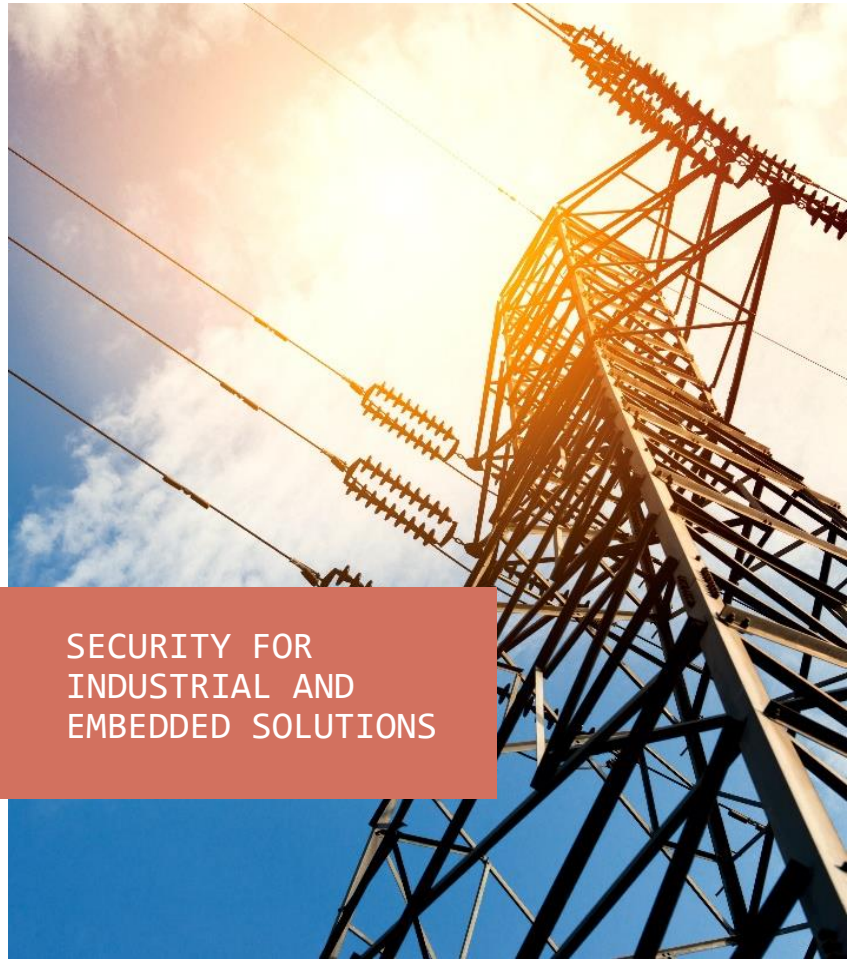
Мастер-класс по разворачиванию решения ViPNet SIES

Алексей Власенко
Ведущий менеджер продуктов

Решение ViPNet SIES

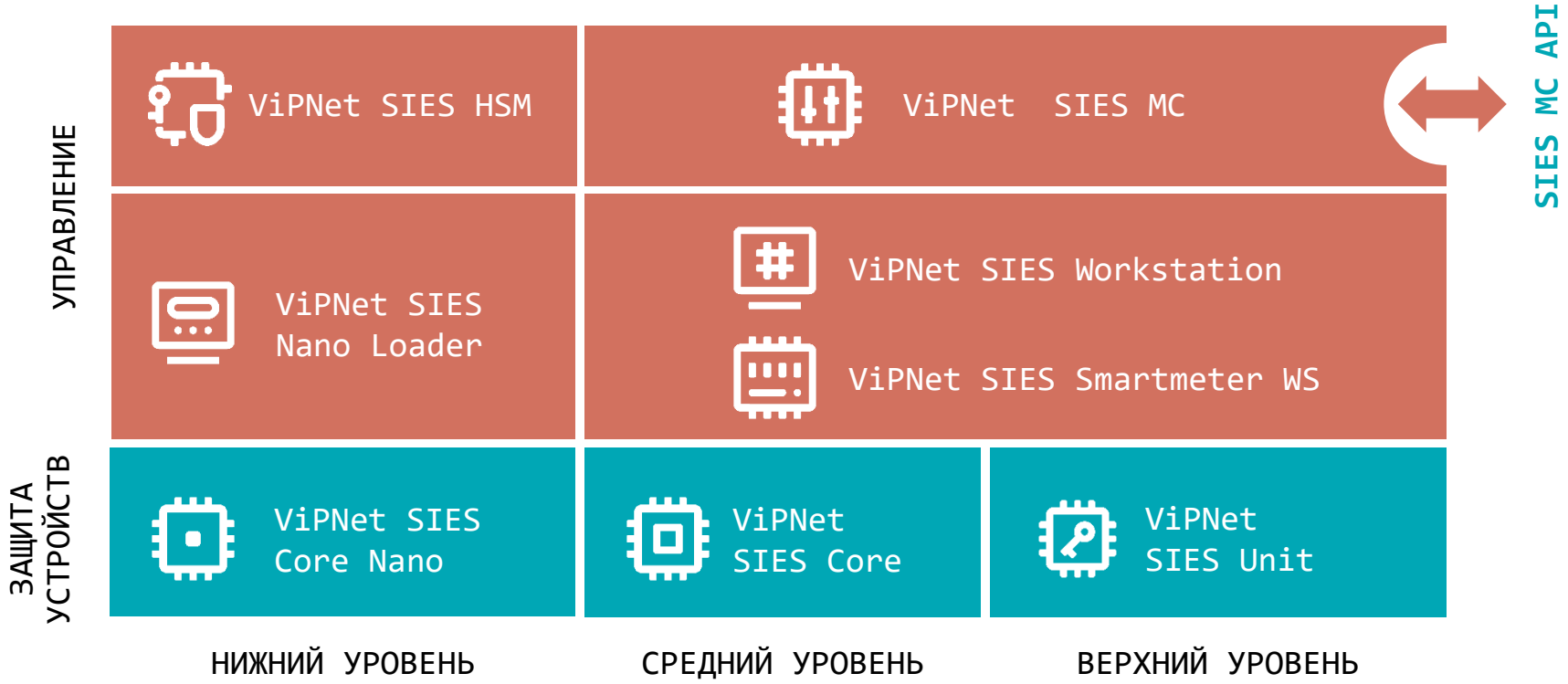


Решение ViPNet SIES

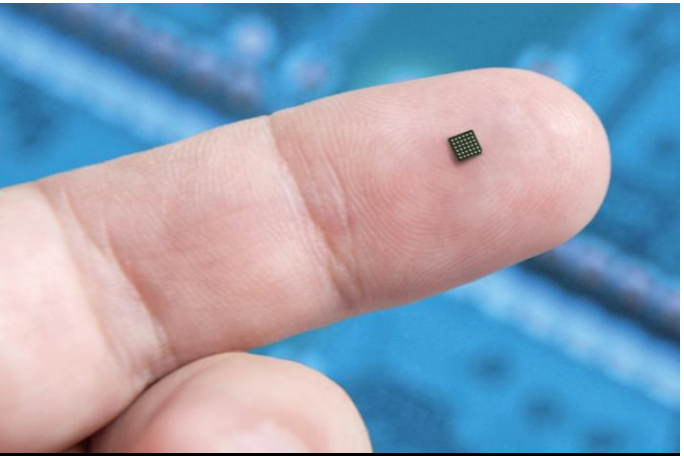
Встраиваемые криптографические средства защиты информации:

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

Состав решения ViPNet SIES



ПАК ViPNet SIES Core Nano



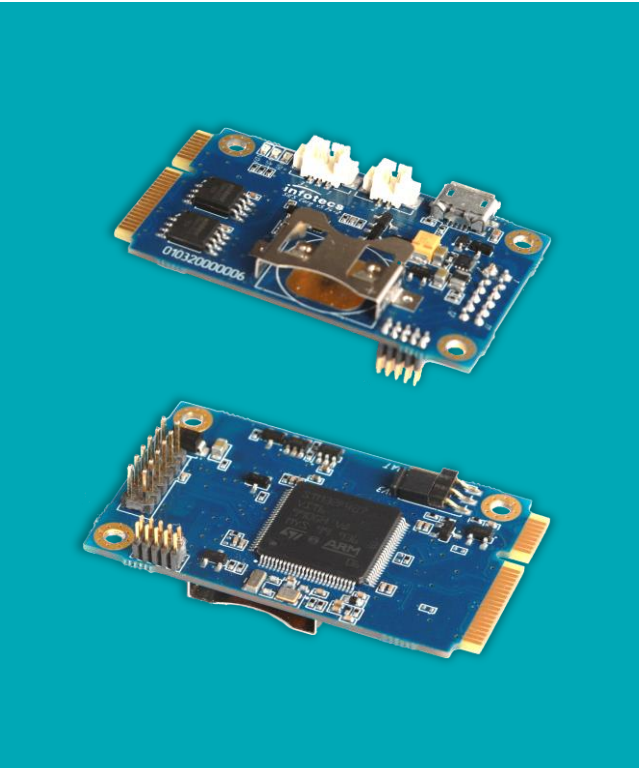
Встраивание:
- На аппаратном уровне – SPI
- На программном уровне – Core Nano API

