

Мастер-класс по разворачиванию решения ViPNet SIES

Алексей Власенко
Ведущий менеджер продуктов

техно infotecs
2022 Фест

ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

Решение ViPNet SIES

Решение ViPNet SIES

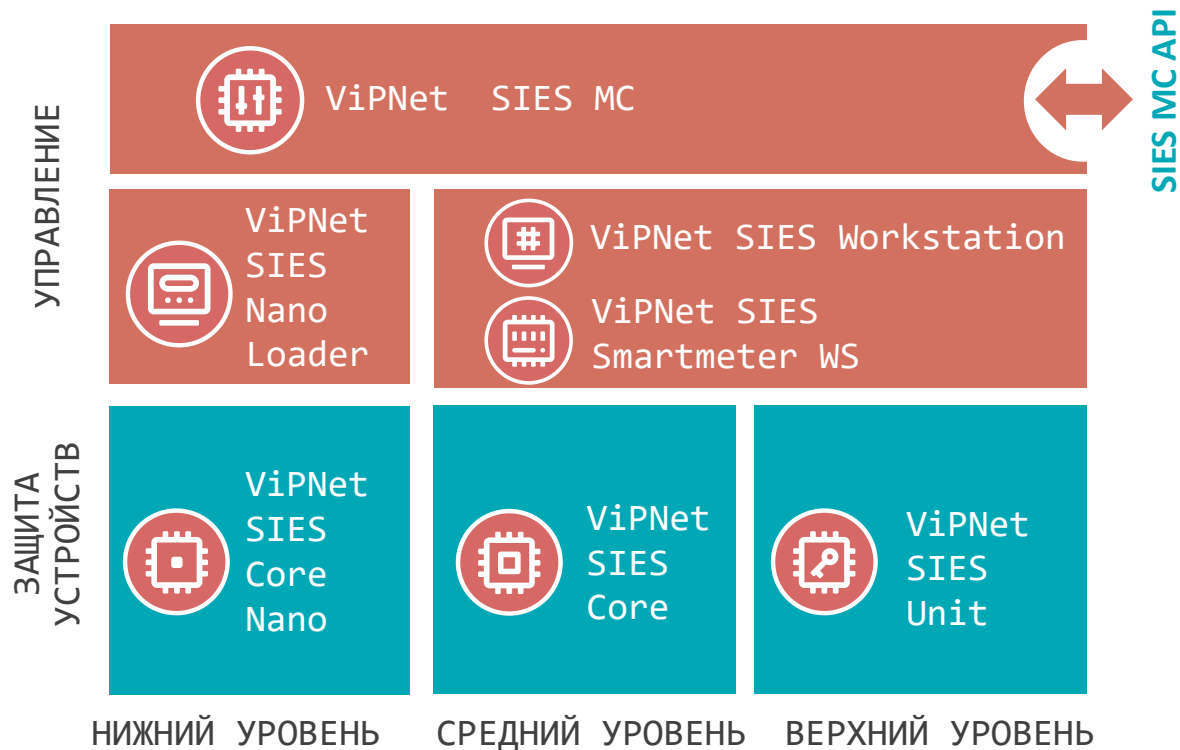
Встраиваемые криптографические средства защиты информации:

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



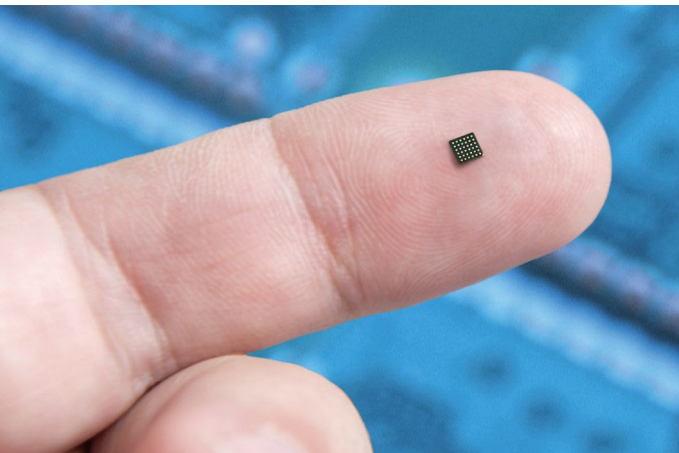
SECURITY FOR
INDUSTRIAL AND
EMBEDDED SOLUTIONS

Состав решения ViPNet SIES



- СКЗИ класса КС1 и КС3 по требованиям ФСБ России
- Возможность использования криптографии на разных по вычислительной мощности устройствах
- Нет зависимости от ОС и архитектуры устройств

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

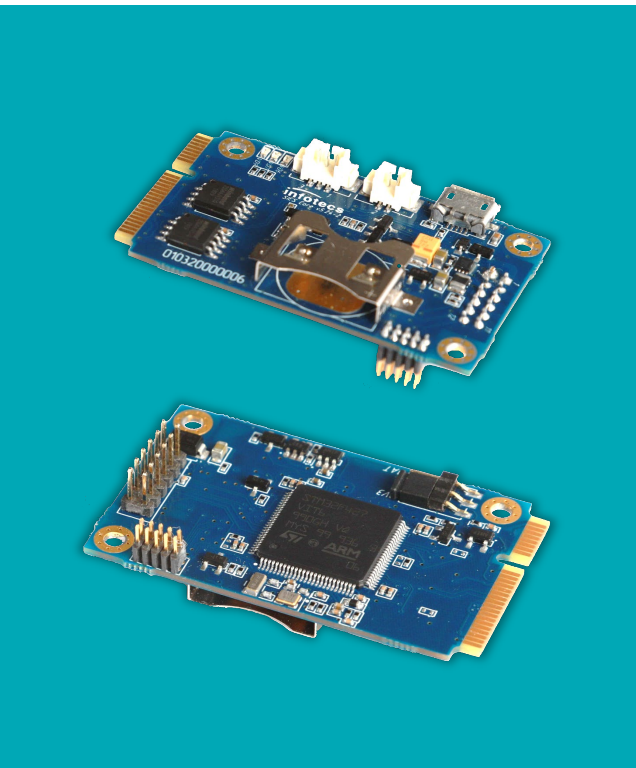
Функциональные особенности:

- 3 резервируемых ключа связи
- Хранение ключевой информации до 16 лет
- Рабочий диапазон температур $-40...+85^{\circ}\text{C}$
- Форм-фактор – микросхема BGA36 $3\times 3\times 0,4$ мм

Соответствие требованиям:

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

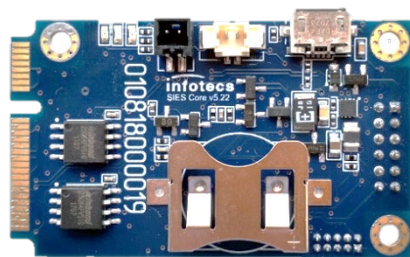
Функциональные особенности:

- 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

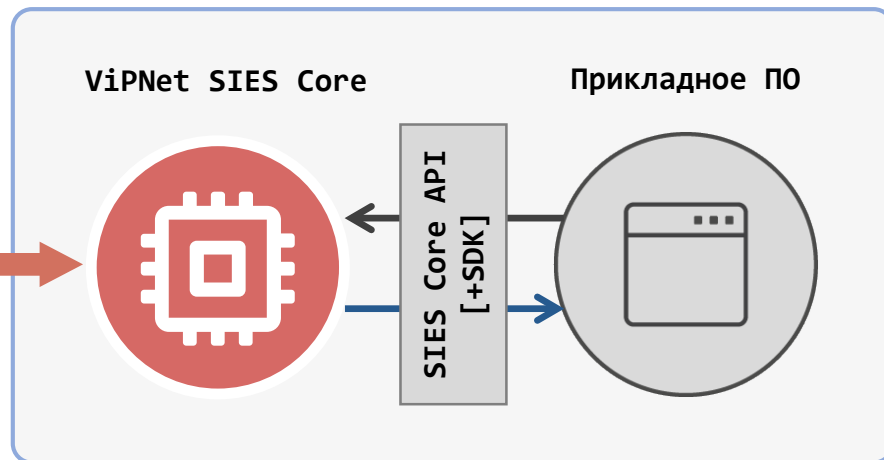
Соответствие требованиям:

- 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

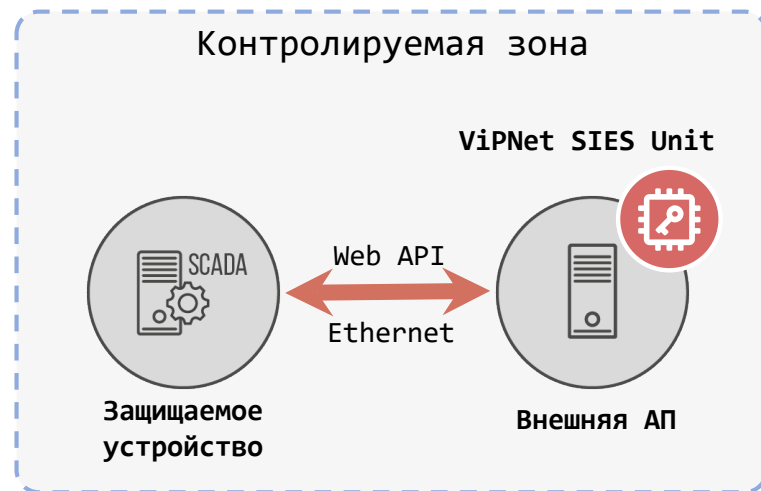
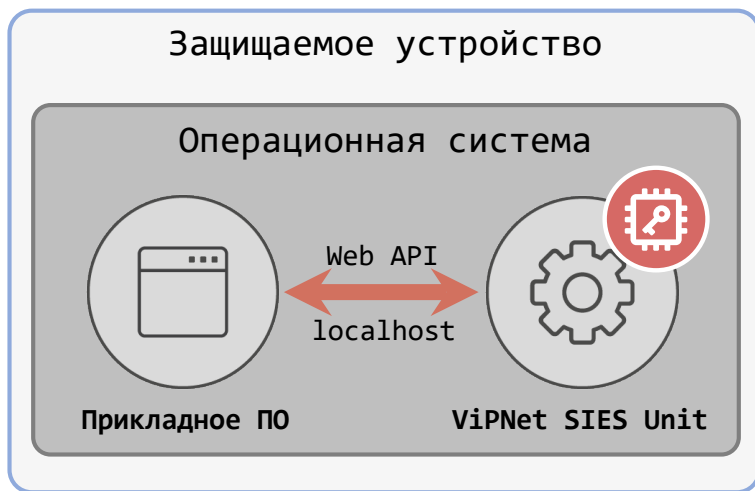
ПК ViPNet SIES Unit

