

# Мастер-класс по разворачиванию решения ViPNet SIES



техно infotecs  
2023 Фест  
ТЕХНИЧЕСКАЯ  
КОНФЕРЕНЦИЯ

Андрей Иванов  
архитектор решений

# Решение ViPNet SIES

## Решение ViPNet SIES

Встраиваемые средства  
криптографической защиты  
информации (СКЗИ):

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



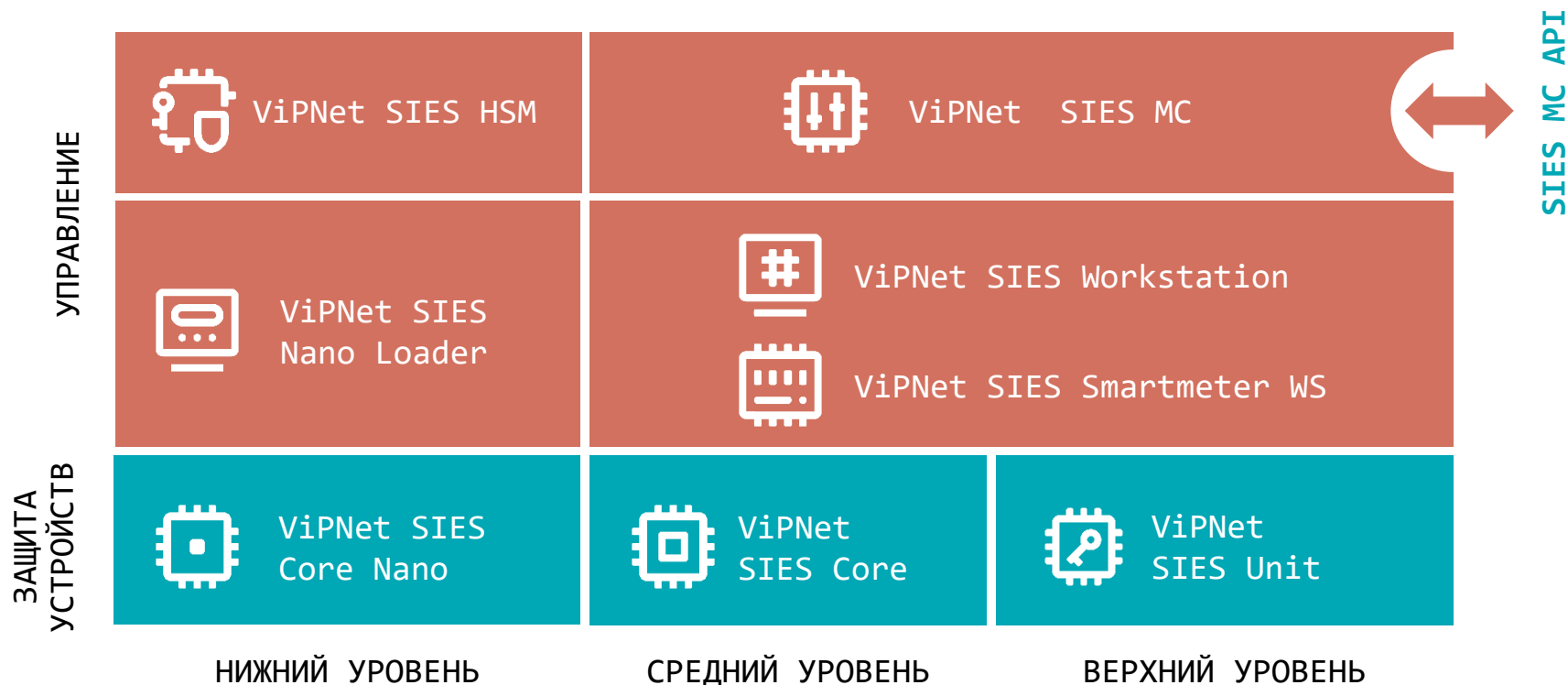
SECURITY FOR  
INDUSTRIAL AND  
EMBEDDED  
SOLUTIONS

# Криптографические сервисы для защищаемых устройств

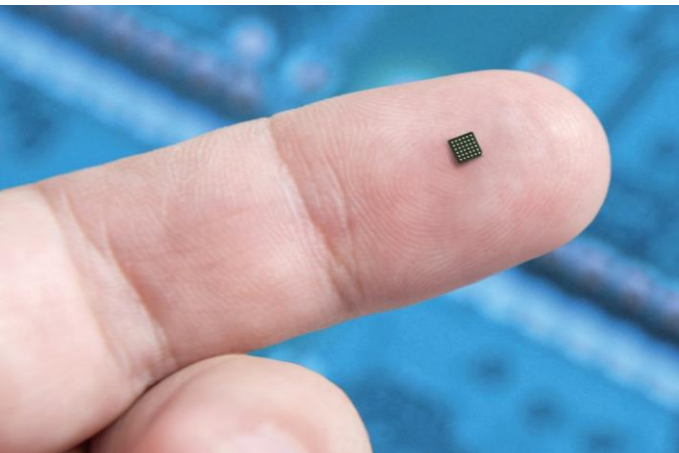


- Зашифрование/расшифрование по CRISP (ГОСТ 34.12-2018, ГОСТ 34.13-2018)
- Создание/проверка имитовставки по CRISP (ГОСТ 34.12-2018, ГОСТ 34.13-2018)
- Создание/проверка ЭП в CMS (ГОСТ 34.10-2018)
- Зашифрование/расшифрование в CMS (ГОСТ 28147-89)
- Создание/проверка хэш (ГОСТ 34.11-2018)

# 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

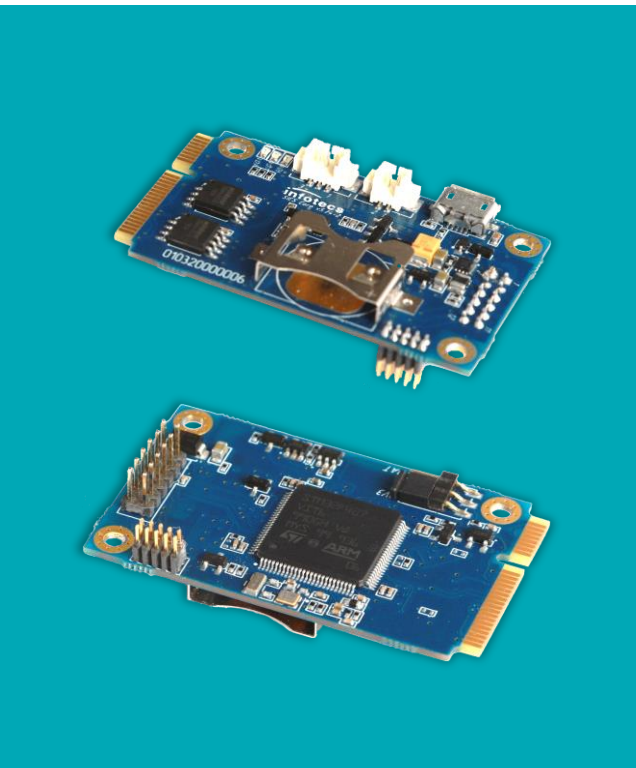
## Функциональные особенности:

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

## Соответствие требованиям:

- СКЗИ класса КСЗ
- 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

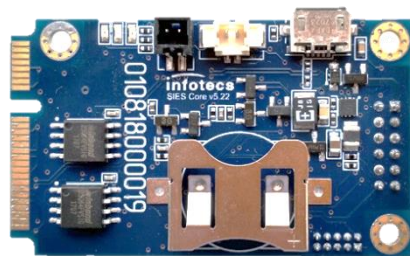
## Функциональные особенности:

- 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°C

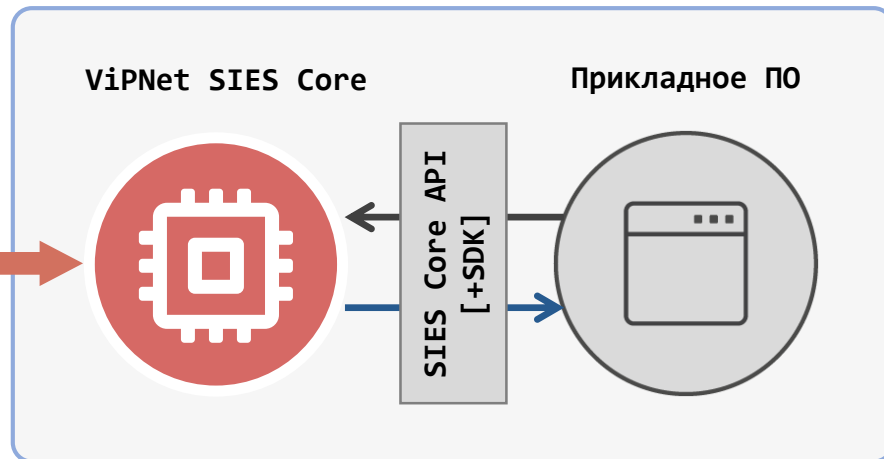
## Соответствие требованиям:

- 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)