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

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

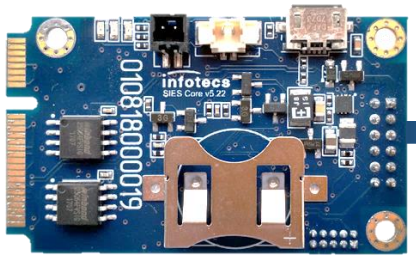
Функциональные особенности:

- 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

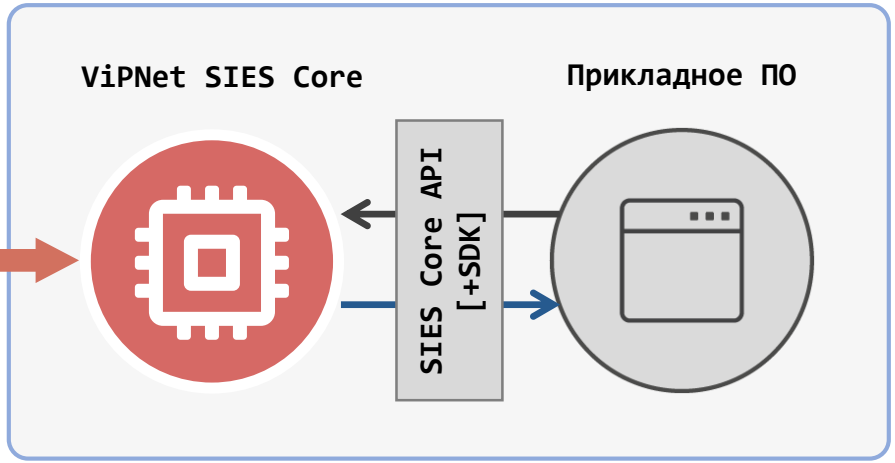
Соответствие требованиям:

- СКЗИ класса КС3

Интеграция ViPNet SIES Core



UART / USB / SPI



ViPNet SIES Core

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

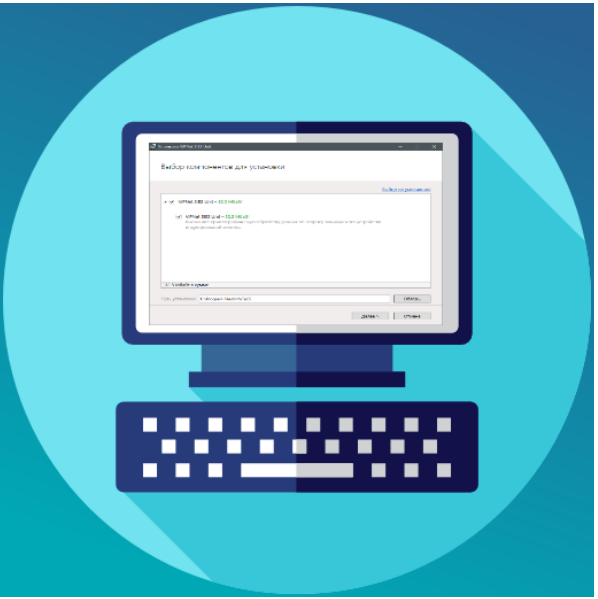
SIES Core SDK:

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

Данные

Защищенные данные

ViPNet SIES Unit



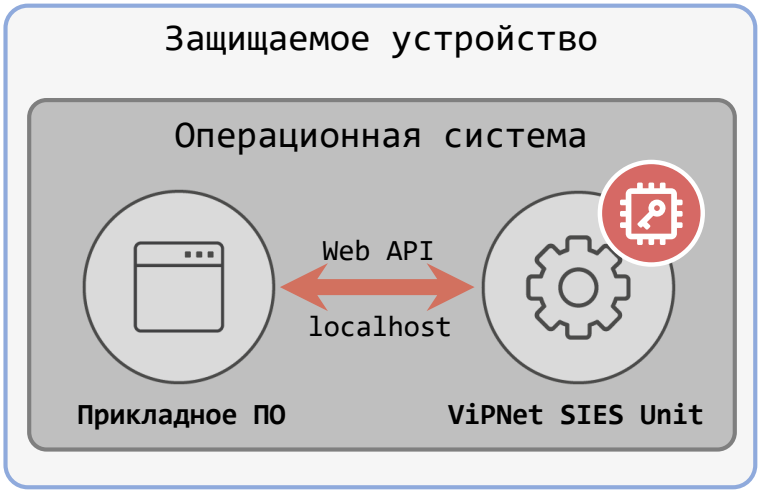
Встраивание:
- ПО устанавливается и работает как сервис ОС
- Интеграция на программном уровне – RESTfull API (HTTP/1.1), gRPC API (HTTP/2) или SDK

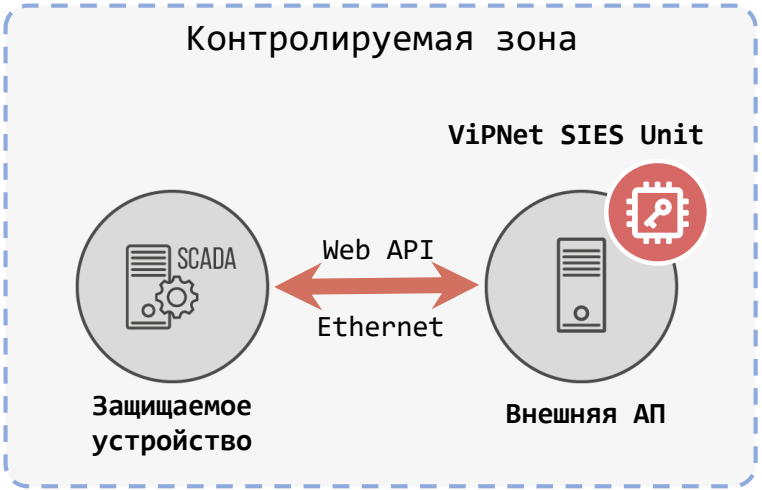
Криптографические функции:
- Зашифрование/расшифрование (CRISP)
- Вычисление/проверка имитовставки (CRISP)
- Зашифрование/расшифрование (CMS)
- Вычисление/проверка ЭП (CMS)
- Вычисление/проверка хэш-кода

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 Смоленск)
- Установка на защищаемое устройство или выделенную платформу