ДЛЯ ИНТЕГРАЦИИ В СЕРВЕРЫ
И РАБОЧИЕ СТАНЦИИ



- Интеграция по REST API (HTTP/1.1), gRPC API (HTTP/2) или SDK;
- Поддерживаемые ОС:
 - Windows 8.1/10
 - Windows Server 2012/2012 R2/ 2016
 - Debian 9.8, 10/ Ubuntu 16, Ubuntu 18 и др ОС Linux (gcc v.6 и выше, systemd система инициализации)
 - Astra Linux Special Edition (Смоленск) 1.6/1.7
- Поддержка архитектур x86-32, x86-64, ARM (armhf)
- Возможность установки на защищаемое устройство или выделенную платформу
- Исполнения с поддержкой различного количества связей: 50, 500, 2000, 10 000 связей
- Сертификат СКЗИ класса КС1 и КС3 по требованиям ФСБ России

Интеграция ViPNet SIES Unit

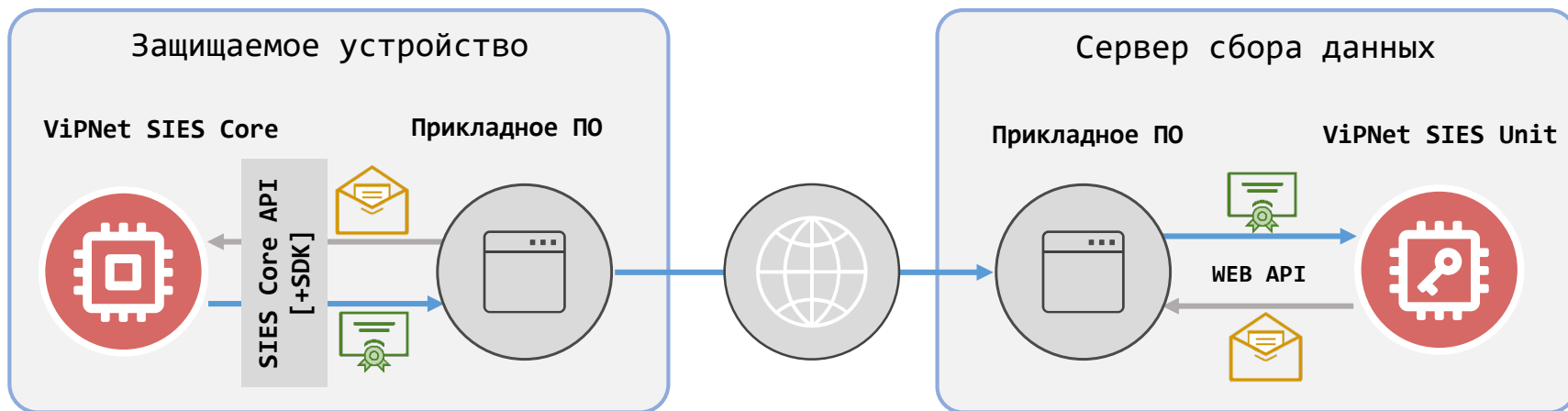


Криптографические сервисы для защищаемых устройств



- 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