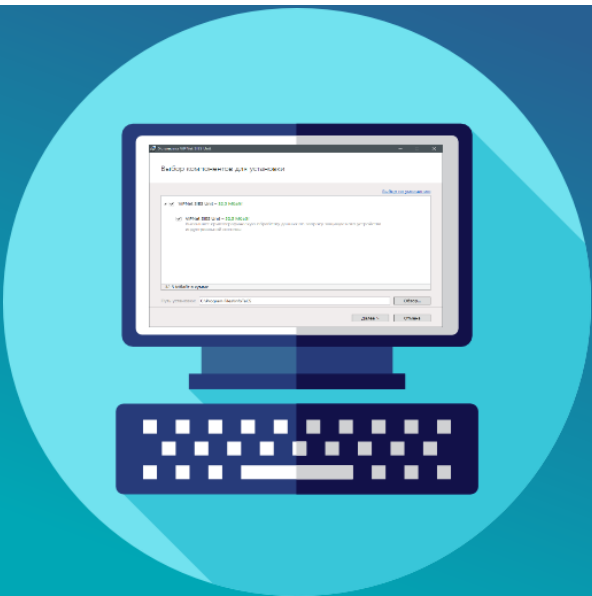
Данные



Защищенные данные



# 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

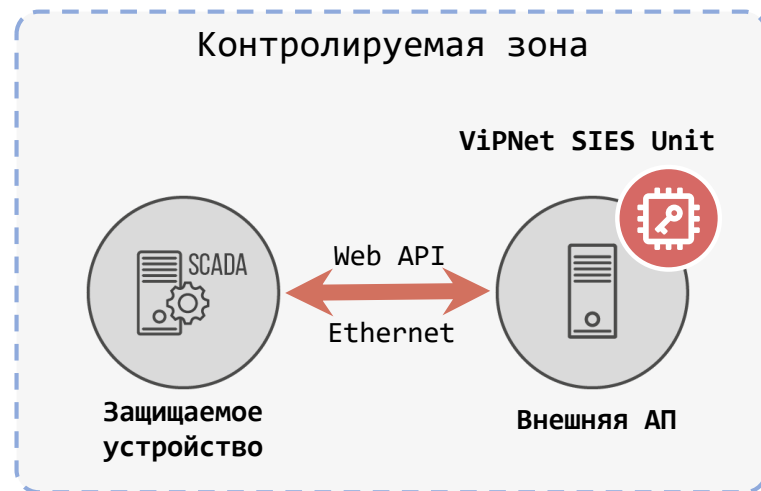
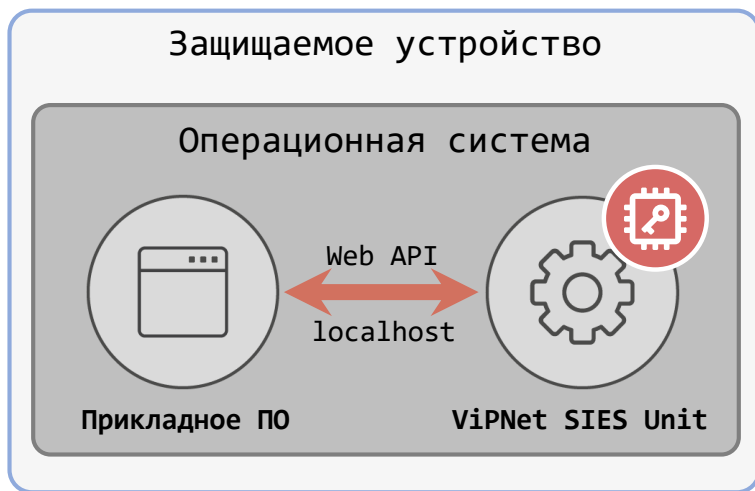
## Функциональные особенности:

- 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

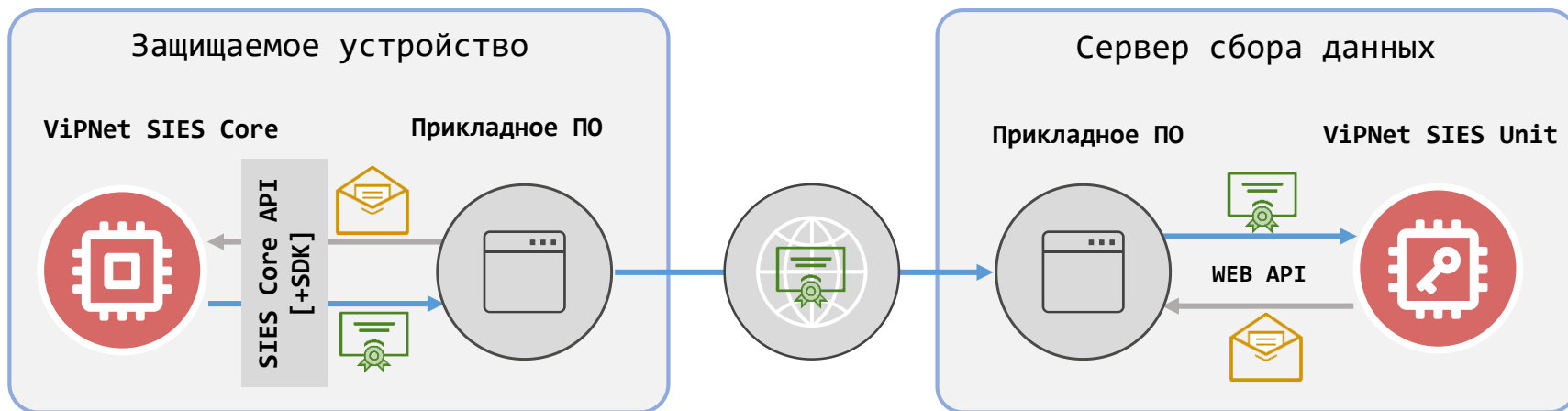
## Соответствие требованиям:

- СКЗИ класса КС1 и КС3

# Интеграция ViPNet SIES Unit



# Защита коммуникаций с помощью ViPNet SIES



Защищенные данные



Незащищенные данные

# 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



Доступ к интерфейсу по WebUI

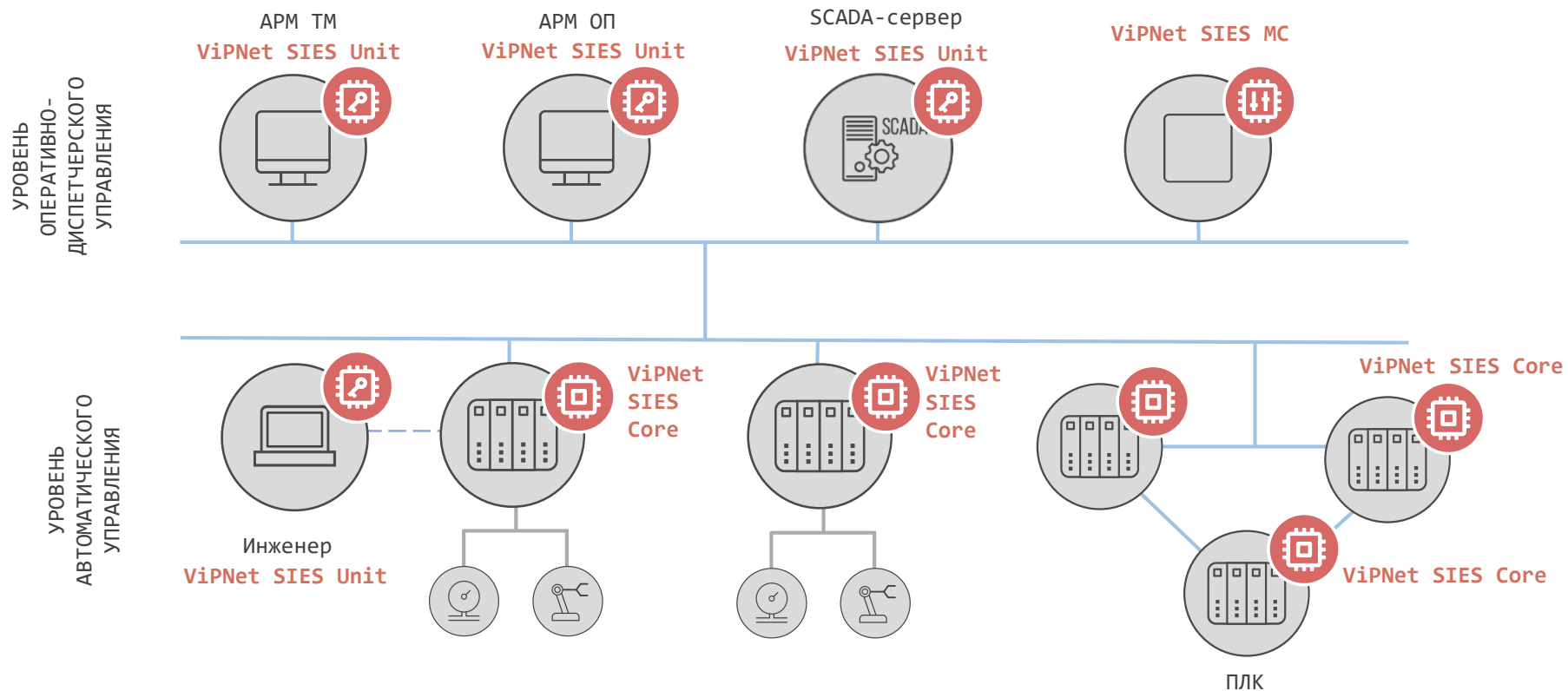


API для подключения и управления сторонними СКЗИ



Сертификат СКЗИ класса КС3 и КС1

# Защищенная АСУ ТП



# Защищенная IIoT/ИСУЭ система

Защищенные  
IIoT- устройства с  
**SIES Core/Core Nano**

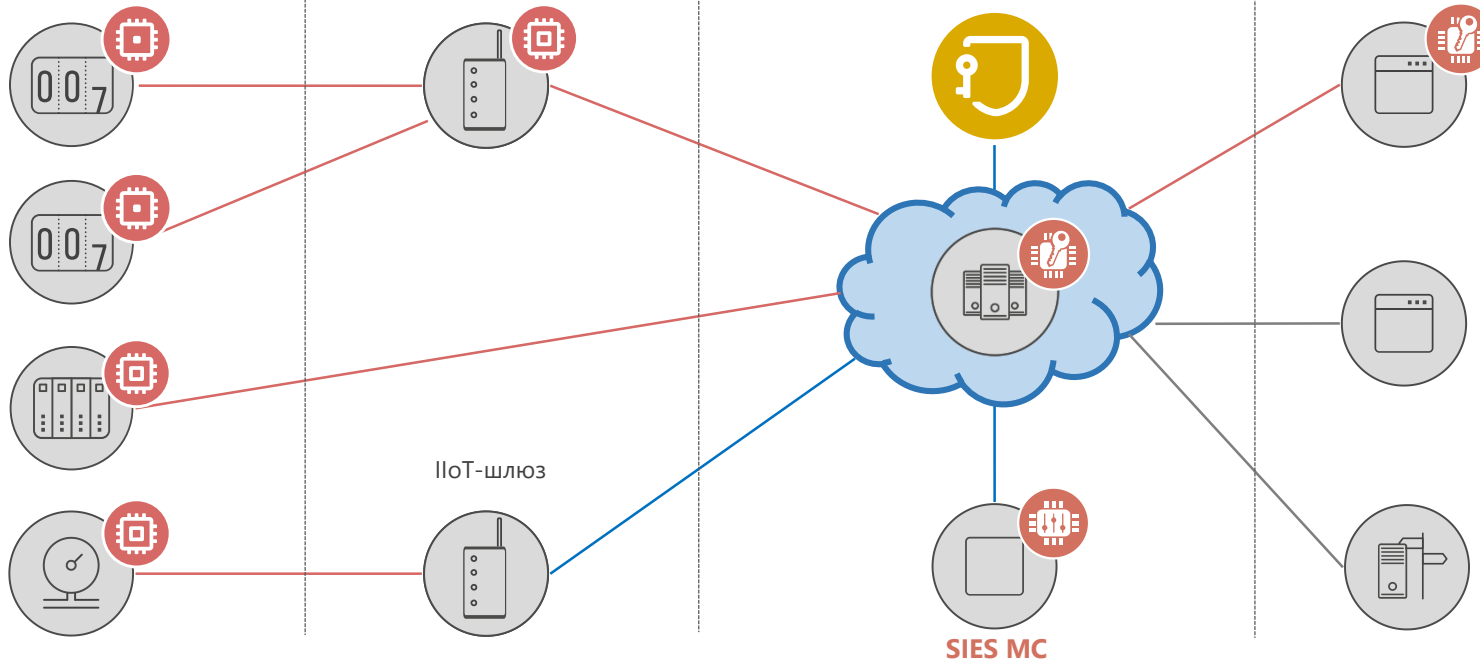
УСПД с  
**SIES Core**

**SIES HSM**

Сервисный инженер с  
**SIES Unit**

Бизнес-приложения