Соответствие требованиям:
- СКЗИ класса КС1 и КС3

Интеграция ViPNet SIES Unit

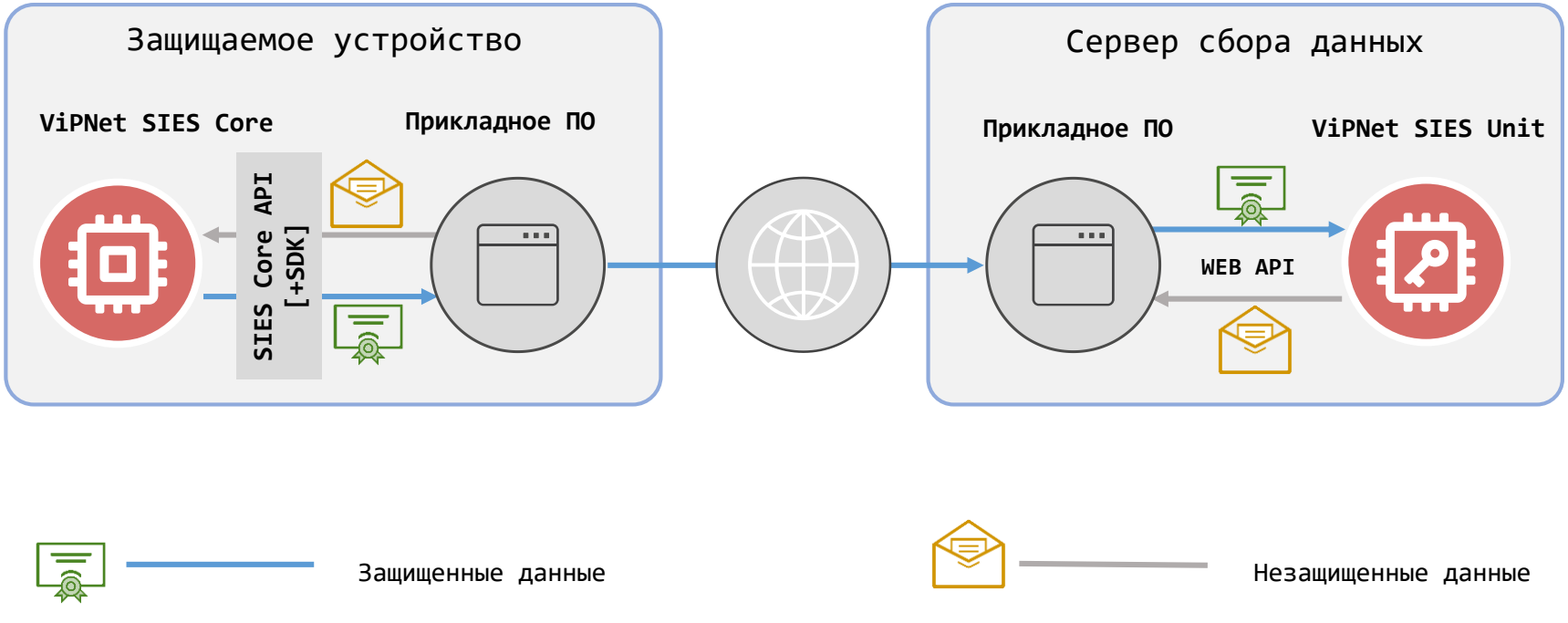




Криптографические сервисы для защищаемых устройств

- Зашифрование/расшифрование по CRISP (ГОСТ 34.12-2018, ГОСТ 34.13-2018)
- Создание имитовставки/ проверка имитовставки по CRISP (ГОСТ 34.12-2018, ГОСТ 34.13-2018)
- Создание ЭП/проверка ЭП в CMS (ГОСТ 34.10-2018)
- Зашифрование/ расшифрование в CMS (ГОСТ 28147-89)
- Создание хэш/проверка хэш (ГОСТ 34.11-2018)

Защита коммуникаций с помощью ViPNet SIES

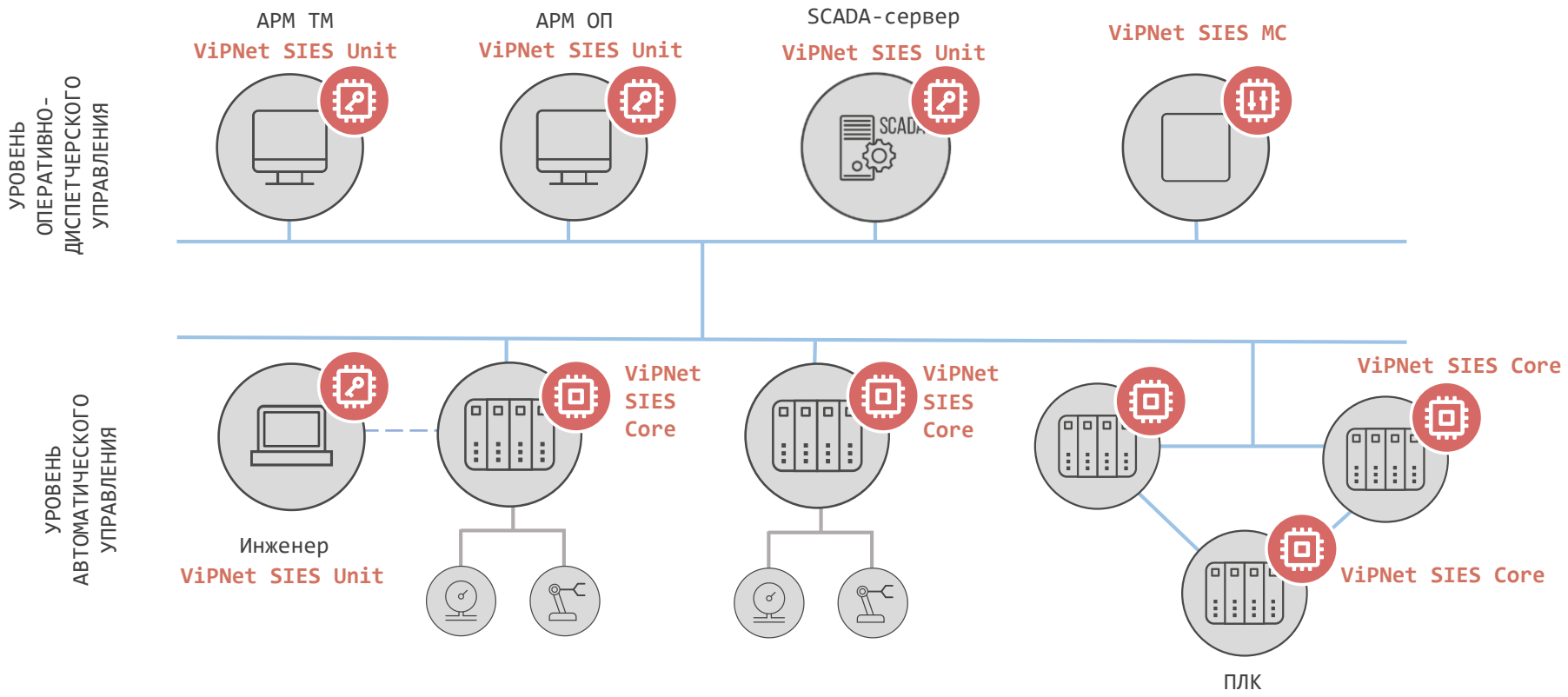


Центр управления ViPNet SIES MC

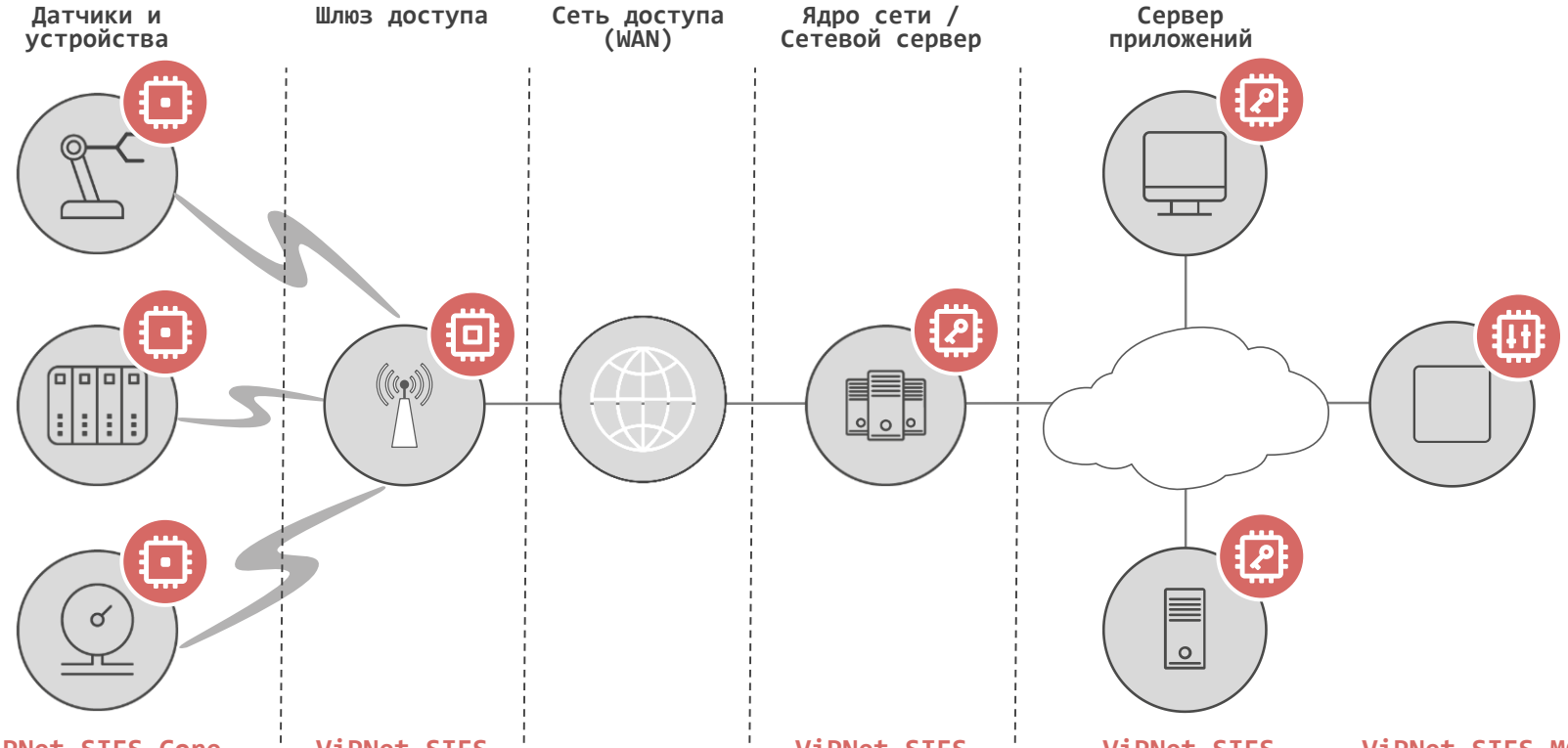
- ПАК ViPNet SIES MC 10000
  - До 1 млн. устройств
  - СКЗИ класса КС3
- ПАК ViPNet SIES MC 3000
  - До 3000 устройств
  - СКЗИ класса КС3
- ViPNet SIES MC VA
  - До 5000 устройств
  - СКЗИ класса КС1