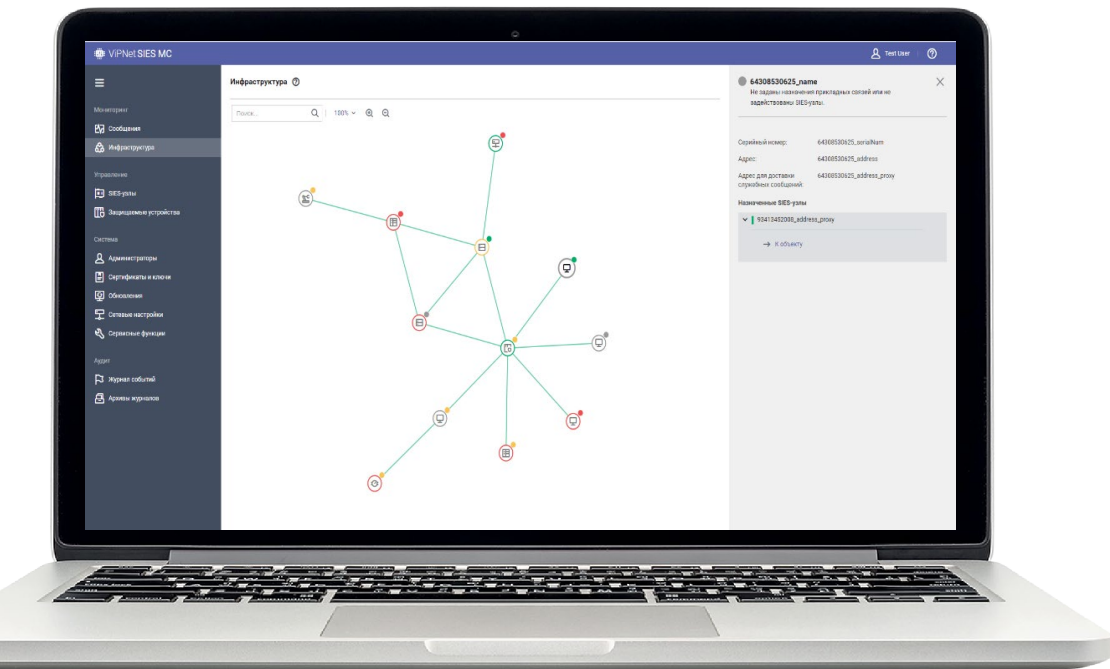


Защищенные данные



Незащищенные данные

ПАК ViPNet SIES MC



Ключевой и
Удостоверяющий центры



Управление связями
в системе



Дистанционная смена
ключевой информации



Управление активами



Разграничение прав
доступа к решению SIES



Доступ к интерфейсу
по WebUI

Центр управления ViPNet SIES MC



ViPNet SIES MC VA

- Max: 5000-узлов
- Max: 500 администраторов безопасности
- Сертификат СКЗИ КС1

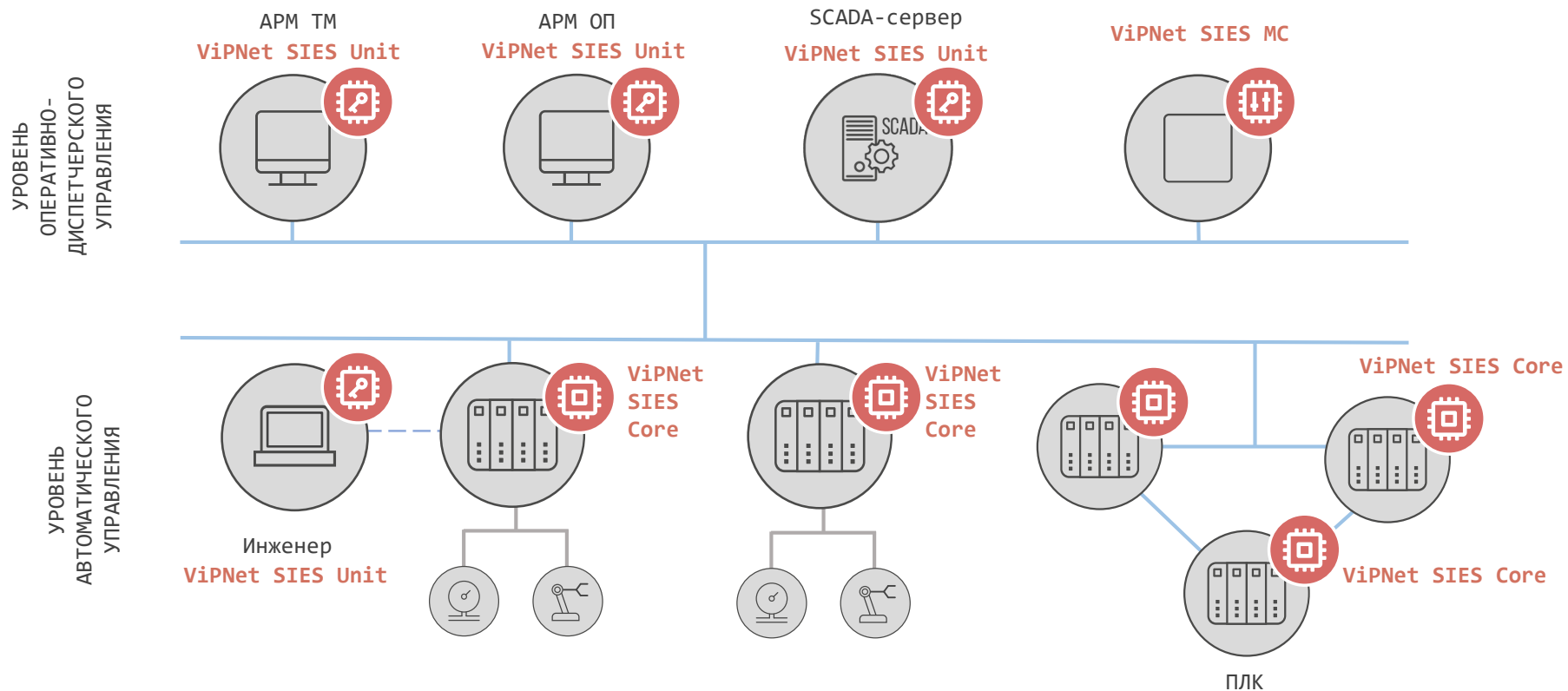
ViPNet SIES MC 3000

- Max: 3000-узлов
- Max: 300 администраторов безопасности
- Сертификат СКЗИ КС3

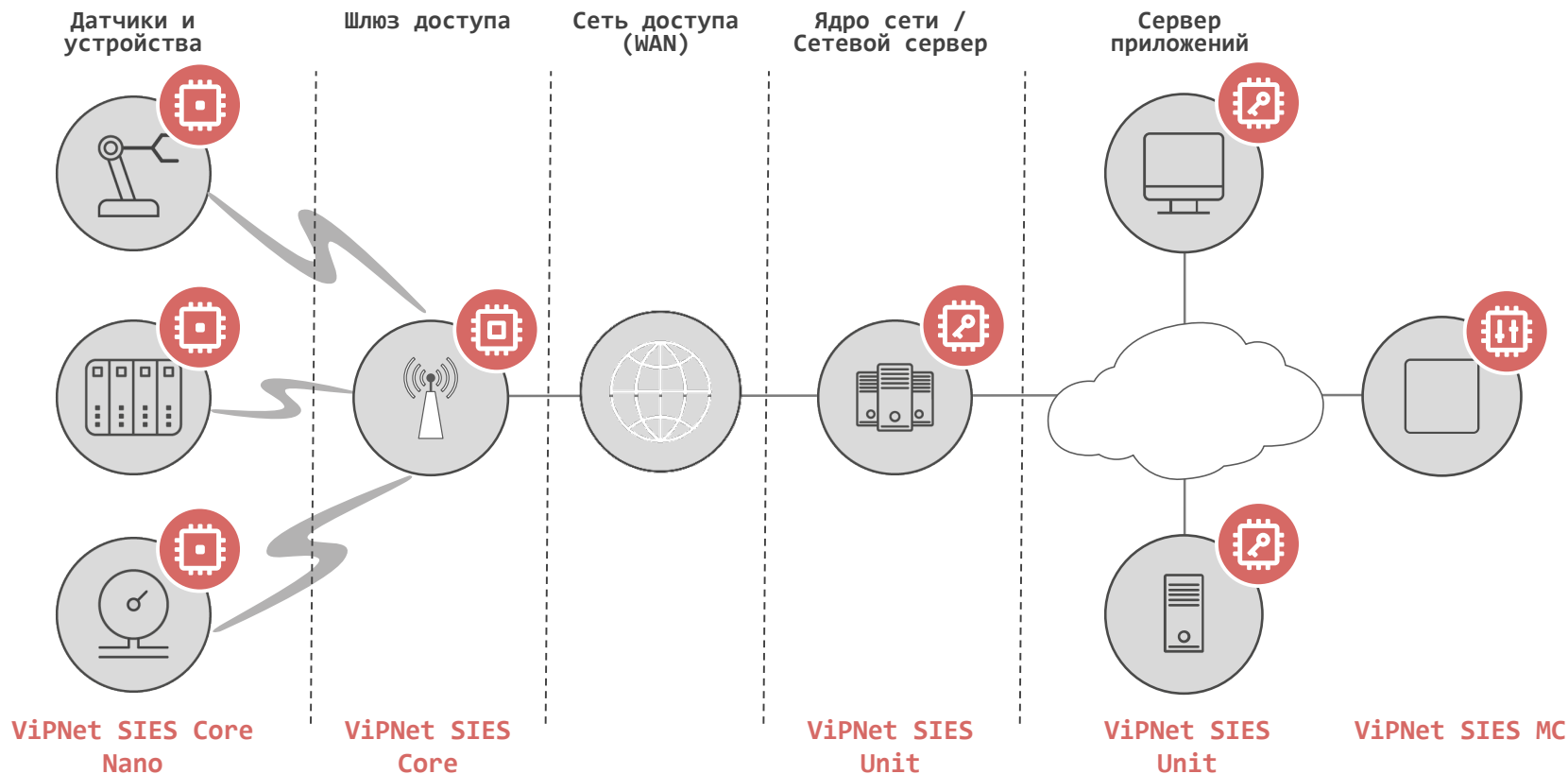
ViPNet SIES MC 10000

- Max: 1 млн узлов
- Max: 1000 администраторов безопасности
- Сертификат СКЗИ КС3