Сторонние системы



Защищенные данные

Защищенные каналы (VPN)

Открытые каналы



## Рекомендация по стандартизации РФ: Р 1323565.1.029-2019. Протокол защищенного обмена CRISP

Протокол защищенной передачи данных для  
индустриальных систем, M2M и IIoT

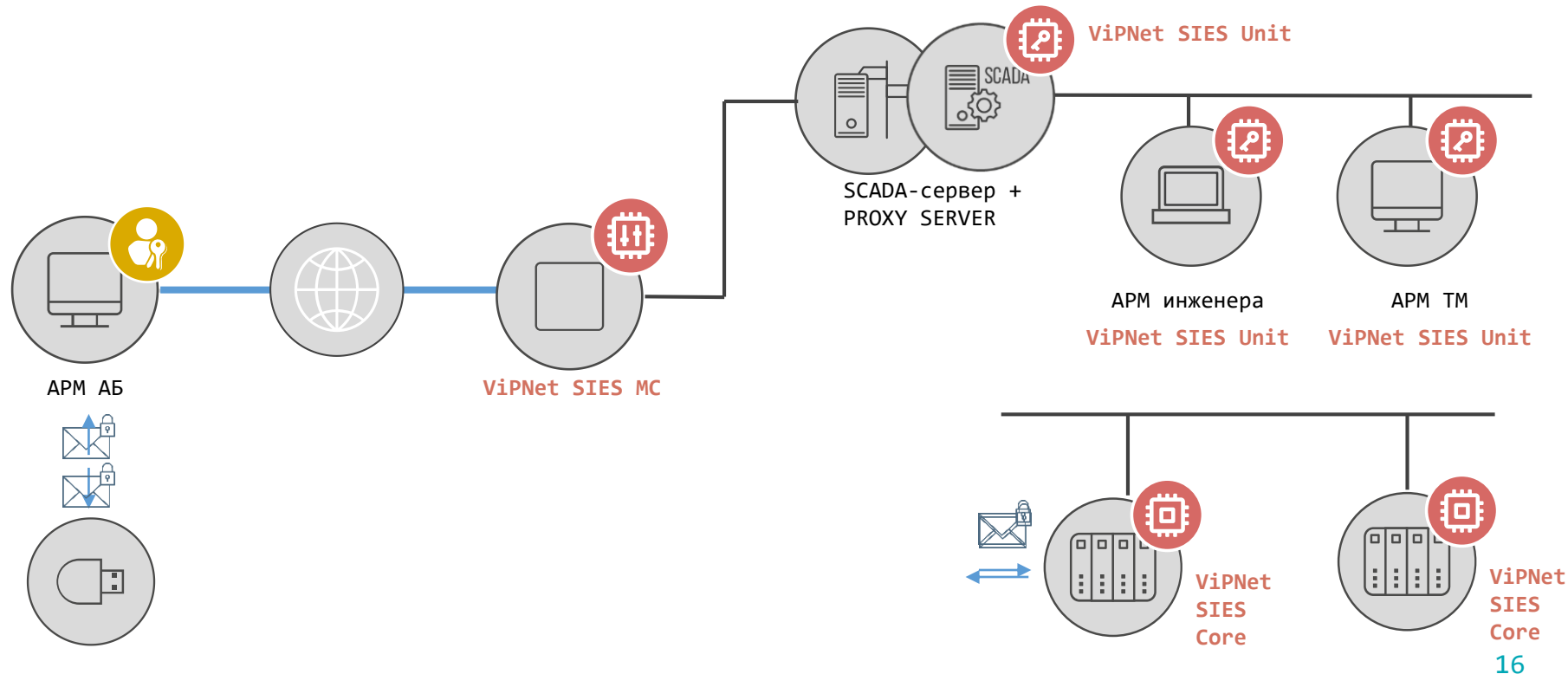


PLC



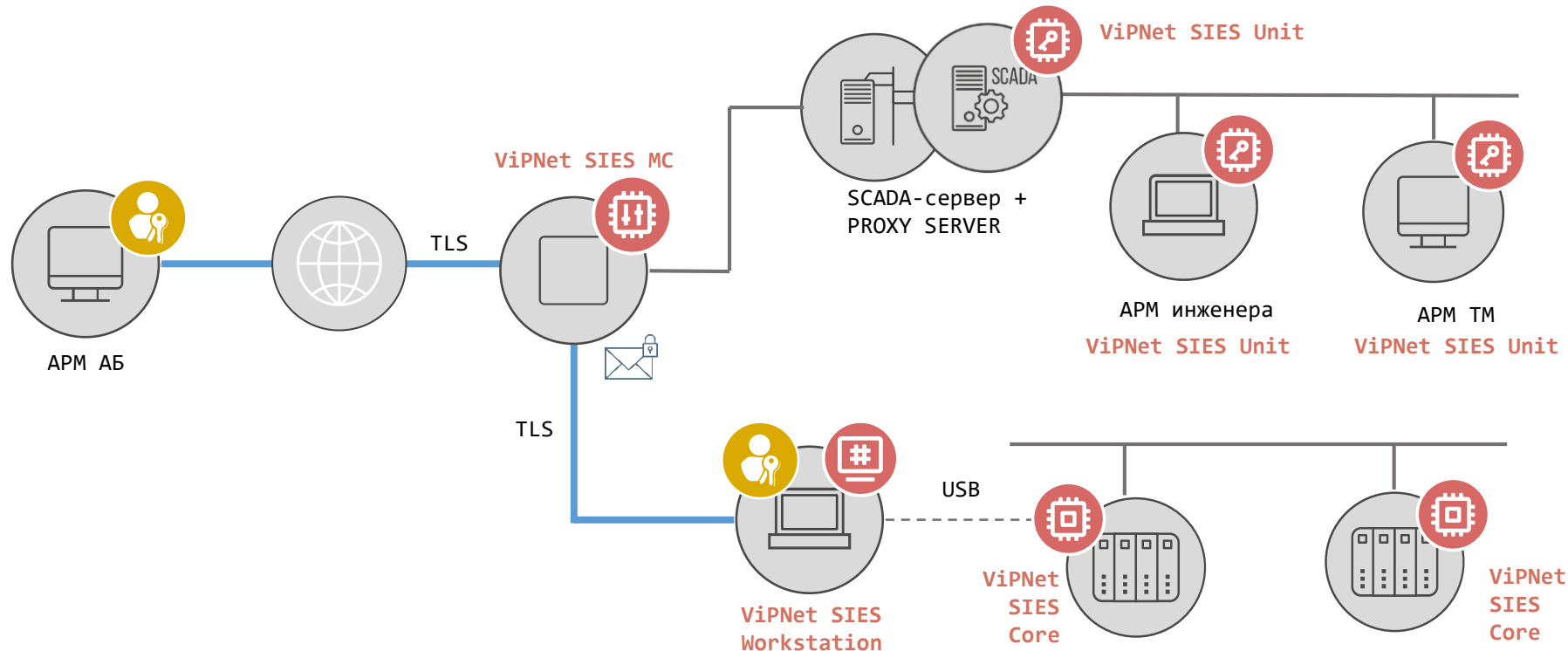
- Обеспечение целостности
- Обеспечение конфиденциальности (опционально)
- Защита от навязывания повторных сообщений
- Поддержка адресных (один-к-одному) сообщений
- Поддержка многоадресных (один-ко-многим, подписочная модель) сообщений
- Минимальные накладные расходы