- 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

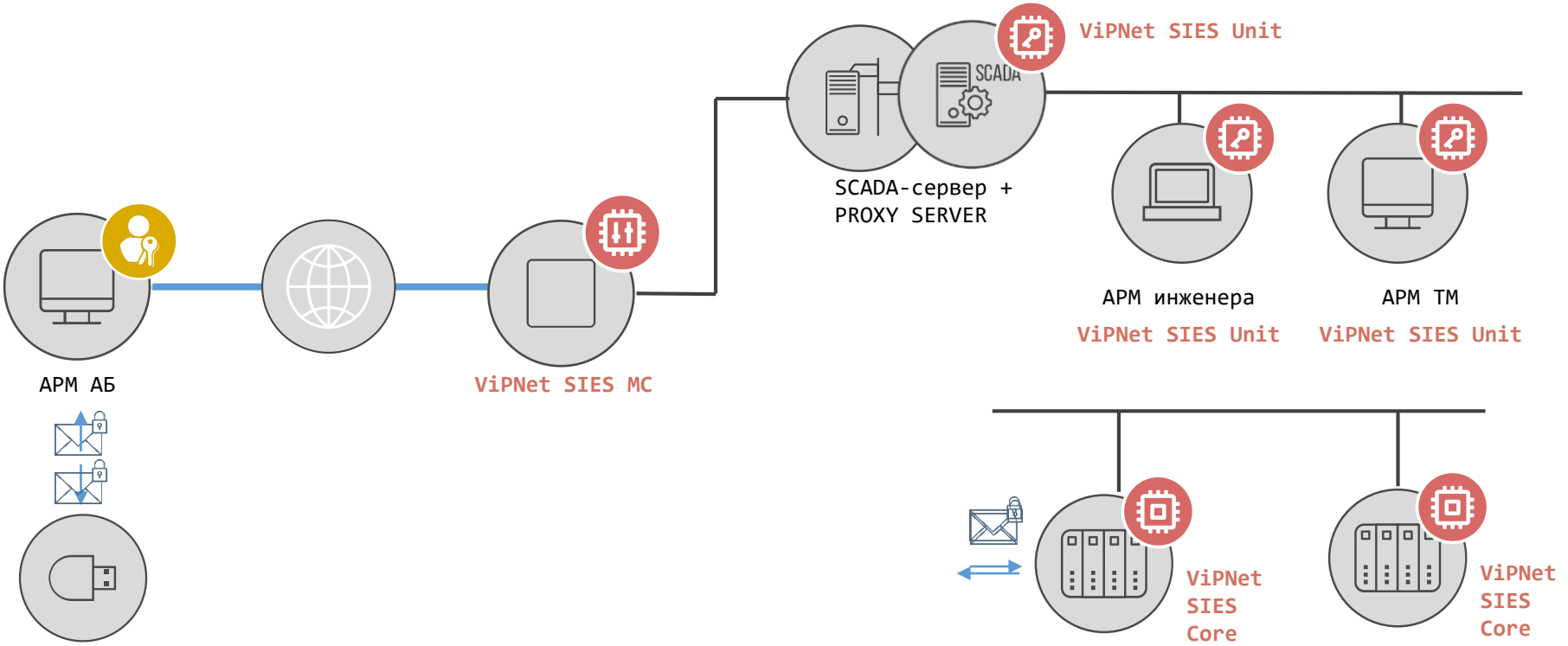
Защищенная АСУ ТП



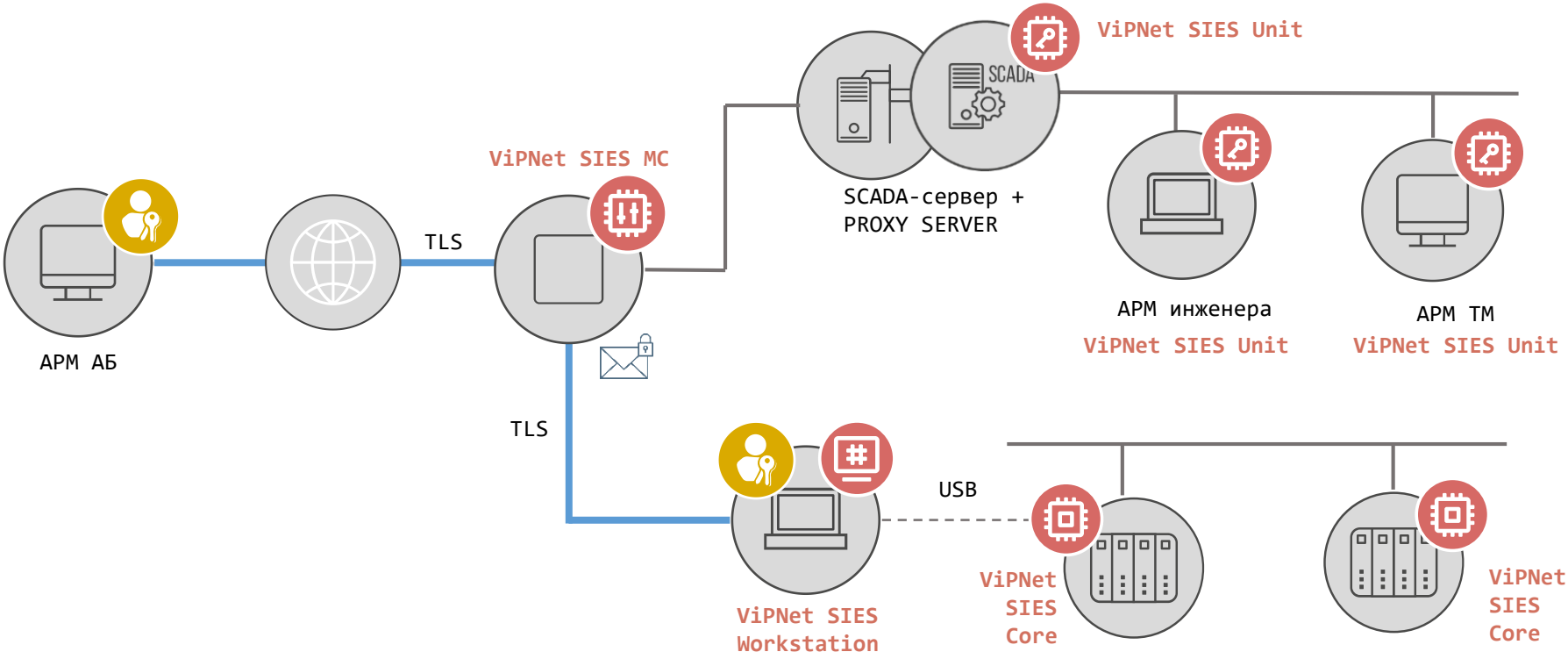
Защита данных в IIoT-системе



Защищенный обмен с SIES-узлами при отсутствии канала связи



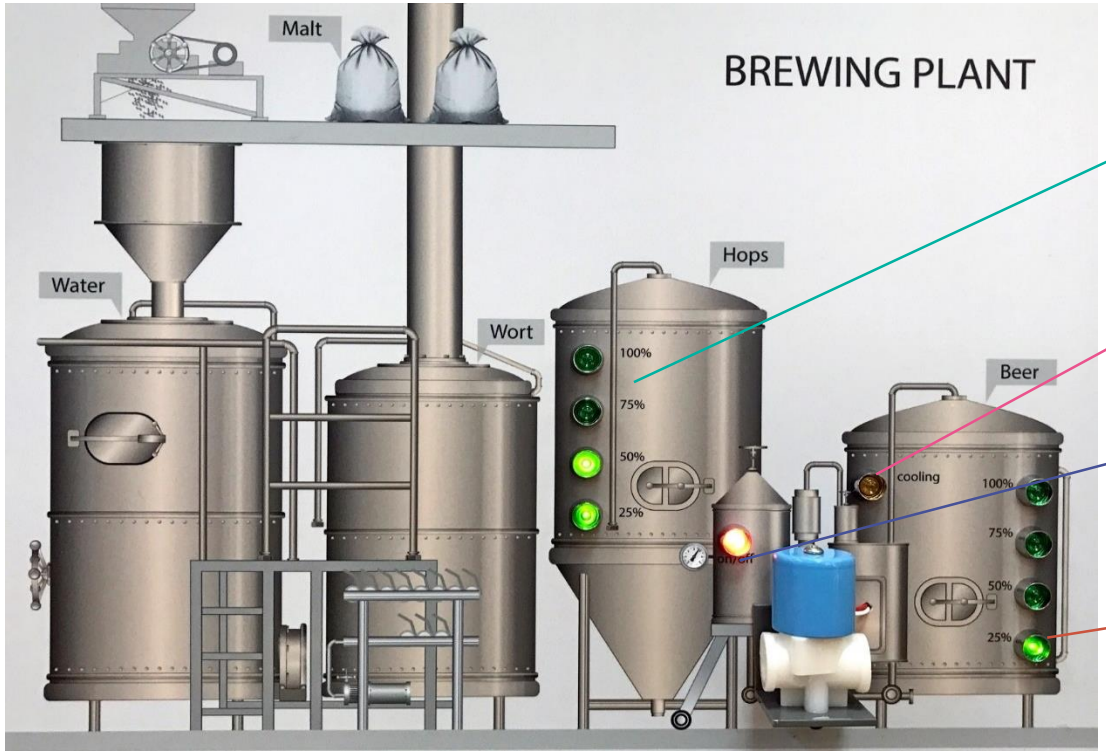
Защищенный обмен с SIES-узлами при отсутствии канала связи



АСУ «Пивоваренный завод»

Технологический процесс пивоварения

