЗИ ViPNet SIES и компонентов АСУ ТП и IIoT-устройств, в которые встроены СКЗИ
- Комплект ViPNet SIES HSM – ключевой центр долговременных ключей для ViPNet SIES Core Nano
- ПАК ViPNet SIES Nano Loader – СКЗИ для подготовки в ViPNet SIES Core Nano и загрузки в него ключевой информации
- ПК ViPNet SIES Workstation – ПО для инициализации ViPNet SIES Core и ViPNet SIES Unit
- ПК ViPNet SIES Smartmeter WS – ПО для инициализации и автоматизированного ввода в эксплуатацию ViPNet SIES Core
- SIES MC API – API для интеграции сторонних СКЗИ в решение ViPNet SIES

Встраивание СКЗИ в концепции Security by Design



Новые продукты ViPNet SIES: крипточип ViPNet SIES Core Nano, ViPNet SIES Nano Loader, ViPNet SIES HSM



ПАК ViPNet SIES Core Nano – СКЗИ для интеграции в приборы учета, IIoT-устройства, датчики

ФОРМ-ФАКТОР:

- Форм-фактор – микросхема 3x3x0,4 мм
- Корпус – BGA36
- Расстояние между выводами – 0,4 мм
- Рабочий диапазон температур -40…+85 ^{0}C
- Напряжение питания – 3,3В
- Ток потребления – 8мА
- Срок службы – 16 лет

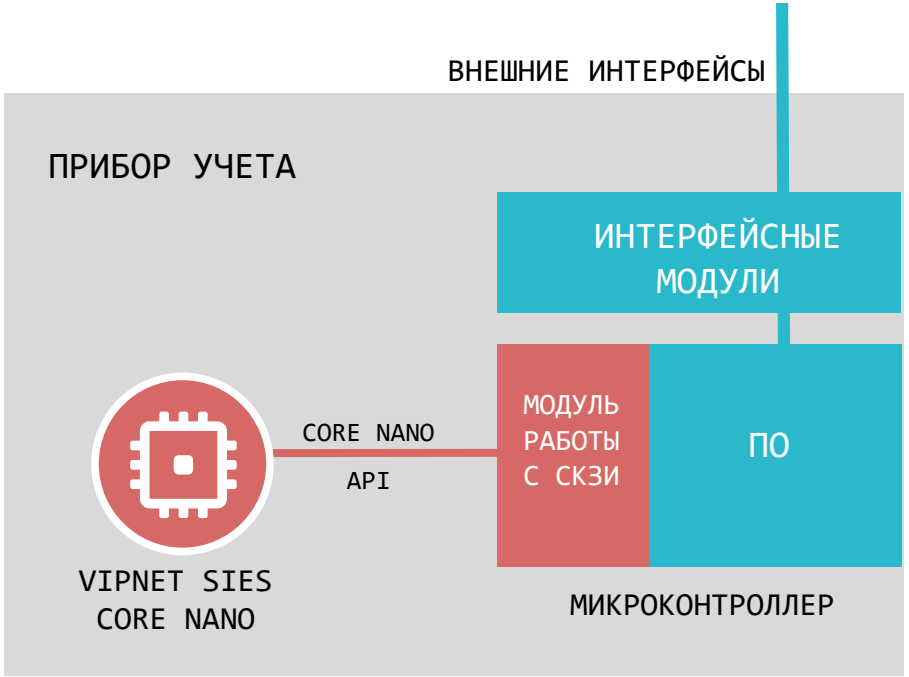
**Релиз выпущен*

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

Интеграция на аппаратном уровне – SPI

Интеграция на программном уровне – Core Nano API

Место установки – завод, производящий устройства

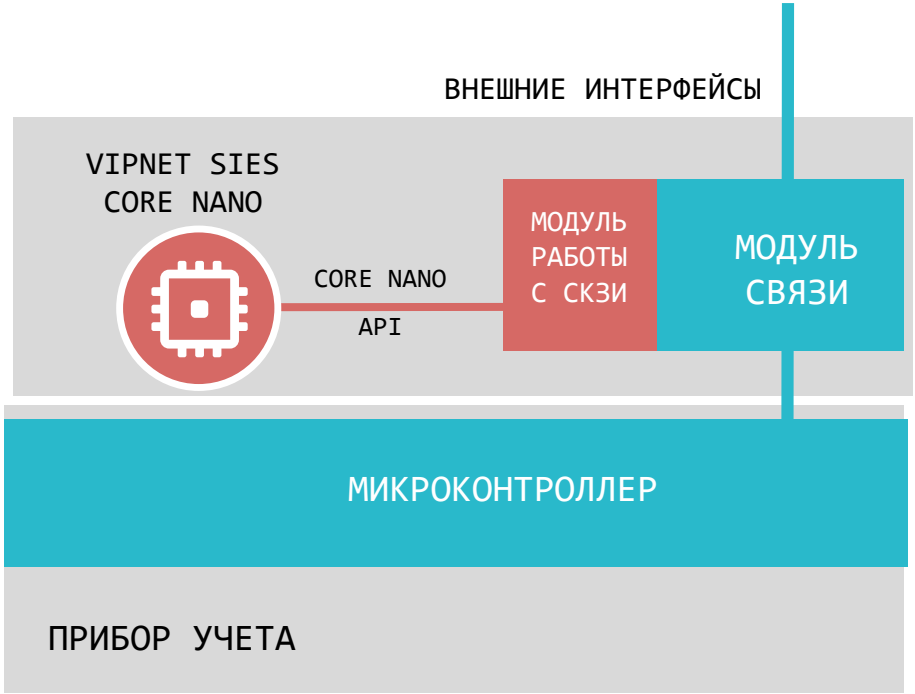


Встраивание ViPNet SIES Core Nano в модули связи

Интеграция на аппаратном уровне – SPI

Интеграция на программном уровне – Core Nano API

Место установки – завод, производящий модули связи



СКЗИ ViPNet SIES Core Nano

Криптографический протокол – Р 1323565.1.029–2019 (CRISP) (наборы 3 и 4)
Криптографические алгоритмы – ГОСТ Р 34.12-2018, ГОСТ Р 34.13-2018, ГОСТ Р 34.11-2018

Соответствие требованиям:

- СКЗИ класса КС3*
- СКЗИ-НР* в части защиты атак инженерного проникновения

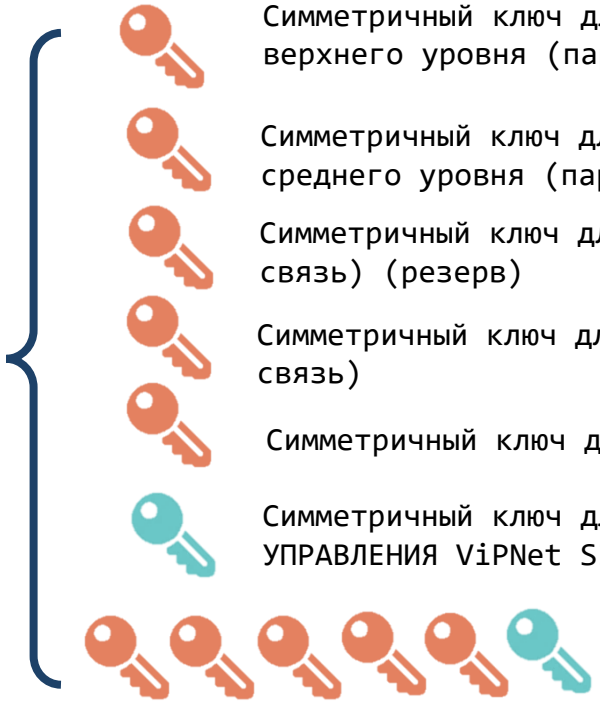
**В процессе тематических исследований*

Криптографические операции:

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

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

СРЕДСТВО ГЕНЕРАЦИИ КЛЮЧЕЙ – SIES HSM



Симметричный ключ для обмена данными с устройством верхнего уровня (парная связь)

Симметричный ключ для обмена данными с устройством среднего уровня (парная связь)

Симметричный ключ для обмена данными с устройством (парная связь) (резерв)

Симметричный ключ для собственных нужд Core Nano (парная связь)

Симметричный ключ для резервированной связи с верхним уровнем

Симметричный ключ для обмена данными с ЦЕНТРОМ УПРАВЛЕНИЯ ViPNet SIES MC

Резервный набор ключей

ViPNet SIES Core Nano: временные и групповые ключи

ГЕНЕРАЦИЯ И СМЕНА КЛЮЧЕЙ ВО ВРЕМЯ ЭКСПЛУАТАЦИИ

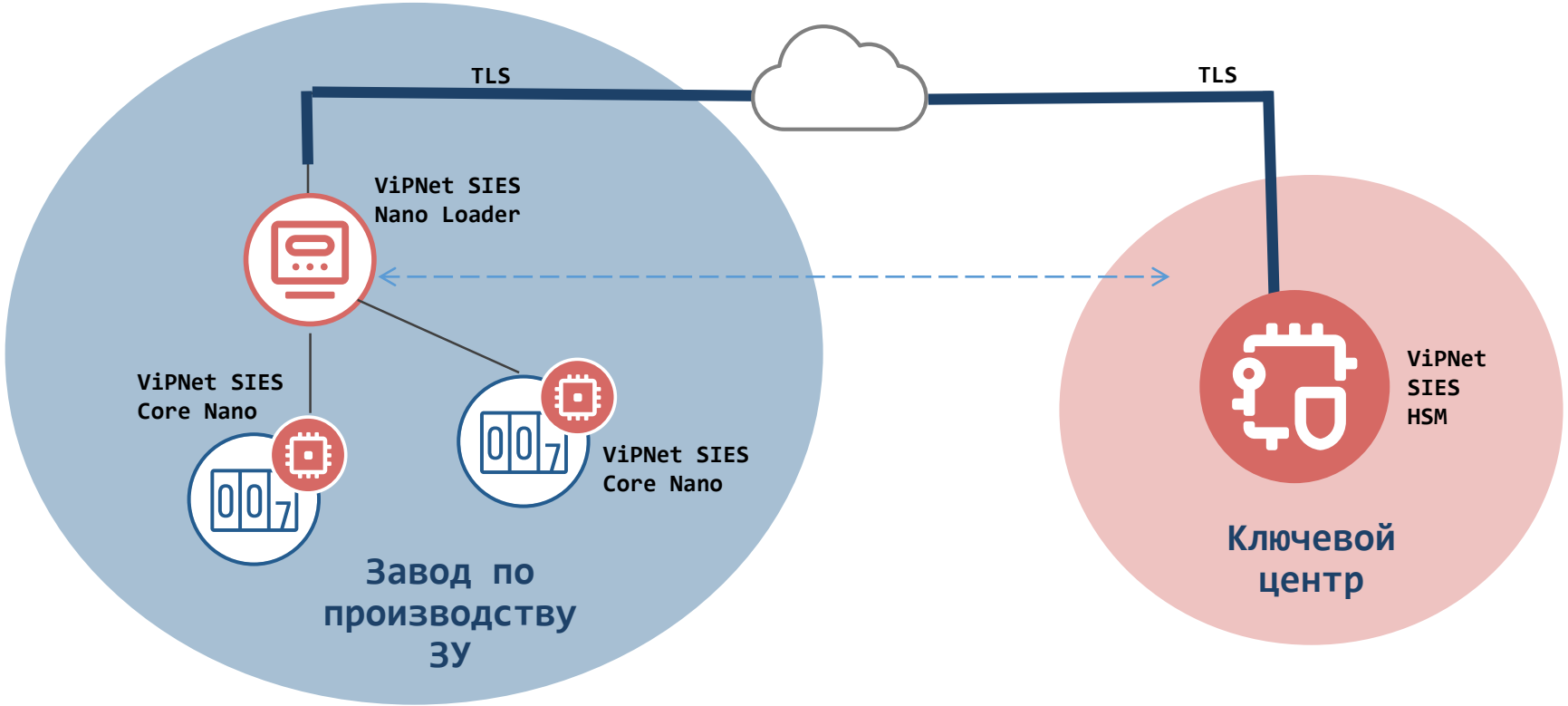
ЗАГРУЗКА ЧЕРЕЗ SIES MC

x20

Временные симметричные ключи для обмена данными с устройствами
Средство генерации ключей – SIES MC

Групповой (мультивещательный ключ), сроком действия до 16 лет
Средство генерации ключей – SIES HSM

Загрузка ключевой информации в ViPNet SIES Core Nano на заводе



ПАК ViPNet SIES Nano Loader

АРМ ввода ключей ПАК ViPNet SIES Core Nano

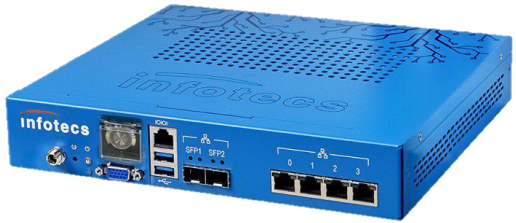
Состоит из:

- АП KB100Q2
- модуля SIES Core Nano Adapter

Позволяет:

- Подключиться к технологической оснастке для загрузки ключей в SIES Core Nano
- Запросить ключи SIES Core Nano в SIES HSM и экспортировать их в защищенном виде
- Загрузить ключи в SIES Core Nano
- Ассоциировать защищаемое устройство и SIES Core Nano
- Загрузить отчет о подготовленных SIES Core Nano и защищаемых ими устройствах в ключевой центр ViPNet SIES HSM

СКЗИ класса КС3*



* *Релиз выпущен*
* *В процессе тематических исследований*

Комплекс ViPNet SIES HSM

Исполнение 1: стандартное исполнение

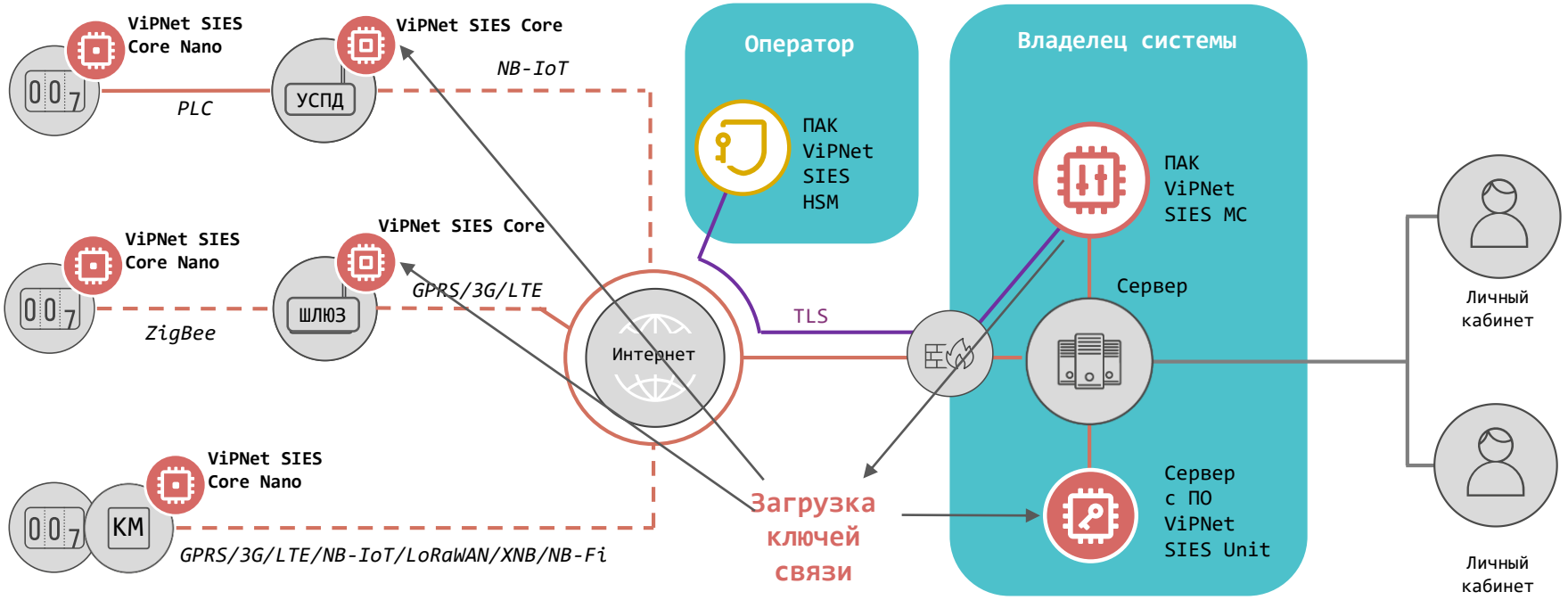
Исполнение 2: исполнение с резервированием

**Релиз запланирован на Q1 2024*

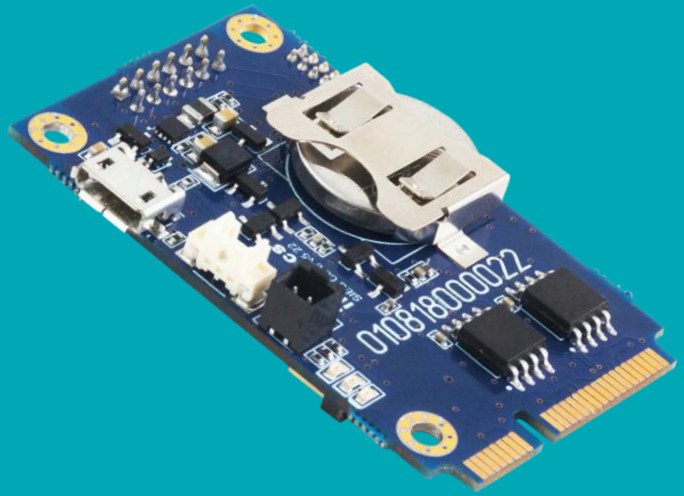
infotecs

- Долговременное защищенное хранение ключевой информации ViPNet SIES Core Nano
- Регистрация производителей устройств и их АРМ загрузки ключей в ViPNet SIES Core Nano
- Генерация и предоставление ключевой информации по запросу АРМ загрузки ключей производителей устройств
- Предоставление ключевой информации по запросу ViPNet SIES MC
- Ядро комплекса – СКЗИ класса КВ