# Защищенный обмен с SIES-узлами при отсутствии канала связи





# Защищенный обмен с SIES-узлами при отсутствии канала связи

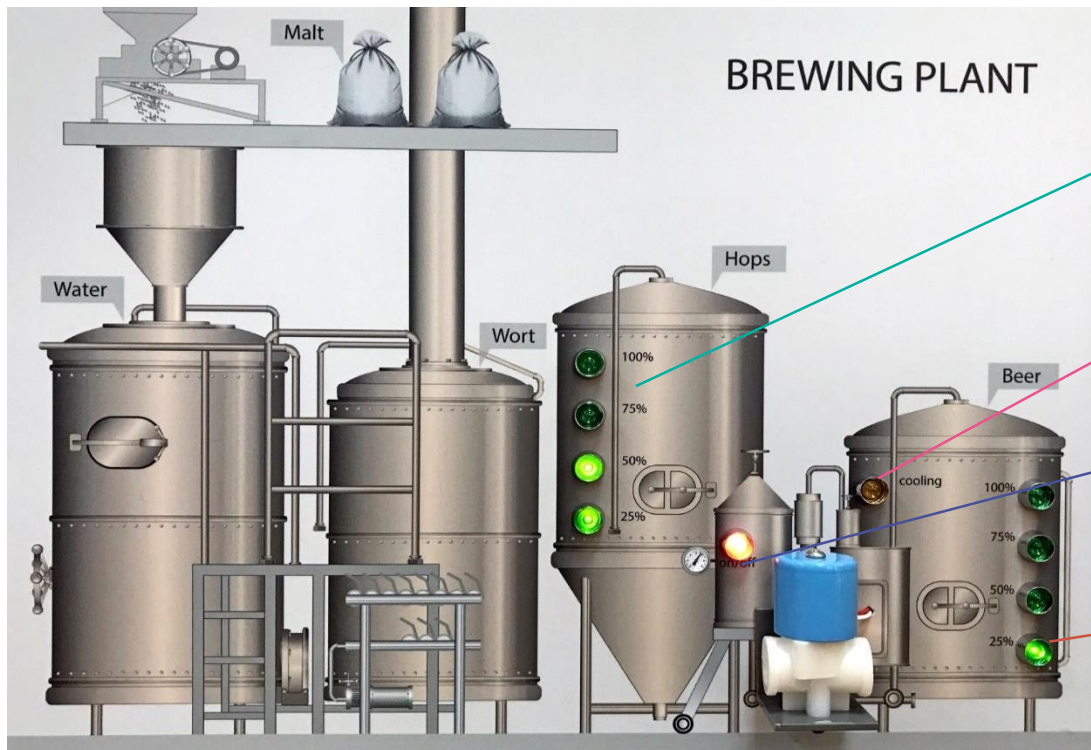


# АСУ «Пивоваренный завод»

# Технологический процесс пивоварения



# Технологический процесс пивоварения



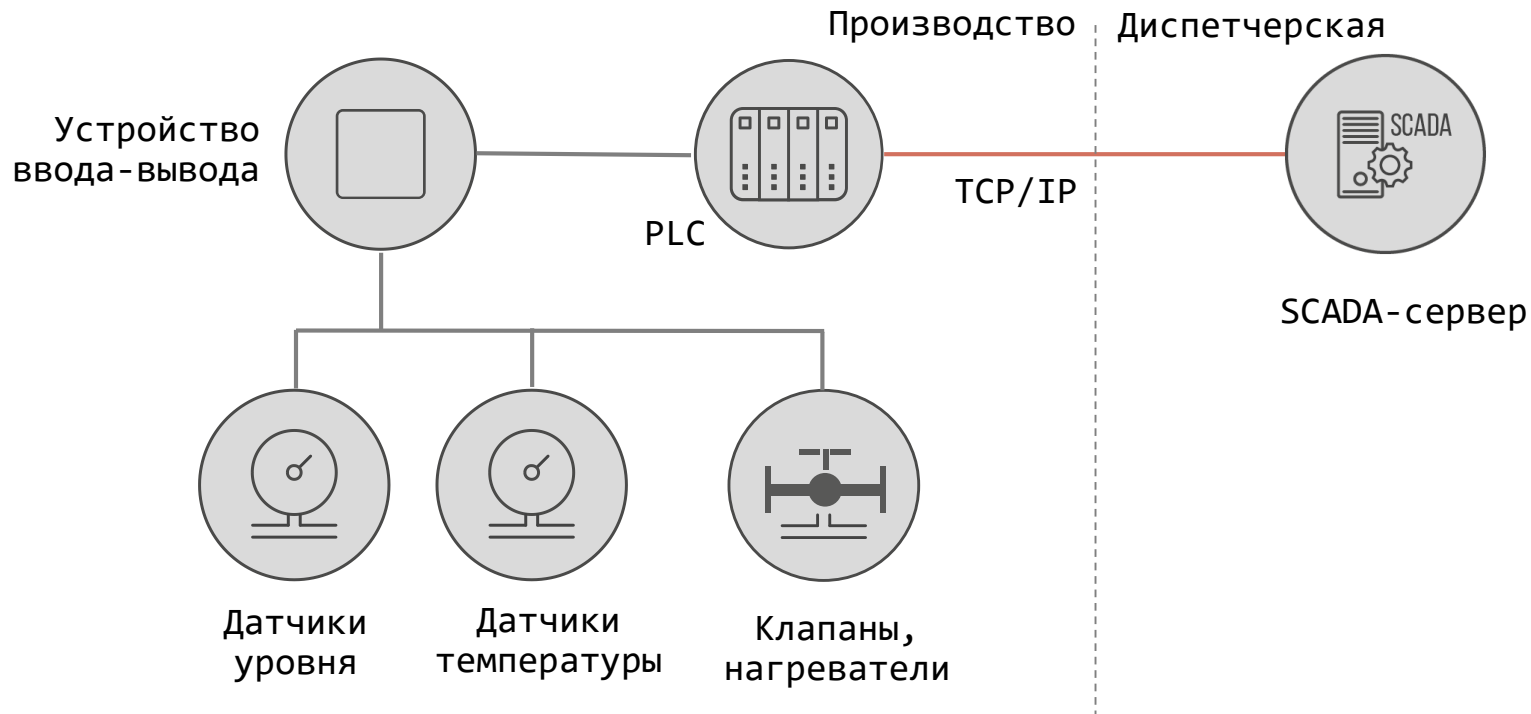
Уровень сусла

Режим  
охлаждения

Состояние  
клапана  
перекачки

Уровень  
ГОТОВОГО  
ПИВА

# Пивоваренный завод

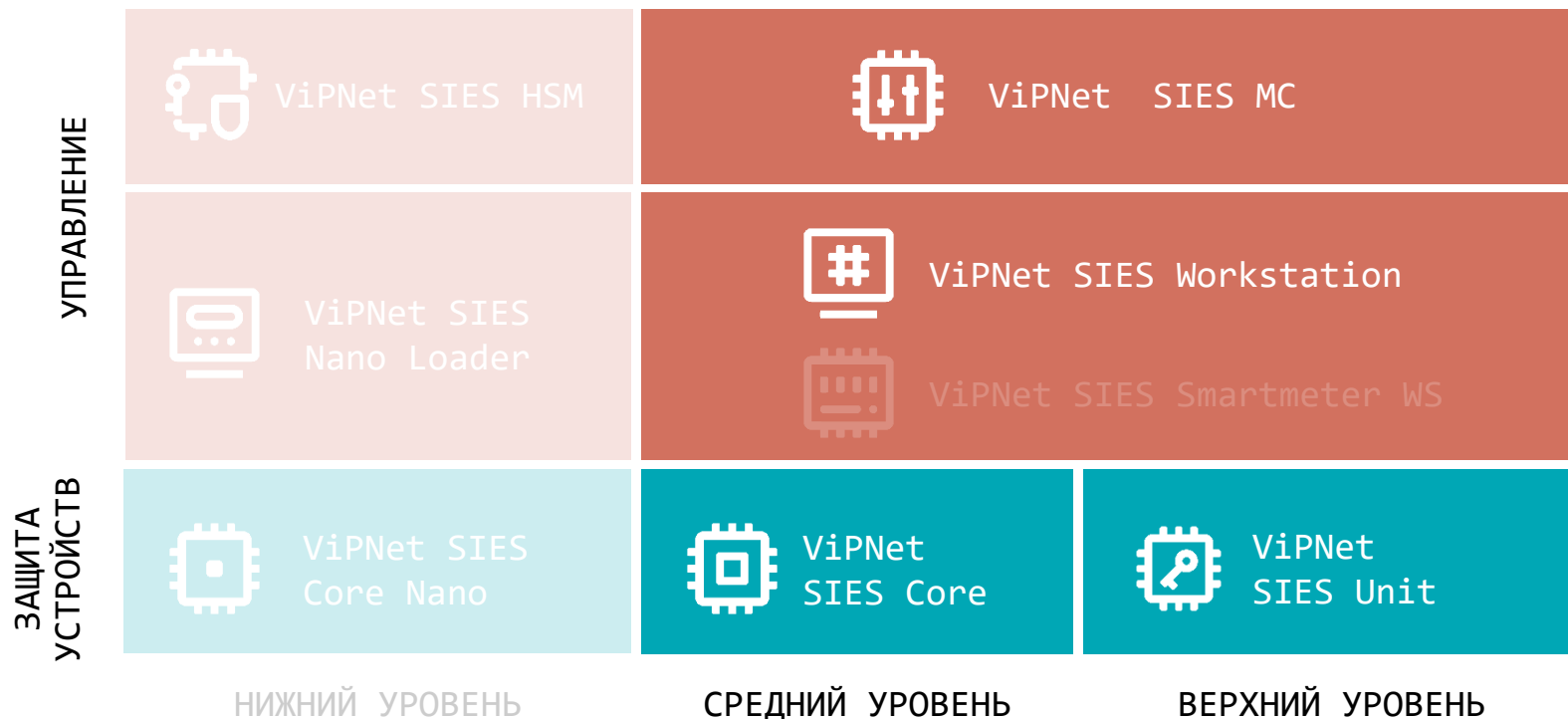


# Внутренний нарушитель!!!

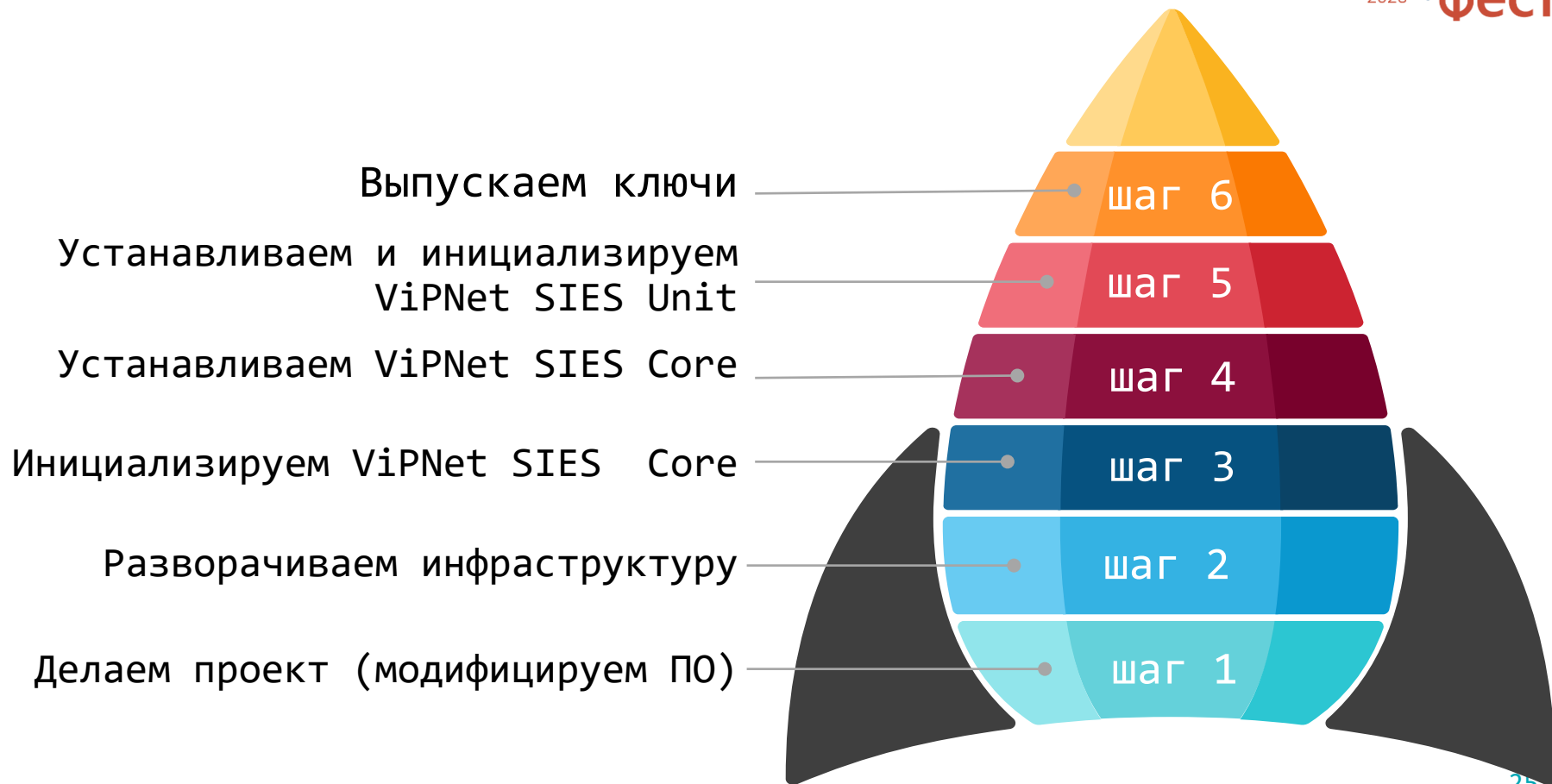
Кто-то украл наш SCADA-проект  
и сливает все пиво,  
как только оно готово.