Технологический процесс пивоварения



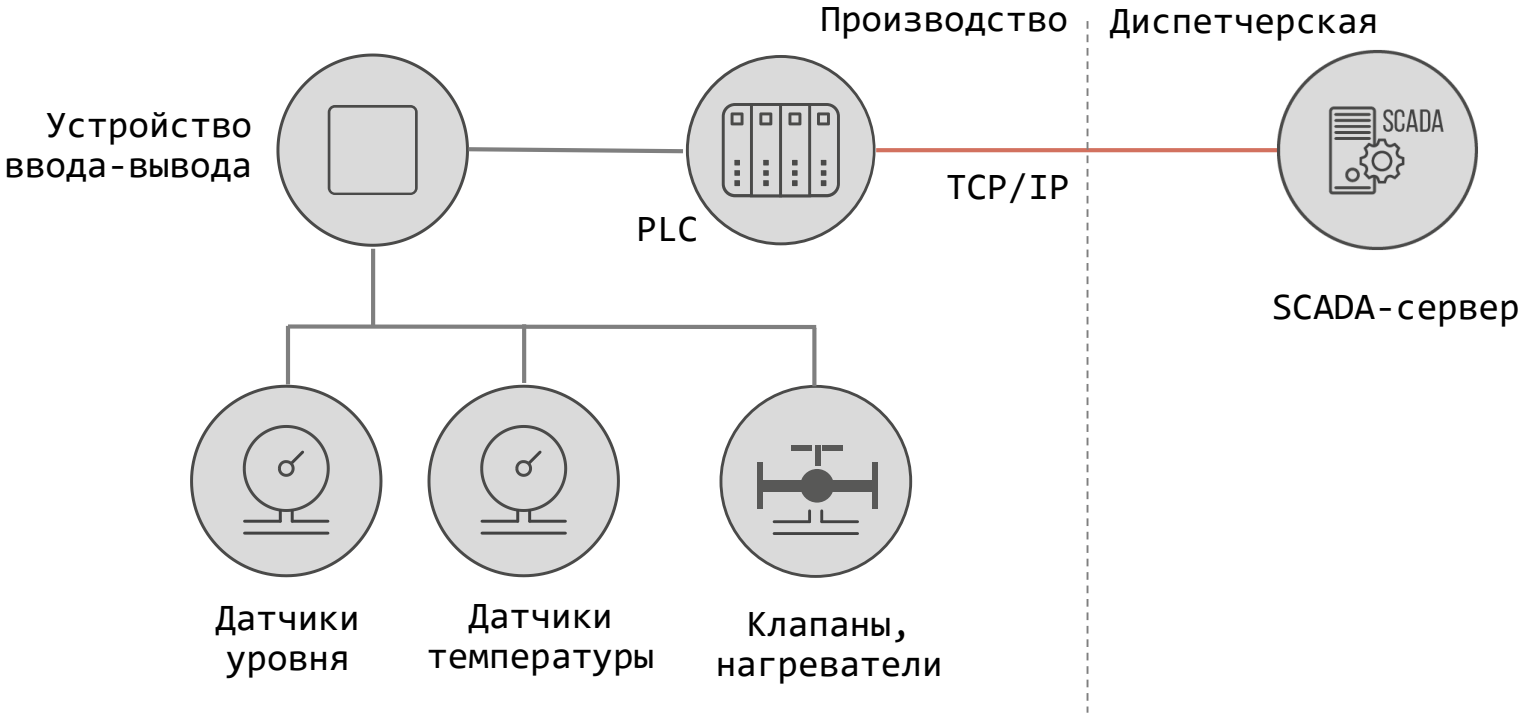
Уровень сусла

Режим охлаждения

Состояние клапана перекачки

Уровень готового пива

Пивоваренный завод



Внутренний нарушитель!!!

Кто-то украл наш SCADA-проект
и сливает все пиво,
как только оно готово.

Разворачивание решения ViPNet SIES

Выпускаем ключи

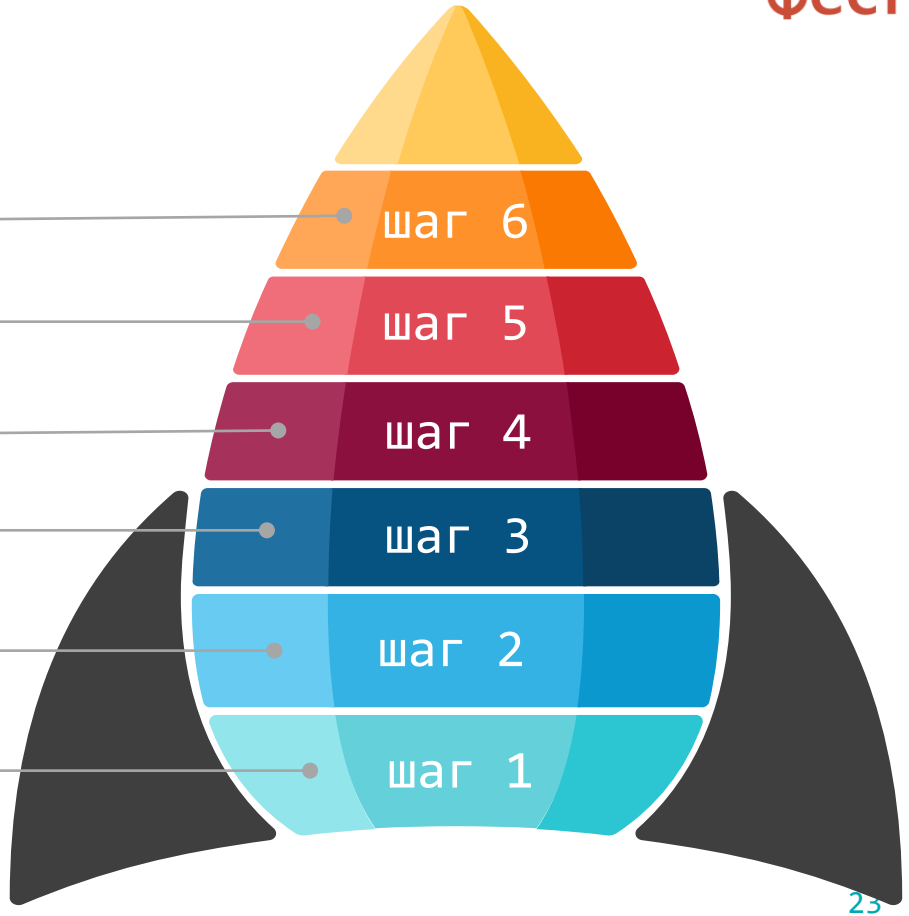
Устанавливаем и инициализируем ViPNet SIES Unit