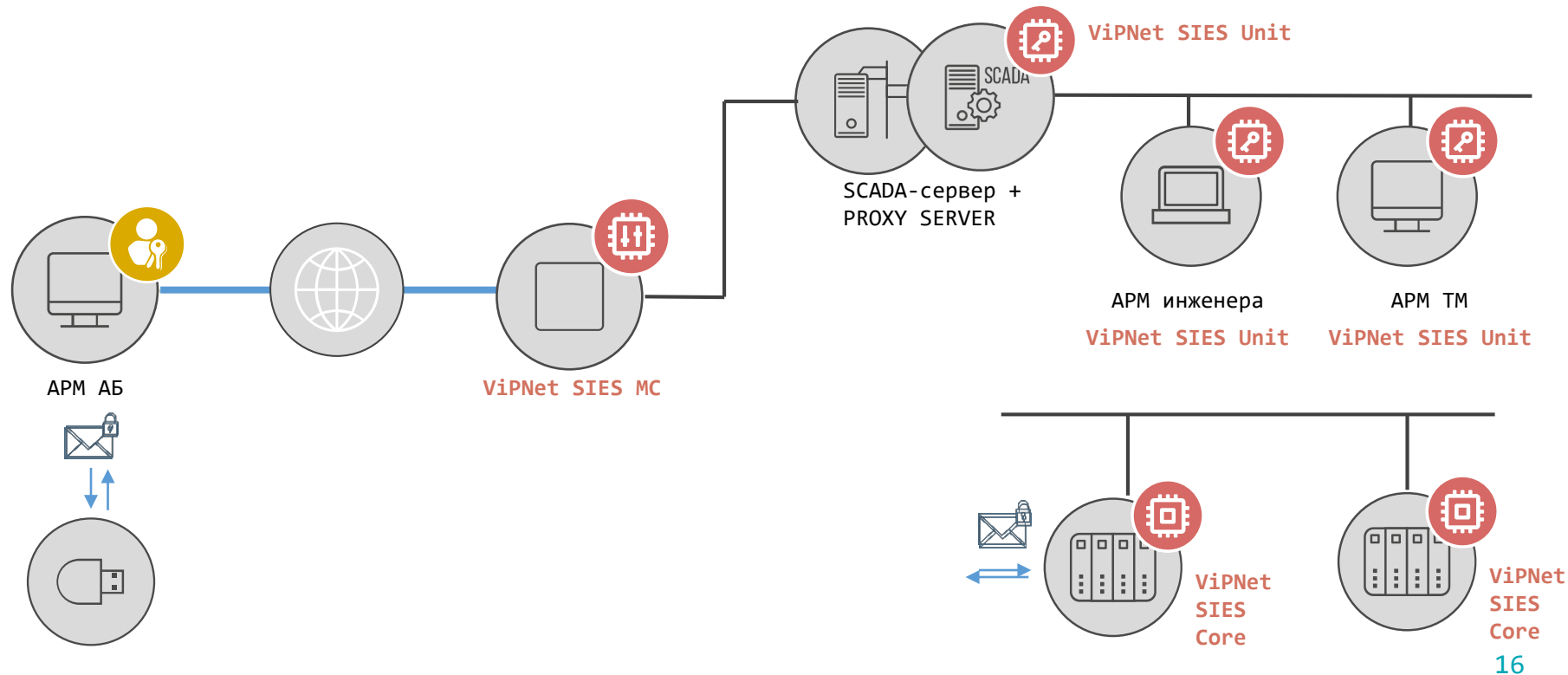
Защищенная АСУ ТП



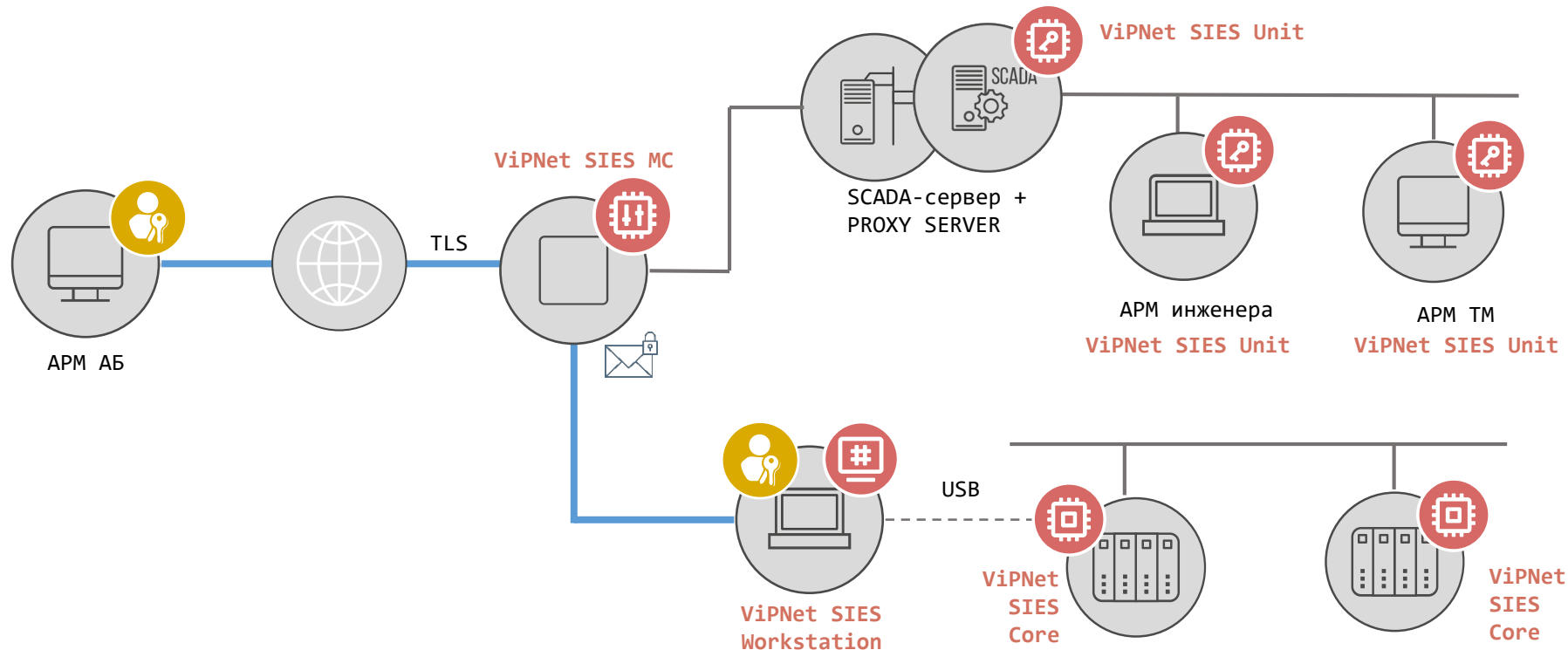
Защита данных в IIoT-системе



Защищенный обмен с SIES-узлами