# Разворачивание решения ViPNet SIES

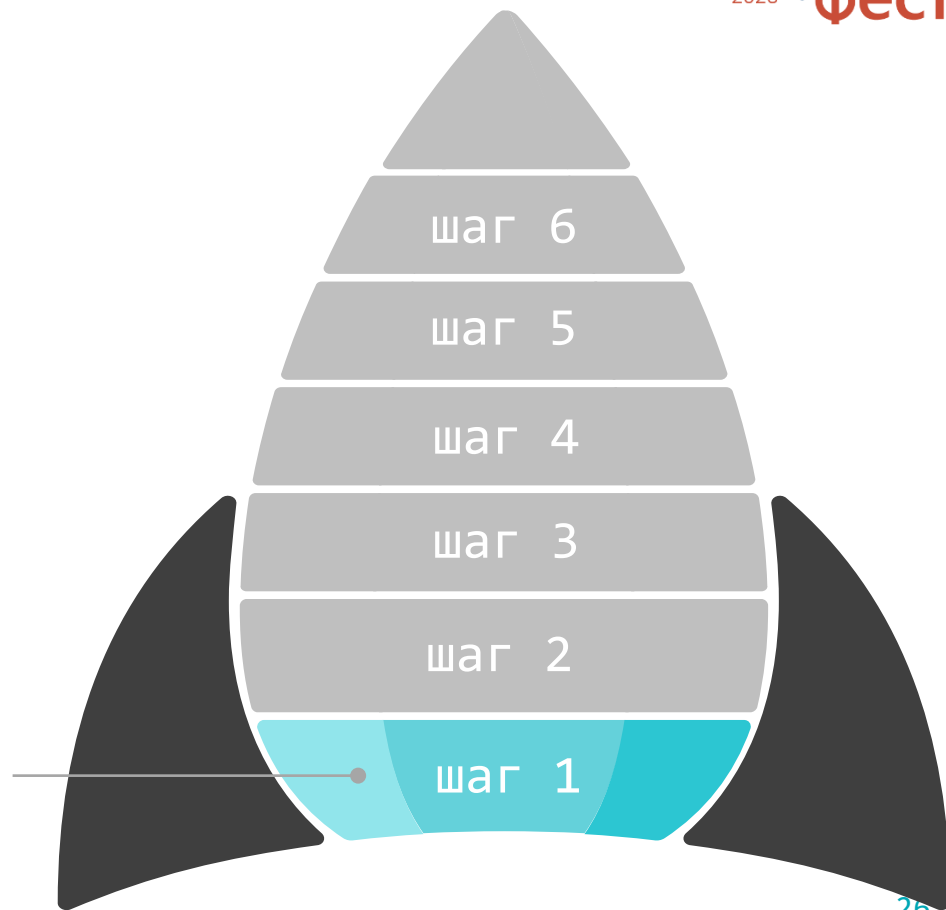
# Состав решения ViPNet SIES



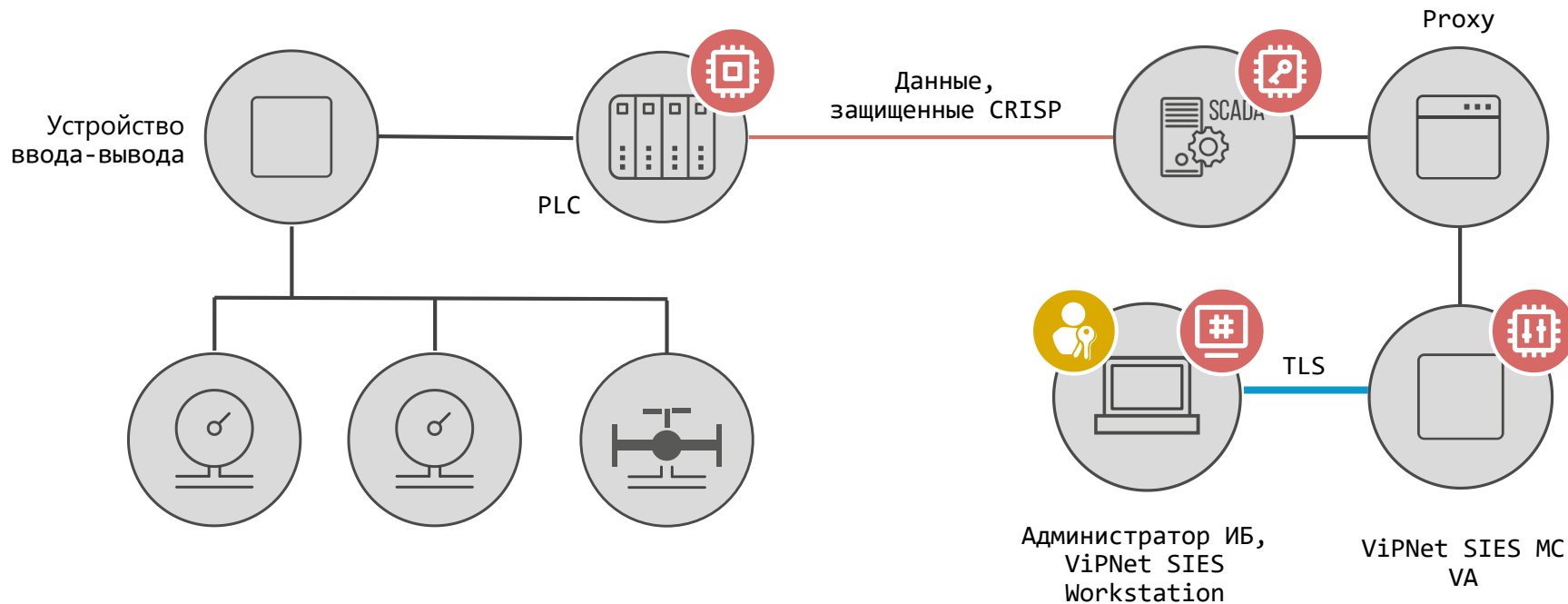


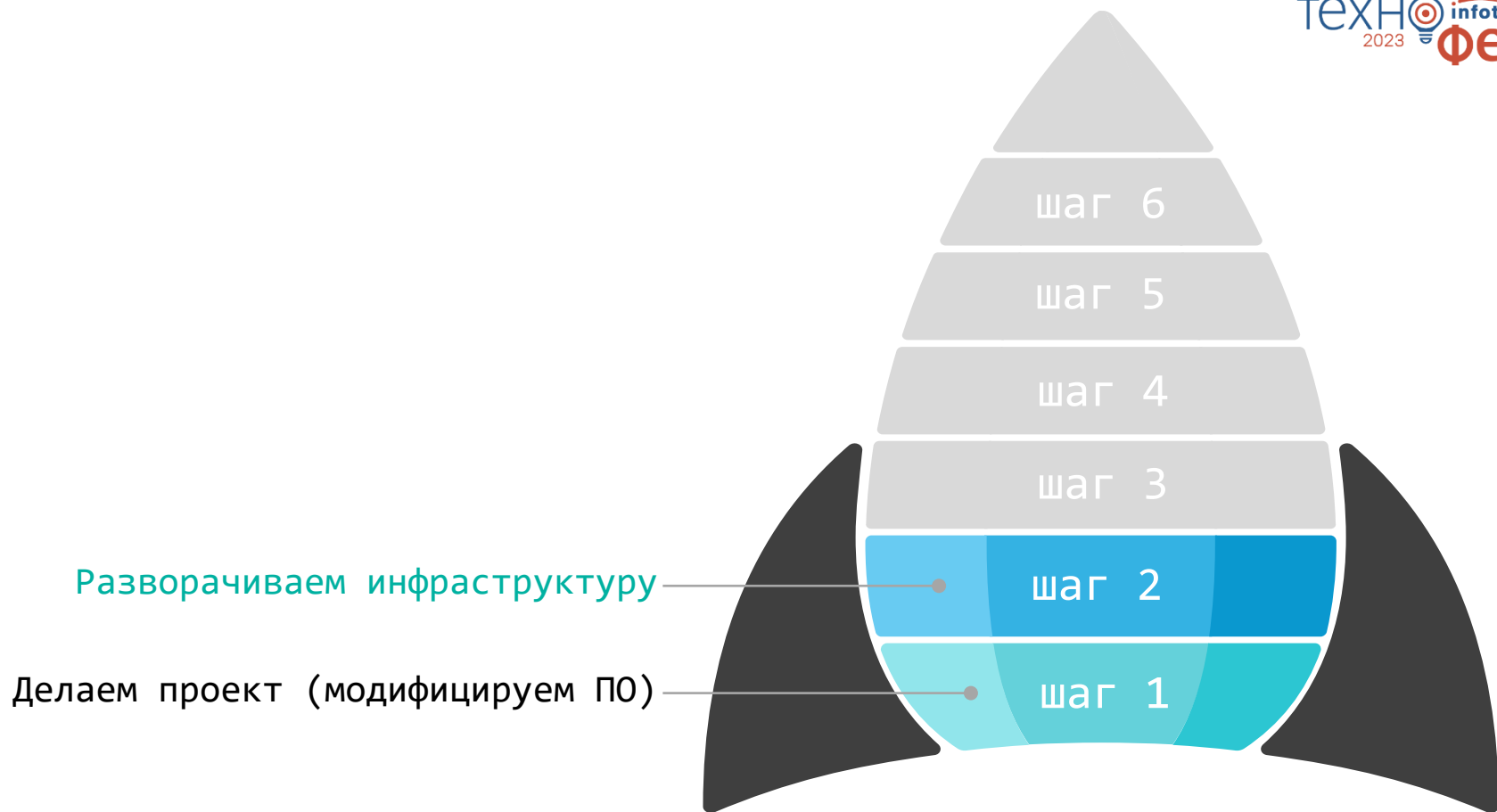


Делаем проект (модифицируем ПО)