Устанавливаем ViPNet SIES Core

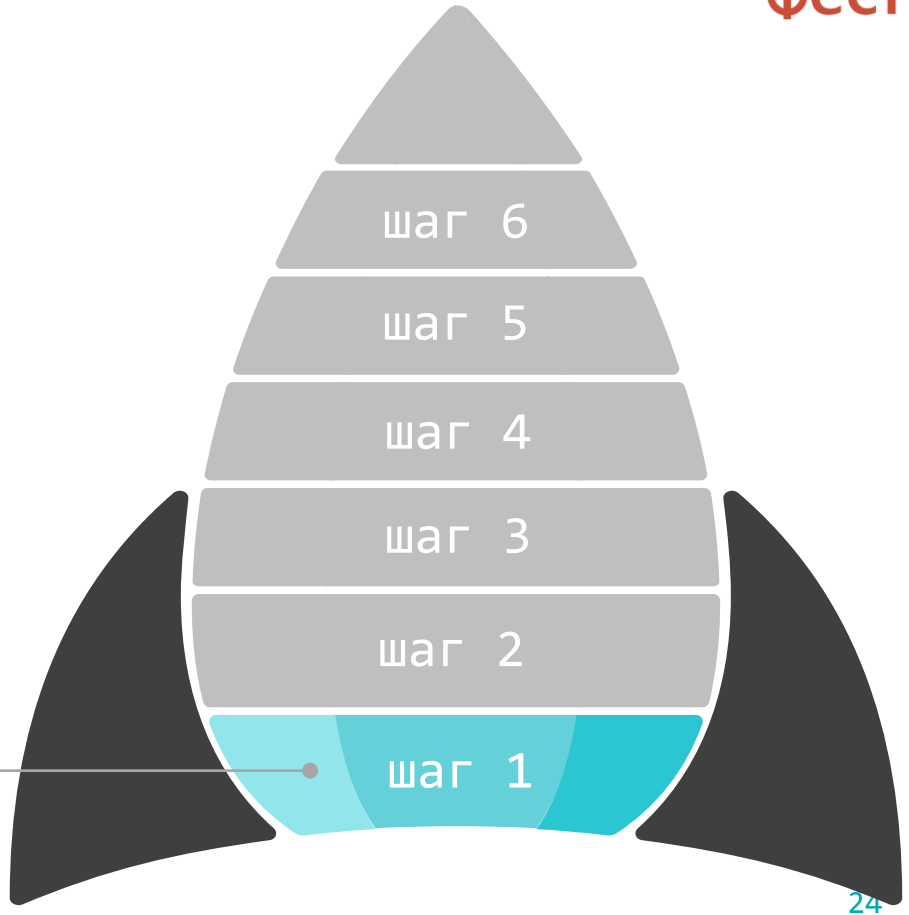
Инициализируем ViPNet SIES Core

Разворачиваем инфраструктуру

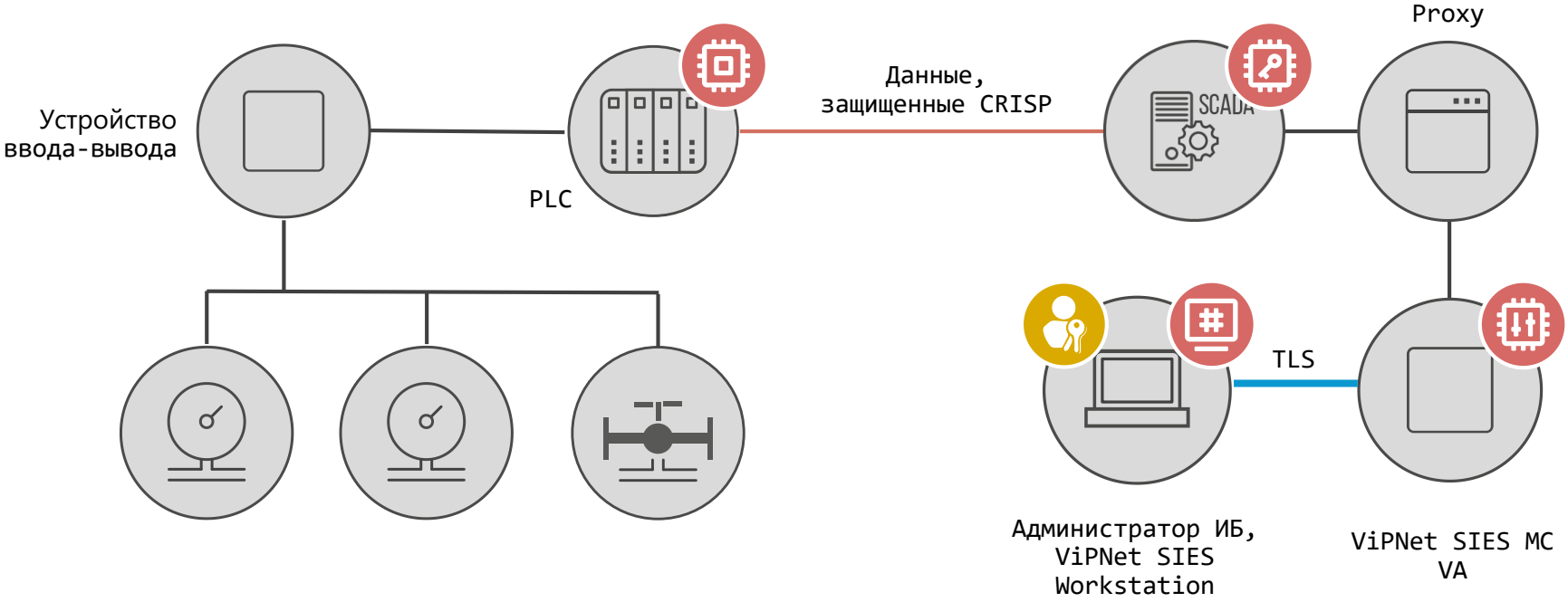
Делаем проект (модифицируем ПО)

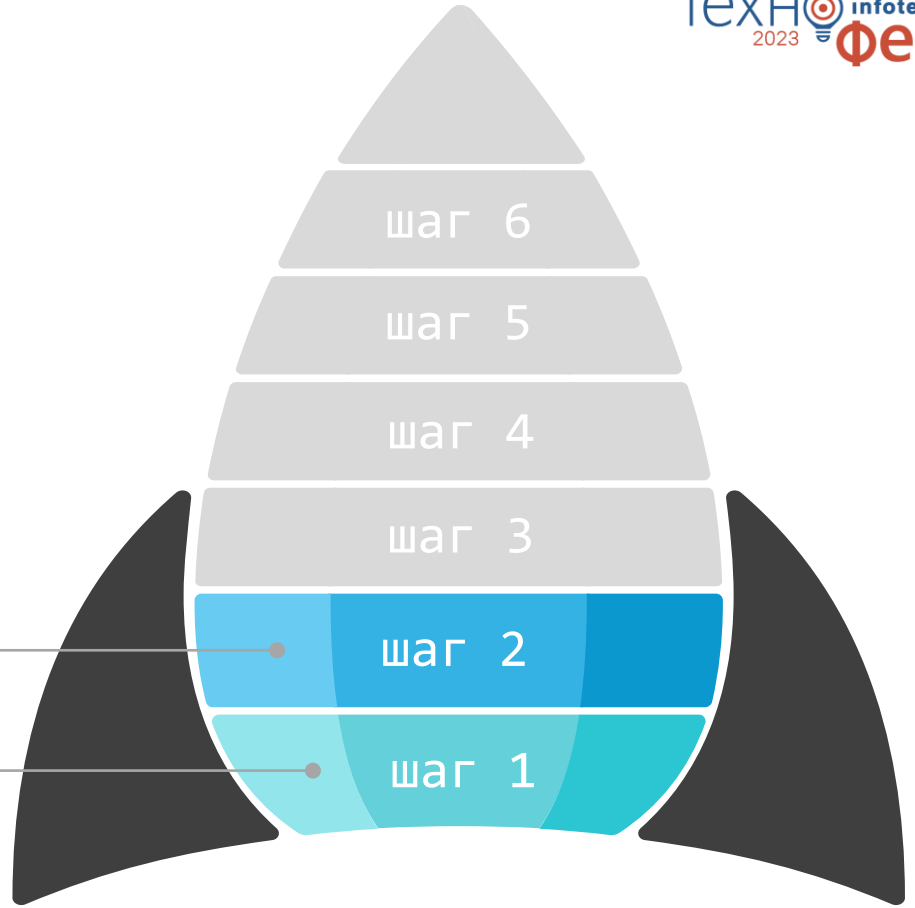


Делаем проект (модифицируем ПО)



Проект пивоваренного завода в защищенном виде




шаг 6
шаг 5
шаг 4
шаг 3
шаг 2
шаг 1
Разворачиваем инфраструктуру
Делаем проект (модифицируем ПО)