при отсутствии канала связи



Защищенный обмен с SIES-узлами при отсутствии канала связи

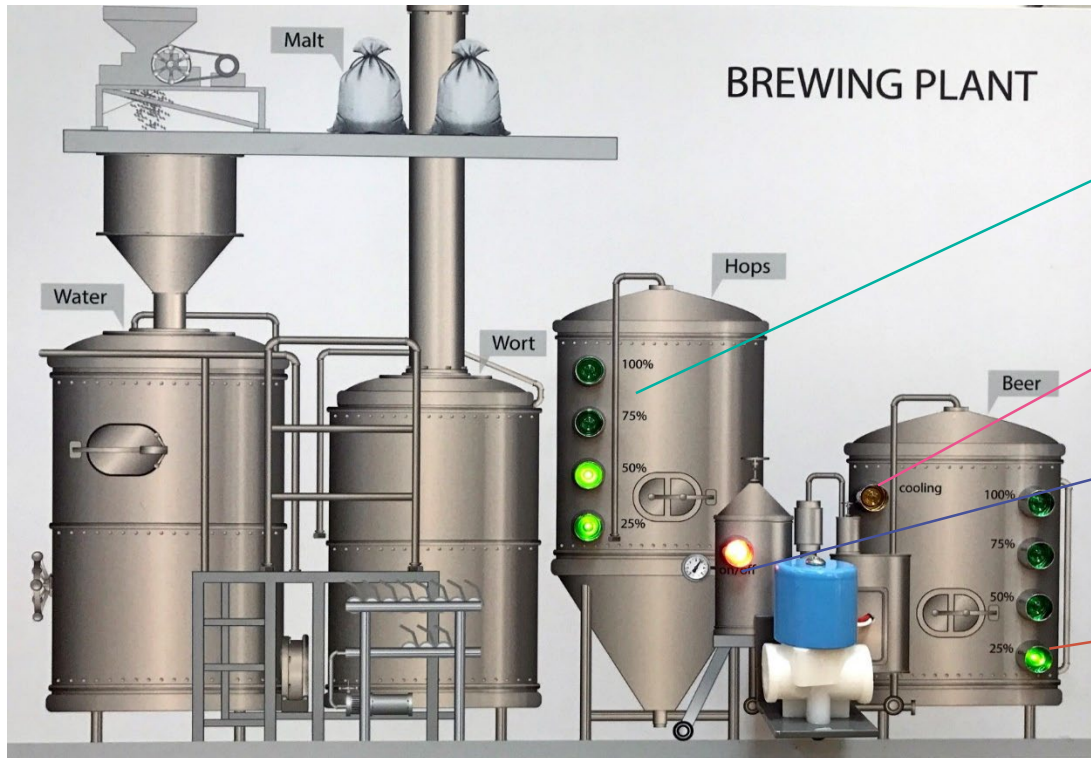


АСУ «Пивоваренный завод»