# Проект пивоваренного завода в защищенном виде





# Развертывание инфраструктуры



Назначение администратора ИБ



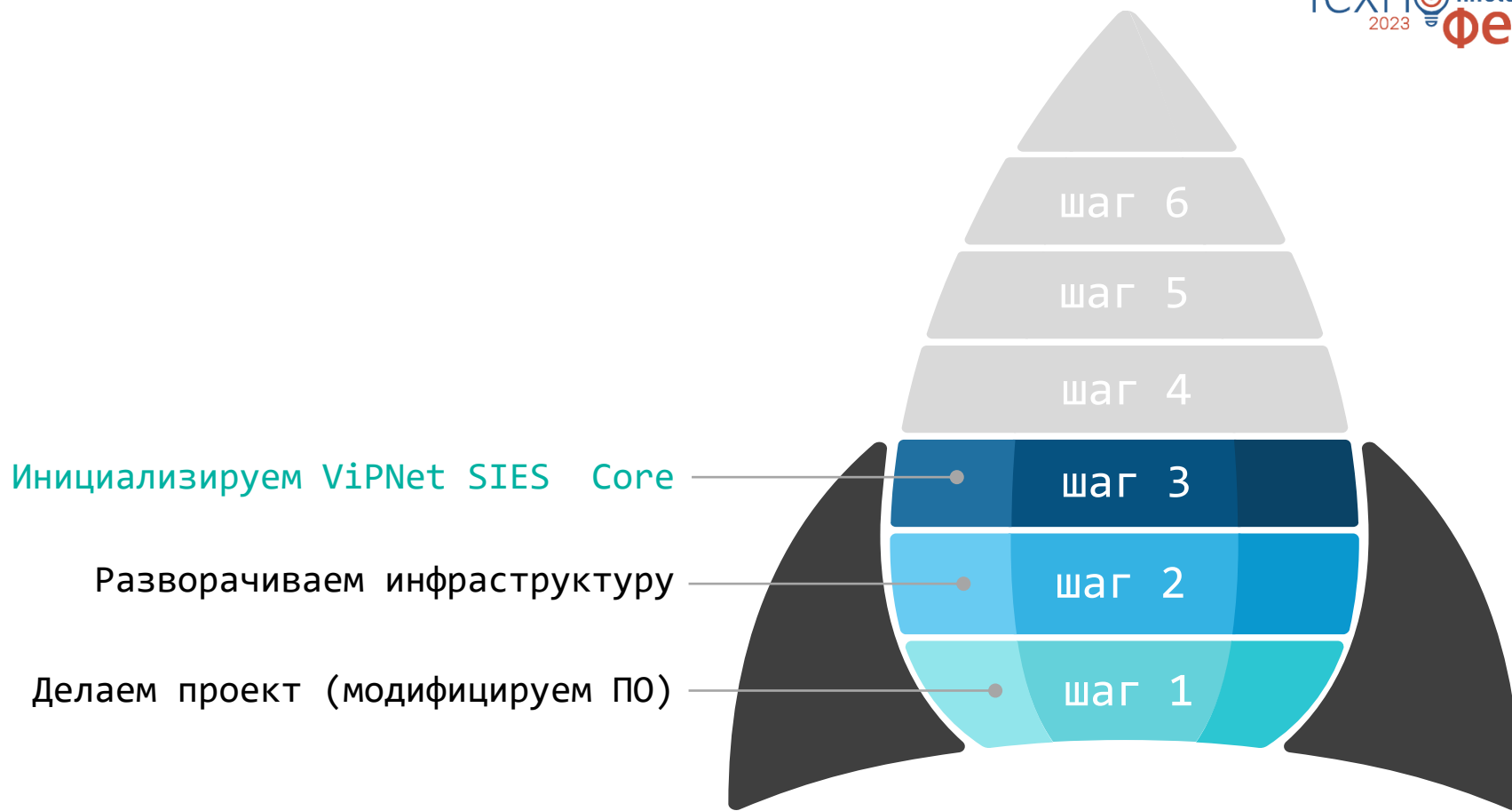
Инициализация ПАК VipNet SIES MC



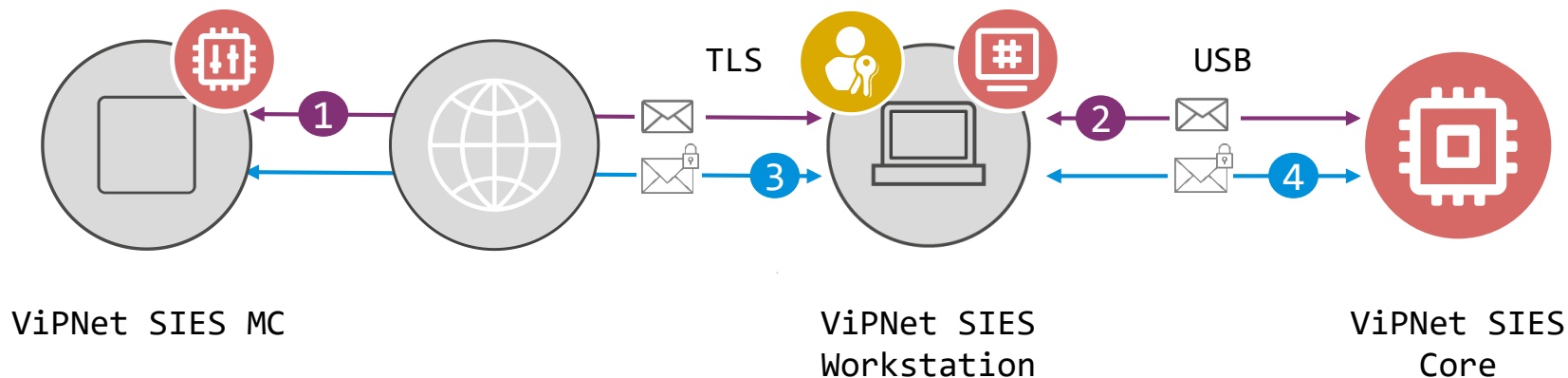
Настройка рабочего места администратора ИБ



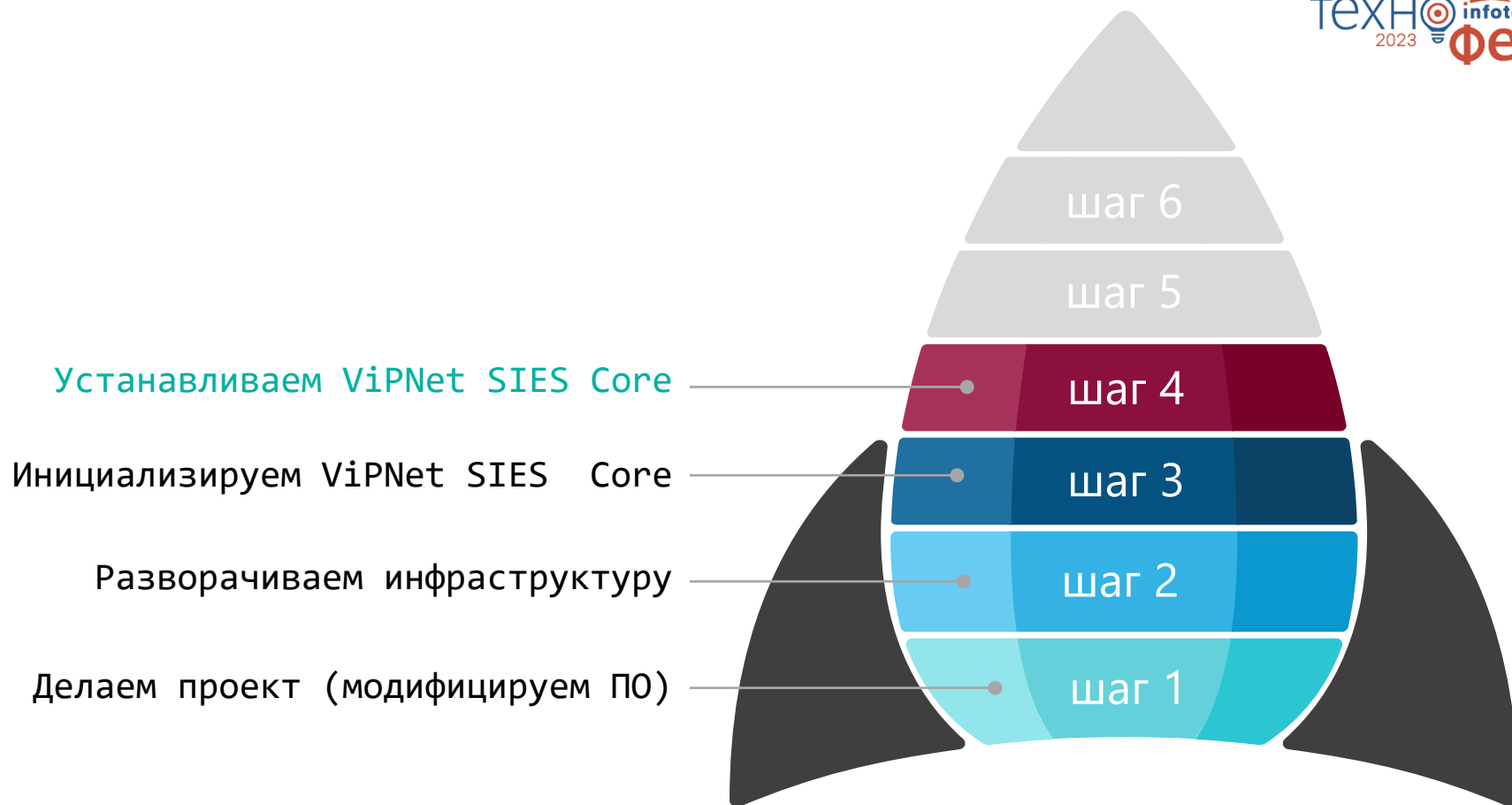
Установка SIES Proxu для проброса управляющих команд



# Инициализация ViPNet SIES Core



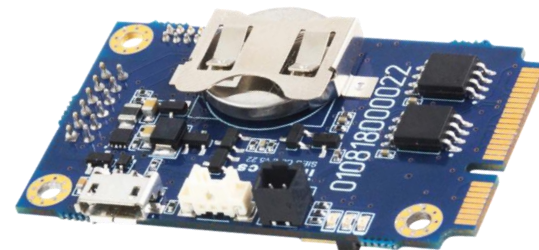
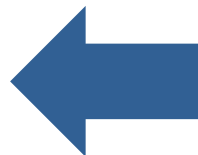
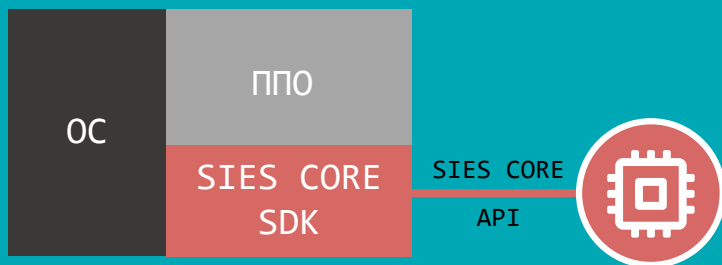
- Начало инициализации
- Завершение инициализации