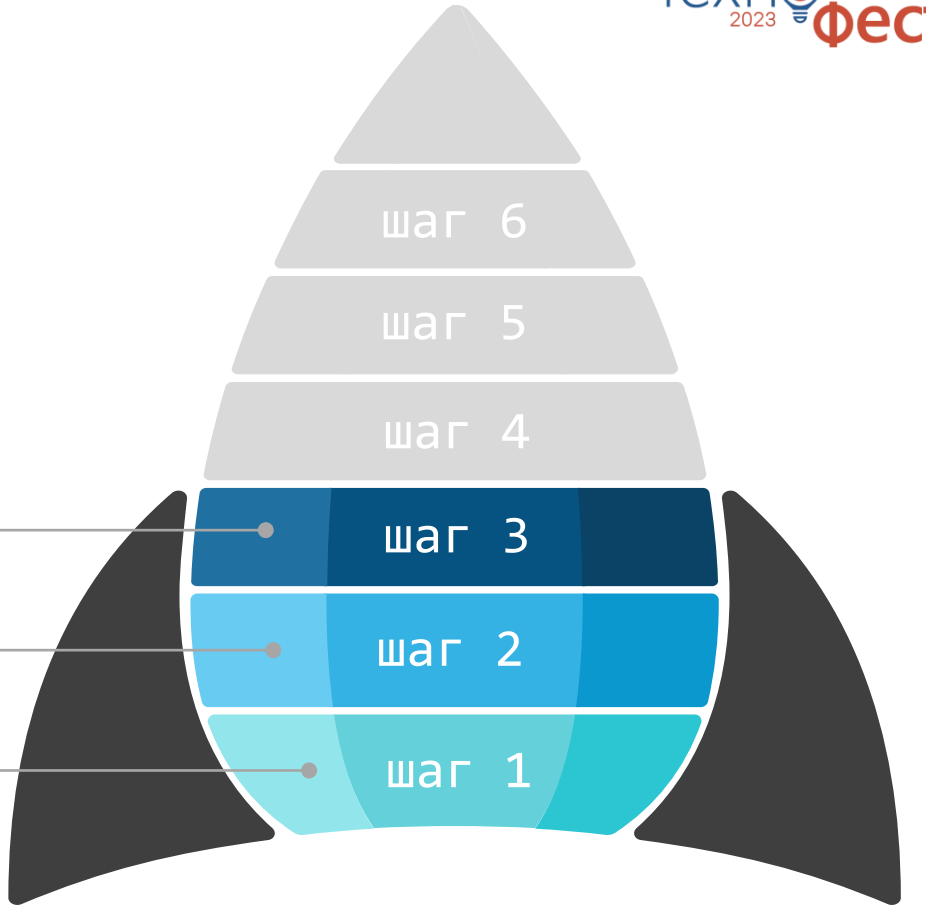
Развертывание инфраструктуры

- Назначение администратора ИБ
- Инициализация ПАК ViPNet SIES MC
- Настройка рабочего места администратора ИБ
- Установка SIES Proxy для проброса управляющих команд

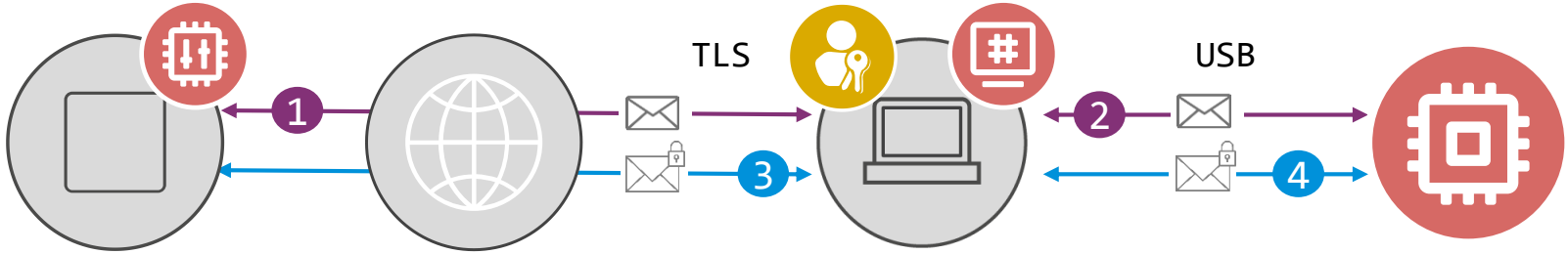
Инициализируем ViPNet SIES Core

Разворачиваем инфраструктуру

Делаем проект (модифицируем ПО)



Инициализация ViPNet SIES Core



ViPNet SIES MC

ViPNet SIES Workstation

ViPNet SIES Core

Начало инициализации

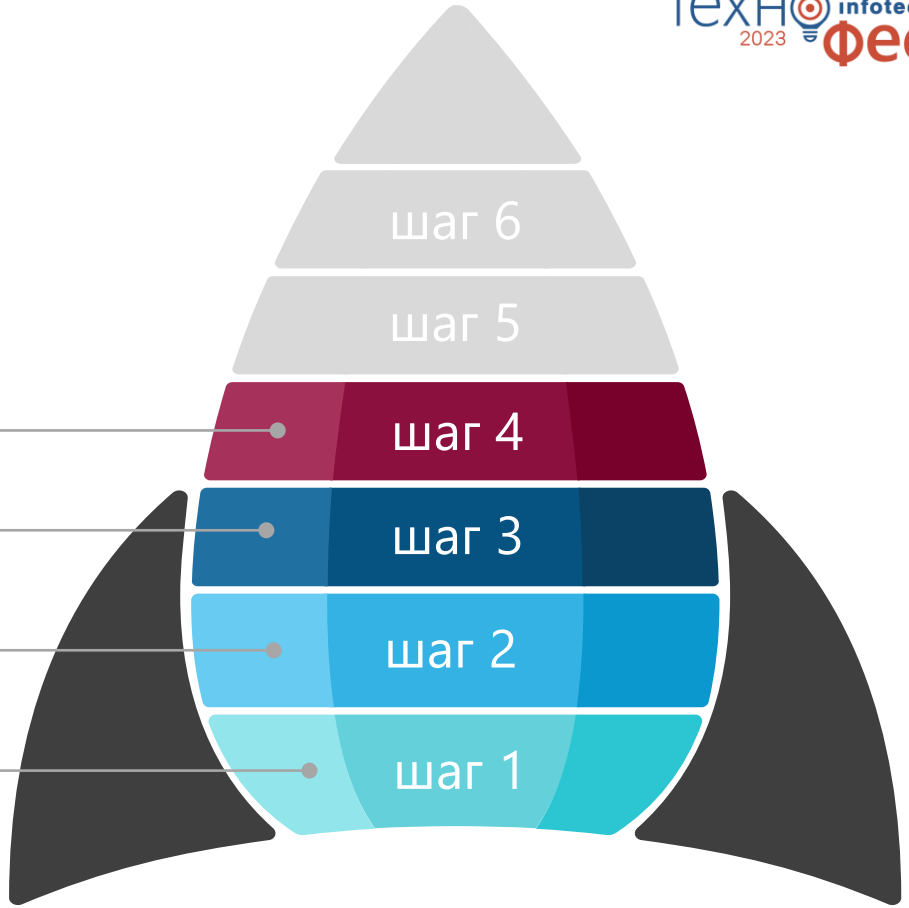
Завершение инициализации

Устанавливаем ViPNet SIES Core

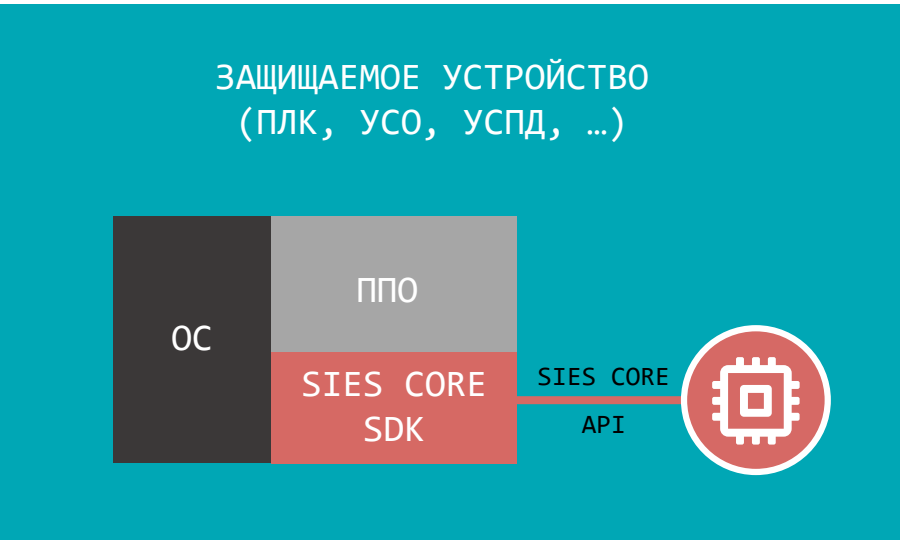
Инициализируем ViPNet SIES Core

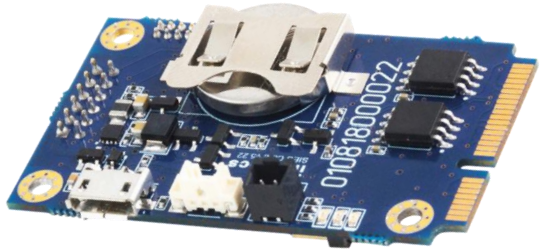
Разворачиваем инфраструктуру

Делаем проект (модифицируем ПО)