Технологический процесс пивоварения



Технологический процесс пивоварения



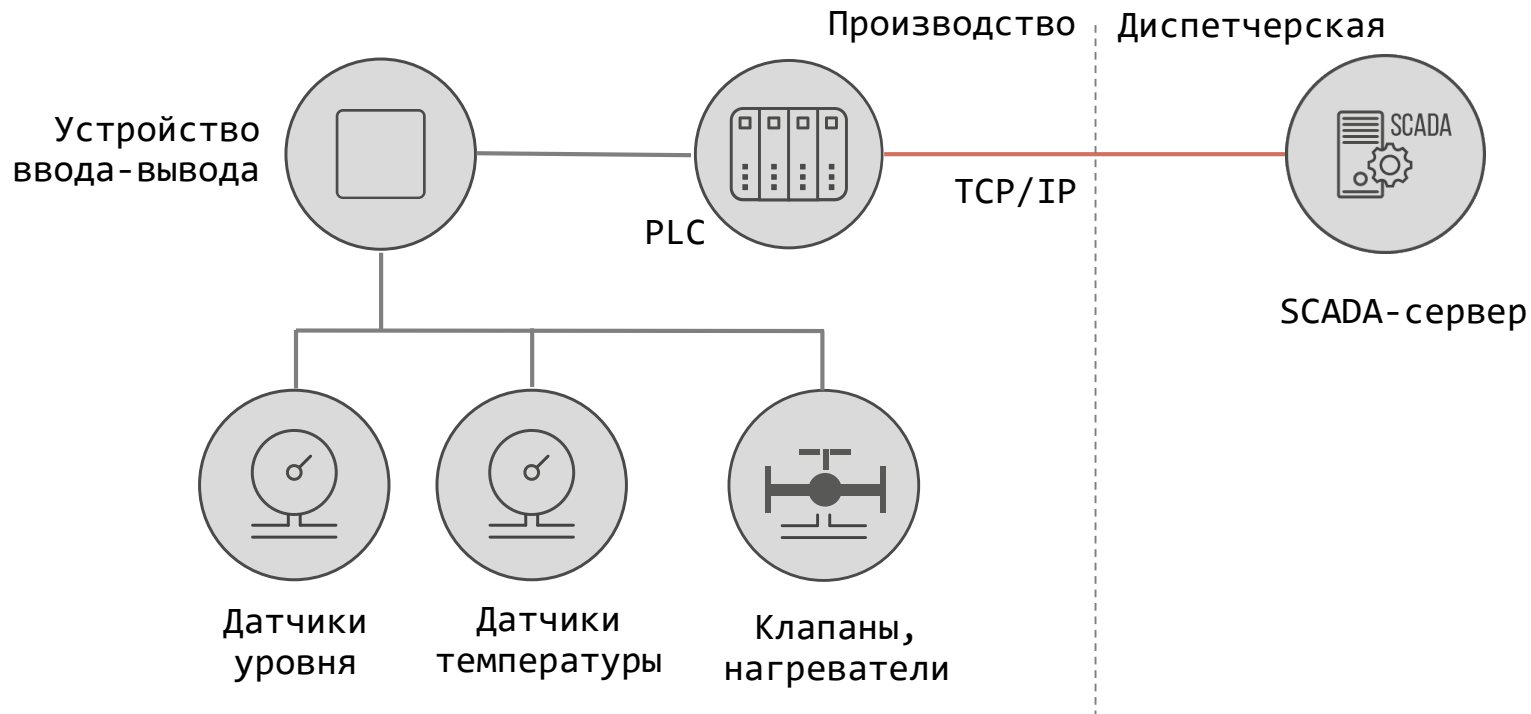
Уровень сусла

Режим
охлаждения

Состояние
клапана перекачки

Уровень