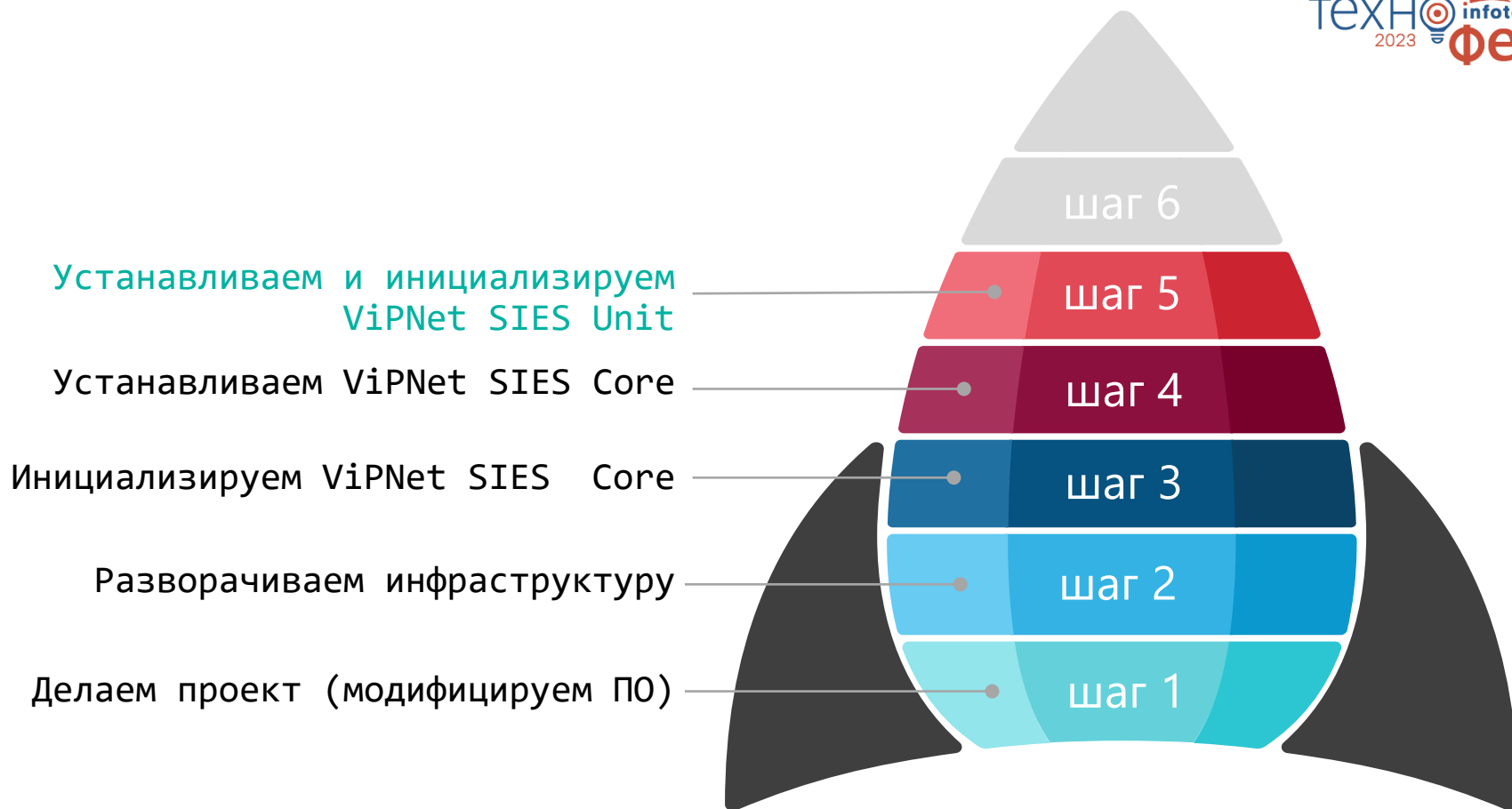


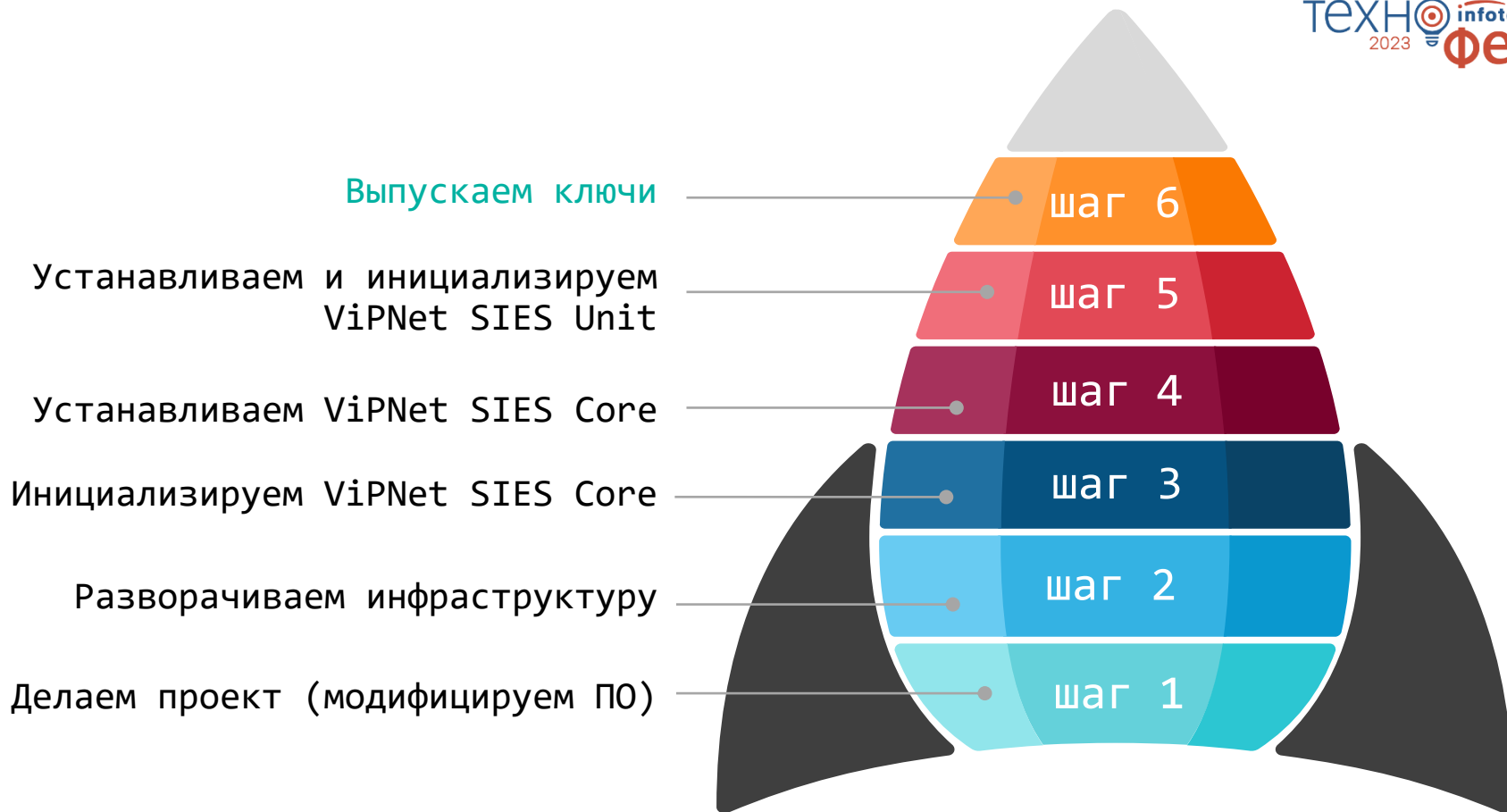
# Установка ПАК VIPNet SIES Core в ПЛК

ЗАЩИЩАЕМОЕ УСТРОЙСТВО  
(ПЛК, УСО, УСПД, ...)

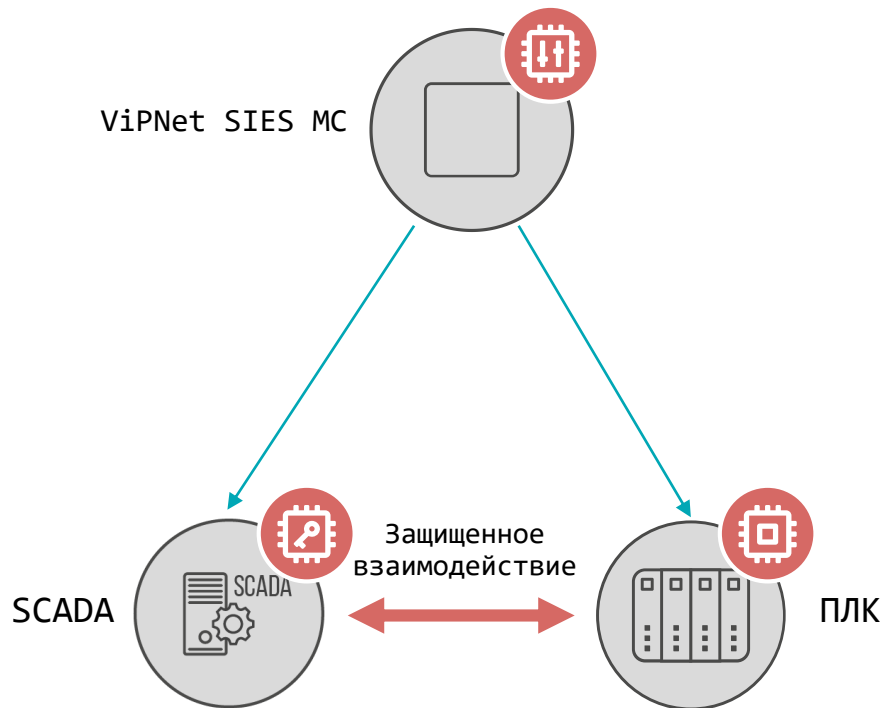


- На аппаратном уровне – USB
- На программном уровне – SIES Core API + SDK (RATP+прикладной протокол)





# 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!

Андрей Иванов

[Andrey.Ivanov2@infotecs.ru](mailto:Andrey.Ivanov2@infotecs.ru)

---

Подписывайтесь на наши соцсети



[vk.com/infotecs\\_news](https://vk.com/infotecs_news)



[https://t.me/infotecs\\_official](https://t.me/infotecs_official)



[rutube.ru/channel/24686363](https://rutube.ru/channel/24686363)