Загрузка ключей в ViPNet SIES Core и ViPNet SIES Unit



Криптомодуль ViPNet SIES Core 2.5



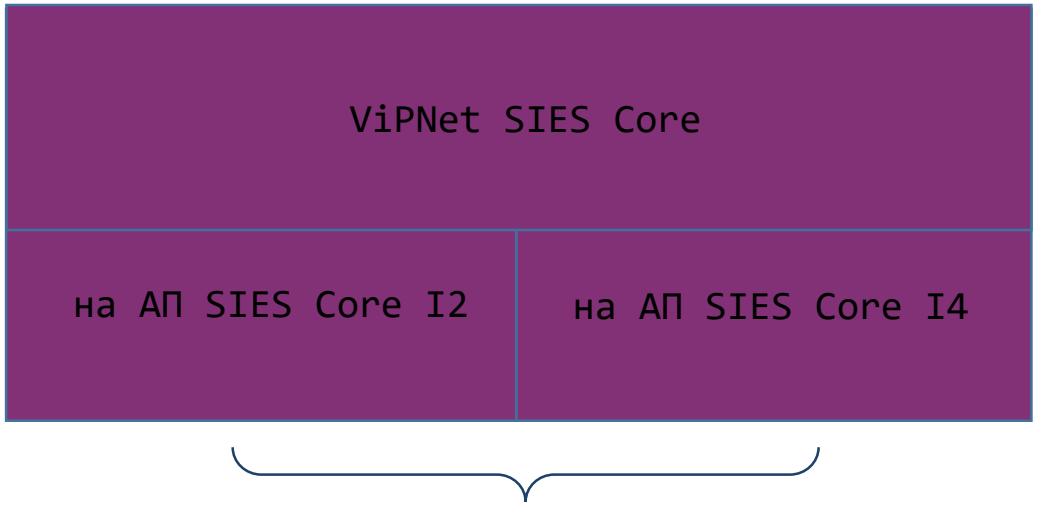
ДЛЯ ИНТЕГРАЦИИ В УСПД / ШЛЮЗ

- Интеграция на аппаратном уровне – USB, UART, SPI
- Интеграция на программном уровне – SIES Core API
- Возможность использования вне контролируемой зоны при подключении ДНСД
- Рабочий диапазон температур – -40…+70 ⁰C
- Форм-фактор – плата PCI Express® Full-Mini Card (51 x 30 x 11,2 мм)
- Наличие SDK под Linux (ARM, x86), Windows, Baremetal (для устройств без ОС)
- Сертификат СКЗИ класса КС3 по требованиям ФСБ России

ПАК ViPNet SIES Core

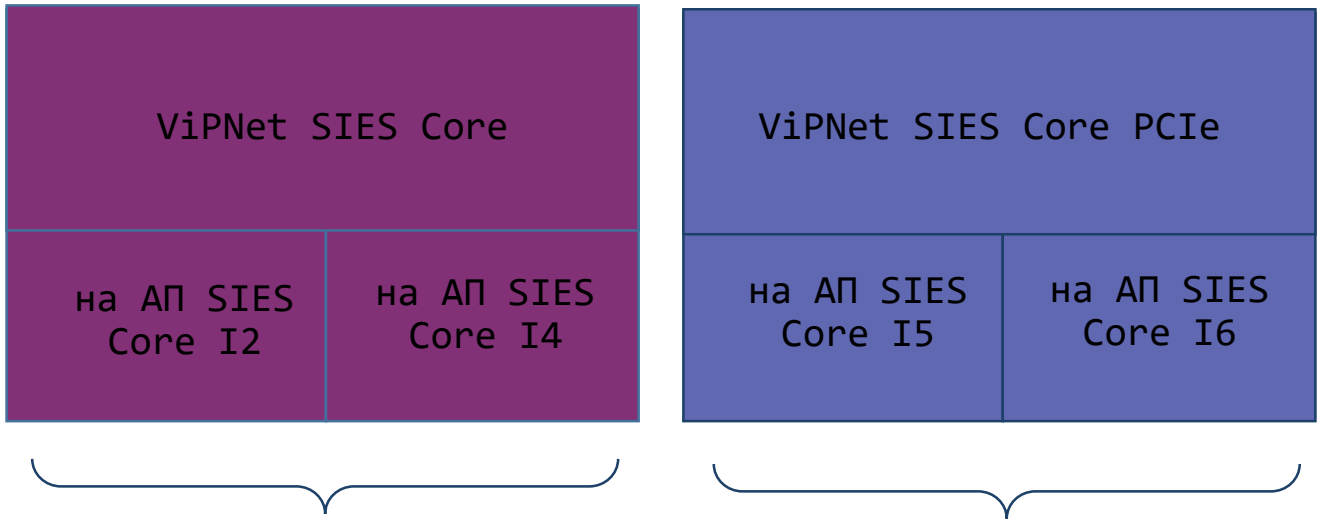
ViPNet SIES Core 2.4

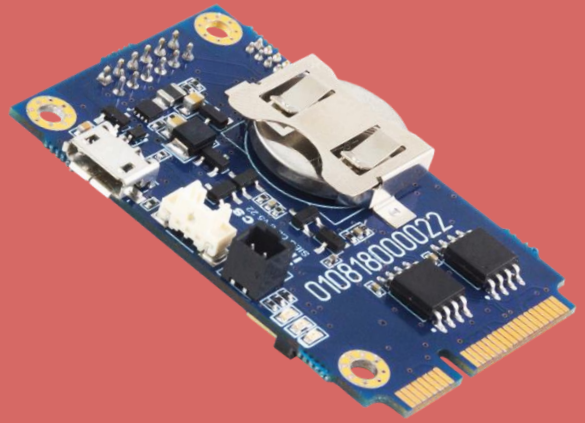
Исполнения



ViPNet SIES Core 2.5

Исполнения





ДЛЯ ИНТЕГРАЦИИ В УСПД / ШЛЮЗ

- Интеграция на аппаратном уровне:
  - USB (Micro USB и PCI-Express разъемы)
- Возможность использования вне контролируемой зоны при подключении ДНСД
- Рабочий диапазон температур – -40…+70 ^{0}C
- Форм-фактор – плата PCI Express® Full-Mini Card (51 x 30 x 11,2 мм) в соответствии со стандартом
- Наличие SDK под Linux (ARM, x86), Windows, RTOS
- СКЗИ класса КС3 по требованиям ФСБ России*

** Релиз выпущен*
** В процессе тематических исследований*

ПАК ViPNet SIES Core PCIe (2.5)

ViPNet SIES Core & SIES Core PCIe 2.5: что «еще» нового?

- Встречная работа с ViPNet SIES Core Nano
- Поддержка алгоритма МАГМА для CMS (служебный и прикладной)
- Ротируемый журнал аудита.