Установка ПАК VIPNet SIES Core в ПЛК





- На аппаратном уровне – USB
- На программном уровне – SIES Core API + SDK (RATP+прикладной протокол)

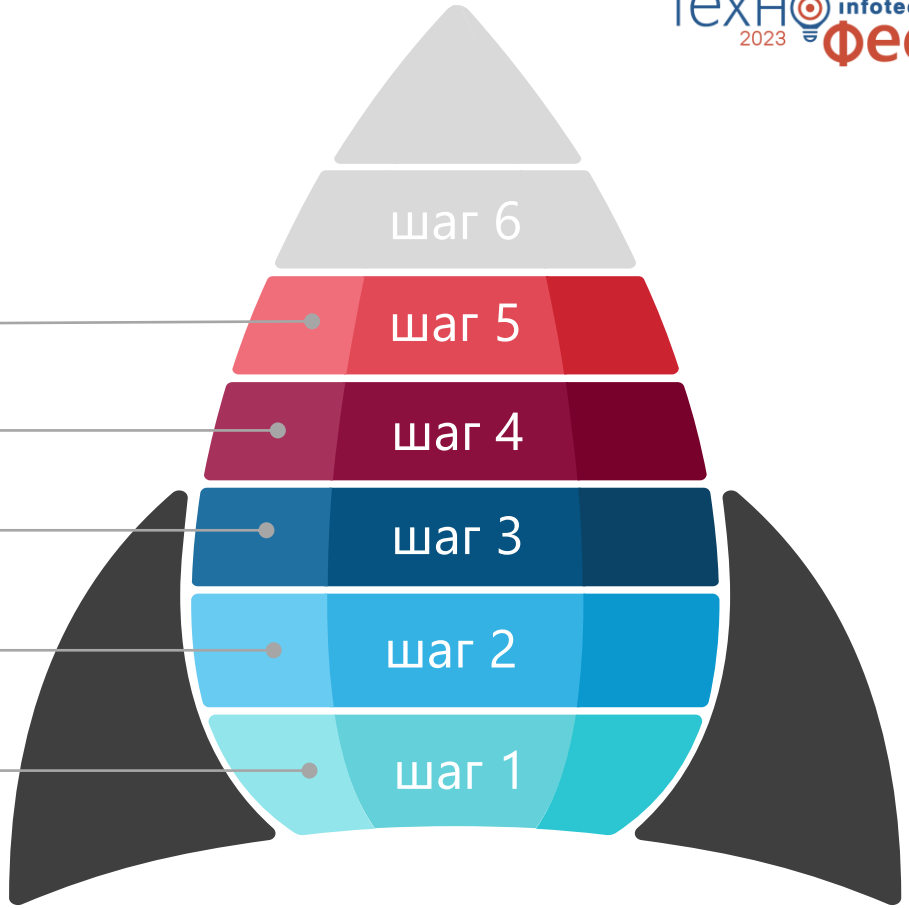
Устанавливаем и инициализируем ViPNet SIES Unit

Устанавливаем ViPNet SIES Core

Инициализируем ViPNet SIES Core

Разворачиваем инфраструктуру

Делаем проект (модифицируем ПО)



Выпускаем ключи

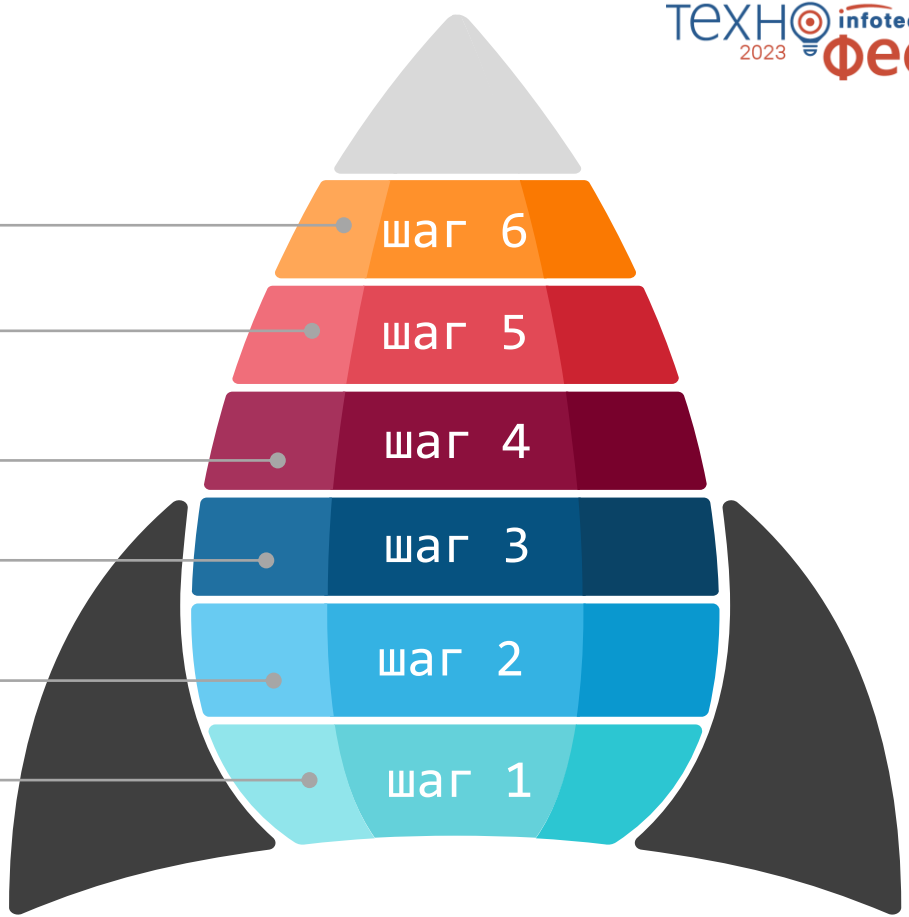
Устанавливаем и инициализируем ViPNet SIES Unit

Устанавливаем ViPNet SIES Core

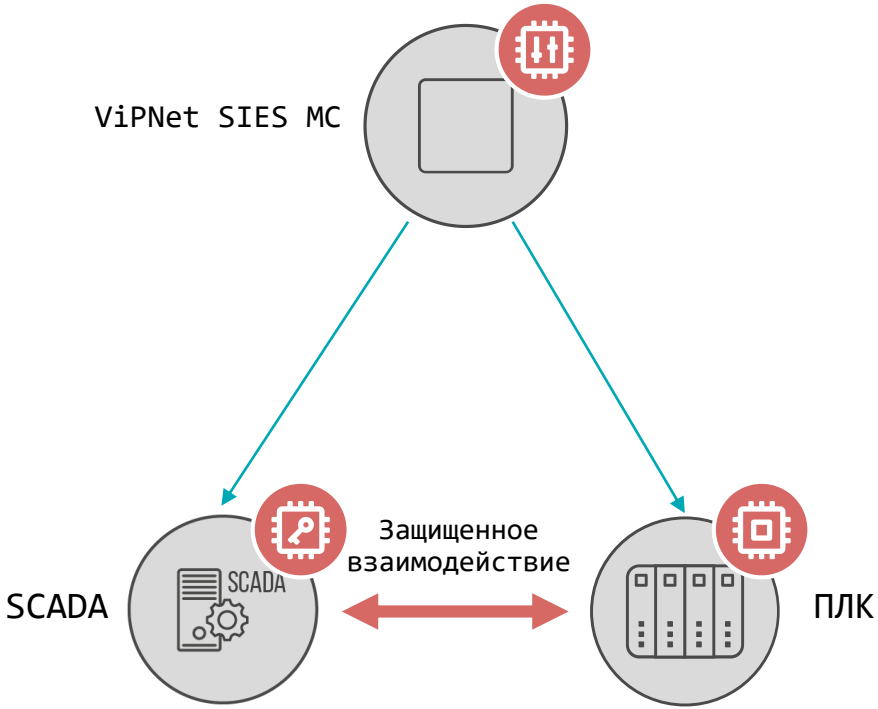
Инициализируем ViPNet SIES Core

Разворачиваем инфраструктуру

Делаем проект (модифицируем ПО)



Загрузка ключей



1. Задание связей между устройствами
2. Синхронизация связей
3. Загрузка ключей

Технологический процесс защищен.

Злоумышленник не может влиять на процесс и не может отключить функцию защиты.

Спасибо за внимание!

Алексей Власенко

Aleksey.Vlasenko@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363