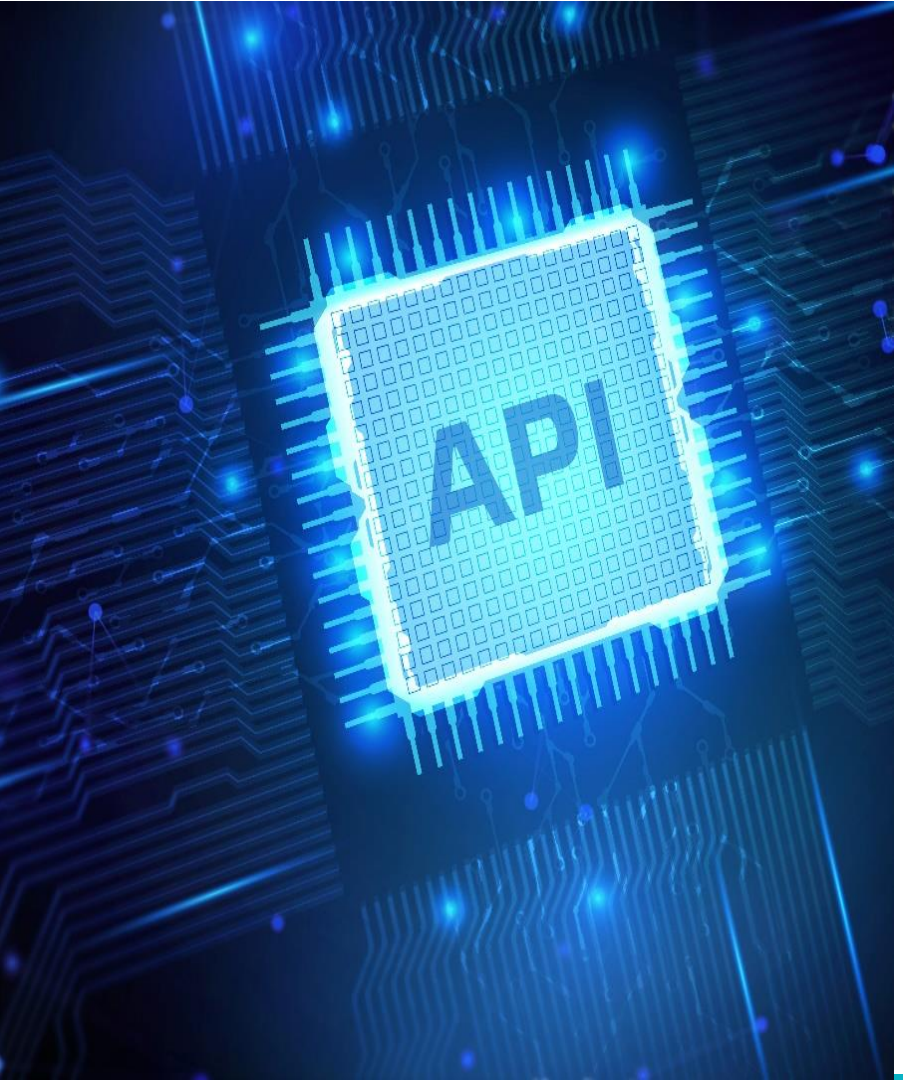
ViPNet SIES Unit 2.5

ИВК И АРМ КОНФИГУРАТОР

ПО ViPNet SIES Unit 2.5

- Интеграция по RESTfull API (HTTP/1.1), gRPC API (HTTP/2) или SDK;
- Поддерживаемые ОС:
  - Windows 10 (x86/64), Windows Server 2012/2012 R2/ 2016,
  - Debian 10 и 11, Ubuntu 16 и 18 и др ОС Linux (gcc v.6 и выше, systemd система инициализации, x86/64 или ARM, менеджер пакетов deb/rmp формата)
  - Astra Linux Special Edition (Смоленск) 1.6 и 1.7, Альт 8 СП
- Возможность установки на выделенный сервер
- Исполнения с поддержкой различного количества связей: 50, 500, 2000, 10 000 связей
- СКЗИ классов КС1 и КС3 по требованиям ФСБ России*

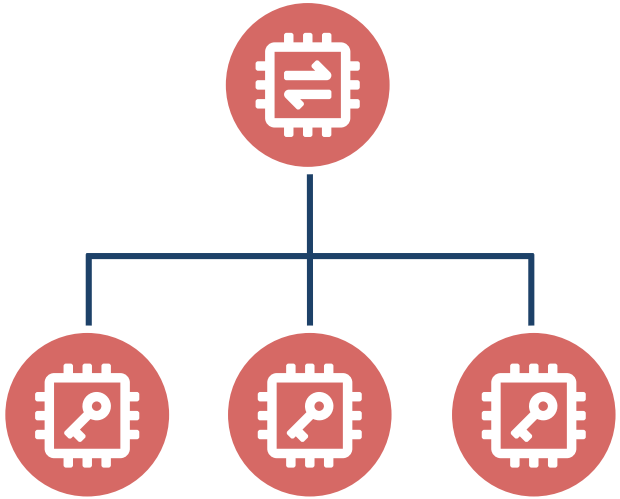
** Релиз выпущен*
** В процессе тематических исследований*



ПО ViPNet SIES Unit 2.5: что «еще» нового?

- Встречная работа с ViPNet SIES Core Nano
- Поддержка алгоритма МАГМА для CMS (служебный и прикладной)
- Использование в среде виртуализации KVM Astra Linux SE 1.7, Альт 8 СП.

ПО ViPNet SIES Unit Router 2.5



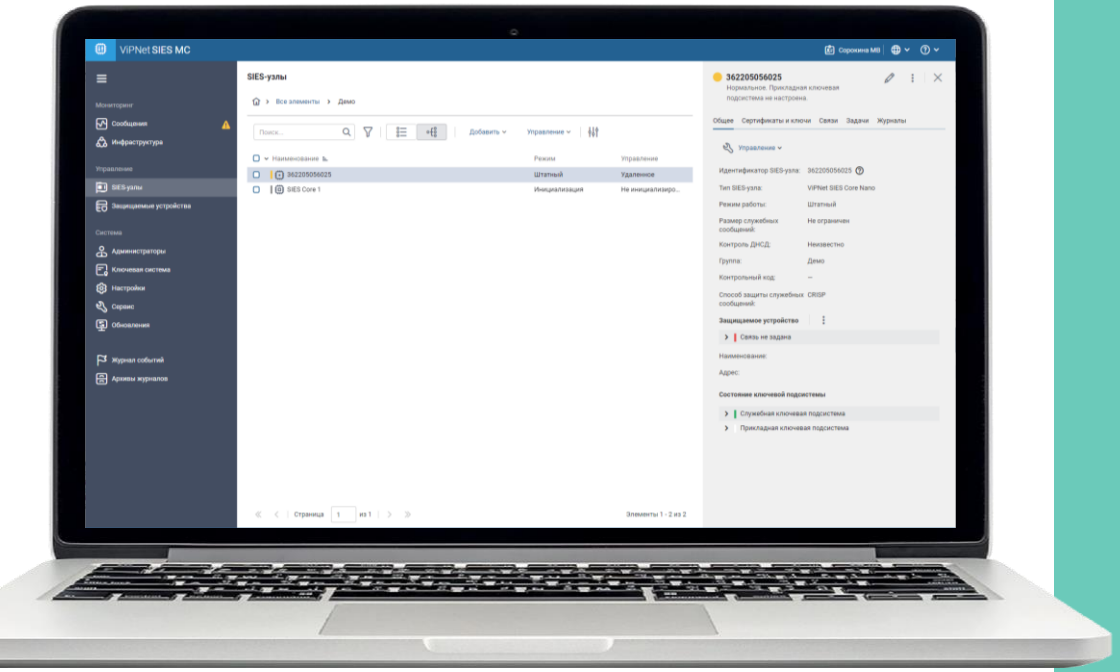
**Релиз запланирован на Q4 2023*

infotecs

- Масштабирование ViPNet SIES Unit
- Единая точка входа для запросов с защищаемых устройств
- Распределение нагрузки для работы навстречу 2 млн. SIES-узлов
- Поддержка API-интерфейса SIES Unit для интеграции с защищаемыми устройствами: RESTfull API (HTTP/1.1), gRPC (HTTP/2)
- Самостоятельная генерация карты маршрутизации запросов
- Возможность объединения в кластер (до 20 узлов SIES Unit Router)

Центр управления ViPNet SIES MC 2.5

ПАК ViPNet SIES MC



- 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

Исполнения ПАК ViPNet SIES MC

ViPNet SIES MC VA

Кол-во SIES узлов – 5 000

ViPNet SIES MC10000

АП: SIES MC10000 Q1 и SIES MC10000 Q2

Кол-во SIES узлов – 1 млн.

ViPNet SIES MC3000

Кол-во SIES узлов – 3 000

ViPNet SIES MC IoT

Кол-во SIES узлов – 2 млн.

**Релиз в разработке, ожидание Q2 2024*

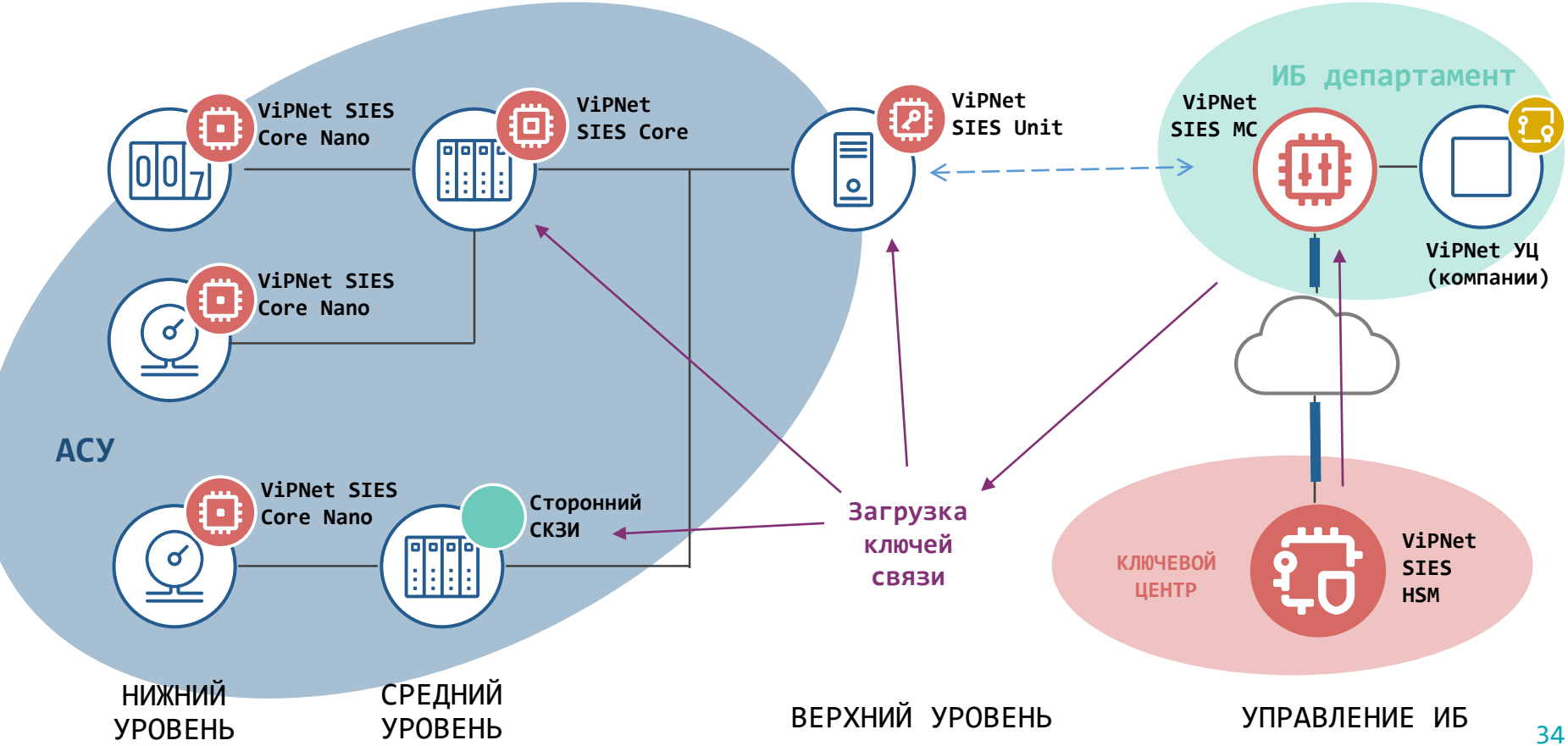
SIES-узлы 2.5

СКЗИ, выполняющие прикладные криптографические операции с данными защищаемых устройств

Защищаемые устройства

средства обработки информации, интегрированные с SIES-узлами

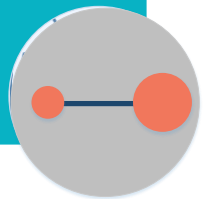
Взаимодействие с ViPNet SIES HSM



Типы связей между защищаемыми устройствами

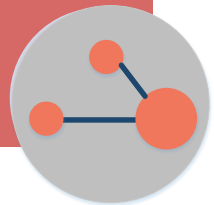
Парные

- Вычисление и проверка имитовставки (CRISP)
- Шифрование в режиме реального времени (CRISP)
- Шифрование и проверка электронной подписи
- Вычисление и проверка хэш-суммы



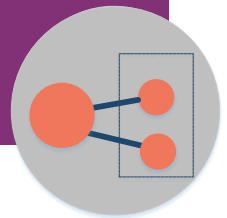
Мультивещательные

- Вычисление и проверка имитовставки (CRISP)
- Шифрование в режиме реального времени (CRISP)



Резервированные

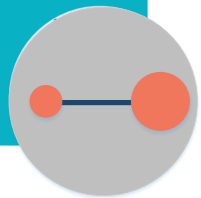
- Вычисление и проверка имитовставки (CRISP)
- Шифрование в режиме реального времени (CRISP)
- Шифрование и проверка электронной подписи
- Вычисление и проверка хэш-суммы



Постоянные/временные

- Вычисление и проверка имитовставки (CRISP)
- Шифрование в режиме реального времени (CRISP)
- Шифрование и проверка электронной подписи
- Вычисление и проверка хэш-суммы

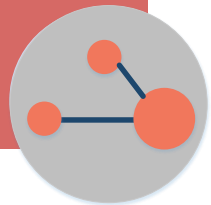
Парные



Постоянные

- Вычисление и проверка имитовставки (CRISP)
- Шифрование в режиме реального времени (CRISP)

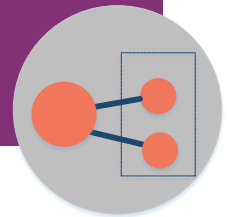
Мультивещательные



Постоянные

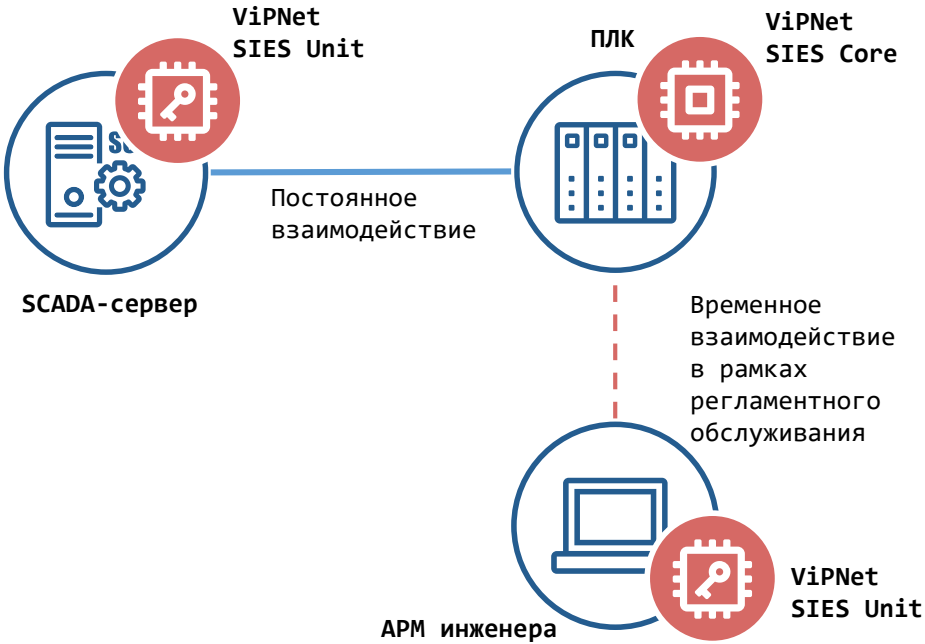
- Вычисление и проверка имитовставки (CRISP)
- Шифрование в режиме реального времени (CRISP)
- Шифрование и проверка электронной подписи
- Вычисление и проверка хэш-суммы

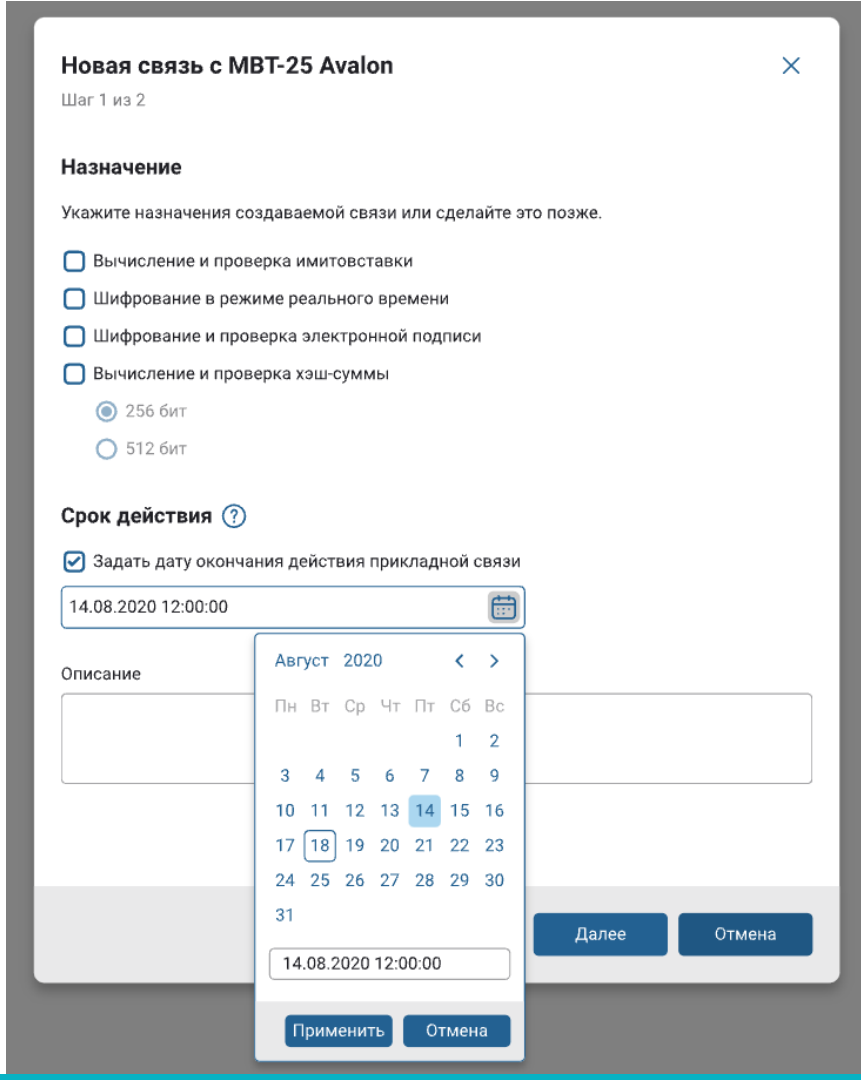
Резервированные



Типы связей между защищаемыми устройствами 2.5

Добавление временных связей между устройствами





Работа с большим количеством защищаемых устройств: файл ведомости

- Источник файла ведомости:
  - ViPNet SIES Nano Loader
  - ИС заводов производителей защищаемых устройств
- Регистрация защищаемых устройств в ViPNet SIES MC на основе файла ведомости
- Регистрация SIES-узлов и их типа в ViPNet SIES MC на основе файла ведомости
- Назначение SIES-узлов на защищаемые устройства

Работа с большим количеством защищаемых устройств: карта сети

- API для взаимодействия с ИС для получения карты сети
- Регистрация защищаемых устройств в ViPNet SIES MC на основе карты сети
- Регистрация и изменение связей между защищаемыми устройствами
- Внесение изменений в атрибуты SIES-узлов и защищаемых устройств

ViPNet SIES MC 2.5: что «еще» нового?

- Поддержка алгоритма МАГМА для CMS (служебный и прикладной)
- Увеличили период архивации журнала аудита
- Отказались от rnd_maker для ViPNet SIES MC VA, генерация энтропии происходит без использования сторонних утилит
- Повысили удобство эксплуатации по ряду параметров

ViPNet SIES Workstation 2.6

ПО ViPNet SIES Workstation

Инициализация ViPNet SIES Core и ViPNet SIES Unit

- Загрузка первичной ключевой информации
- Настройка служебной ключевой подсистемы

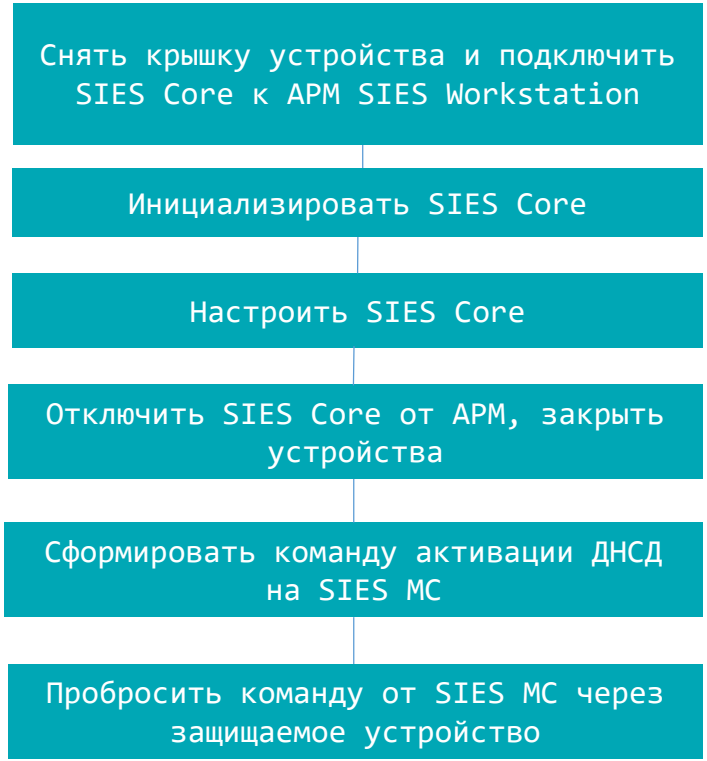
Локальное обслуживание ViPNet SIES Core

- Управление ViPNet SIES Core в режимах штатный, конфигурирование, блокировка

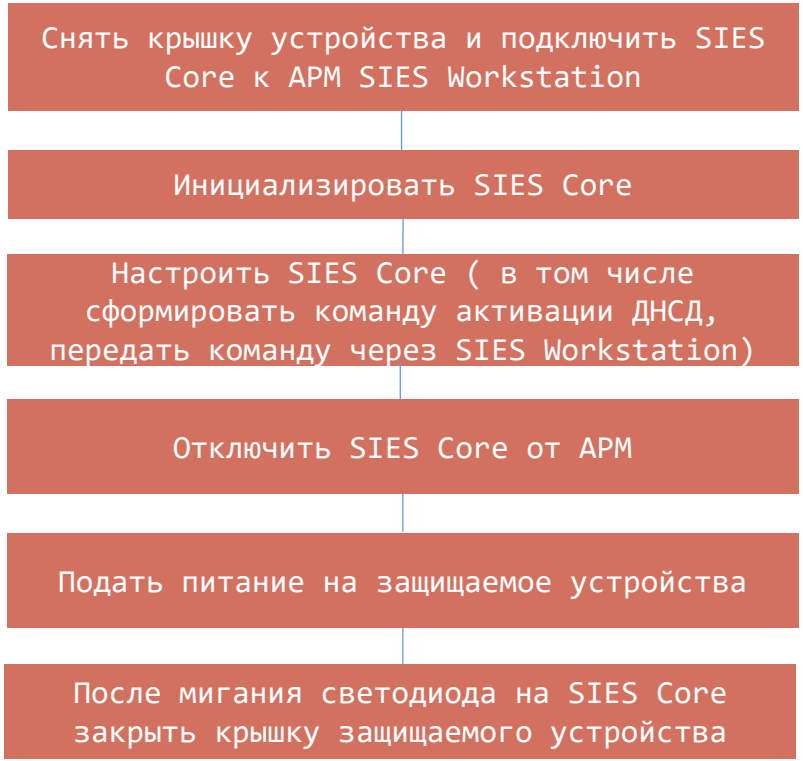
ПО ViPNet SIES Workstation 2.5 & 2.6: что нового?

- Поддержка SIES-узлов версии 2.5
- Версия под Linux: Debian 10.12, Astra Linux Special Edition 1.7, Astra Linux Commom Edition 2.12.42 и 2.12.45, Альт 8.2 СП Рабочая станция 8.2 и 8.4, Альт Рабочая станция 9.1
- Упрощенная включение датчиков контроля доступа к ViPNet SIES Core

Упрощен процесс активации ДНСД

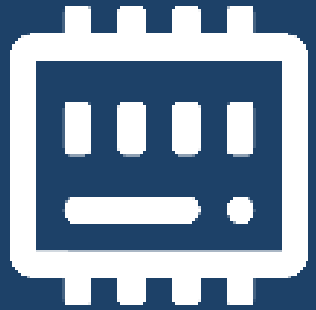


ViPNet SIES Core 2.3 и ниже



ViPNet SIES Core 2.4

ViPNet SIES Smartmeter WS 2.6



АВТОМАТИЗИРОВАННЫЙ ВВОД В ЭКСПЛУАТАЦИЮ ЗАЩИЩАЕМЫХ УСТРОЙСТВ С VIPNET SIES CORE В ТОПОЛОГИИ «ЗВЕЗДА»

- Автоматическая инициализация ViPNet SIES Core и регистрация связанного с ним защищенного устройства (ЗУ) в ViPNet SIES MC
- Автоматическое создание связей между ЗУ и центральным сервером с ViPNet SIES Unit, а также загрузка прикладной ключевой информации в СКЗИ
- Поддержка парных и резервированных связей
- Ручной и автоматический режимы работы
- Возможность поточной работы с 8 ЗУ и ViPNet SIES Core
- Возможность включения ДНСД после подготовки ЗУ с ViPNet SIES Core
- Получение отчетов о подготовленных ЗУ и с ViPNet SIES Core
- Версия для Linux и Windows

ПО ViPNet SIES Smartmeter WS

Спасибо за внимание!

Марина Сорокина

Marina.Sorokina@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363