ГОТОВОГО ПИВА

Пивоваренный завод

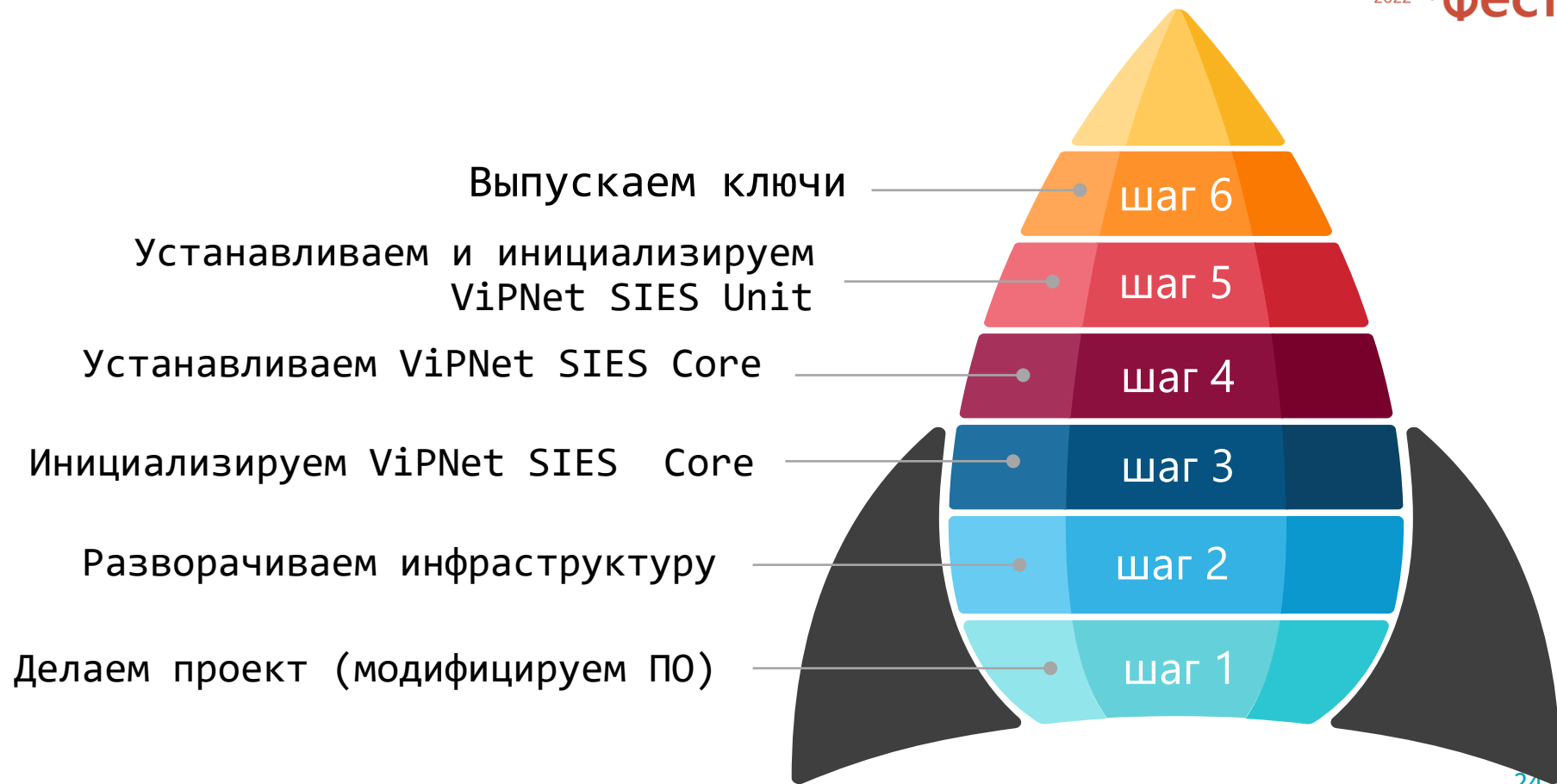




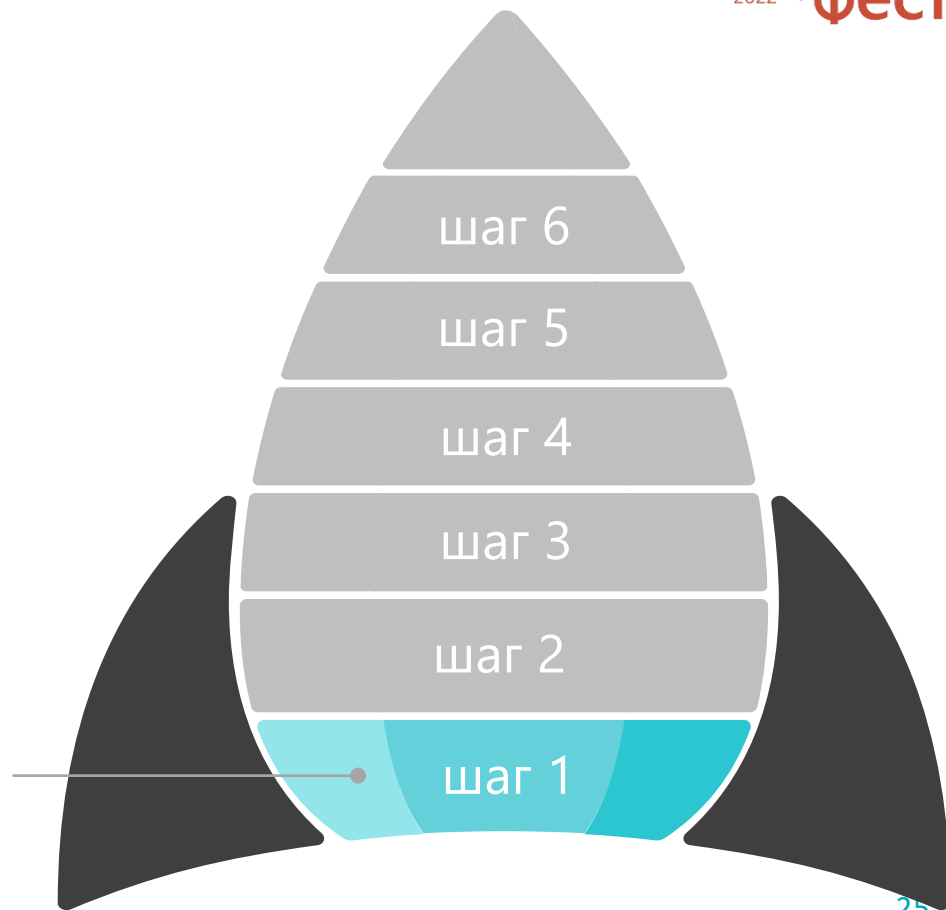
Внутренний нарушитель!!!

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

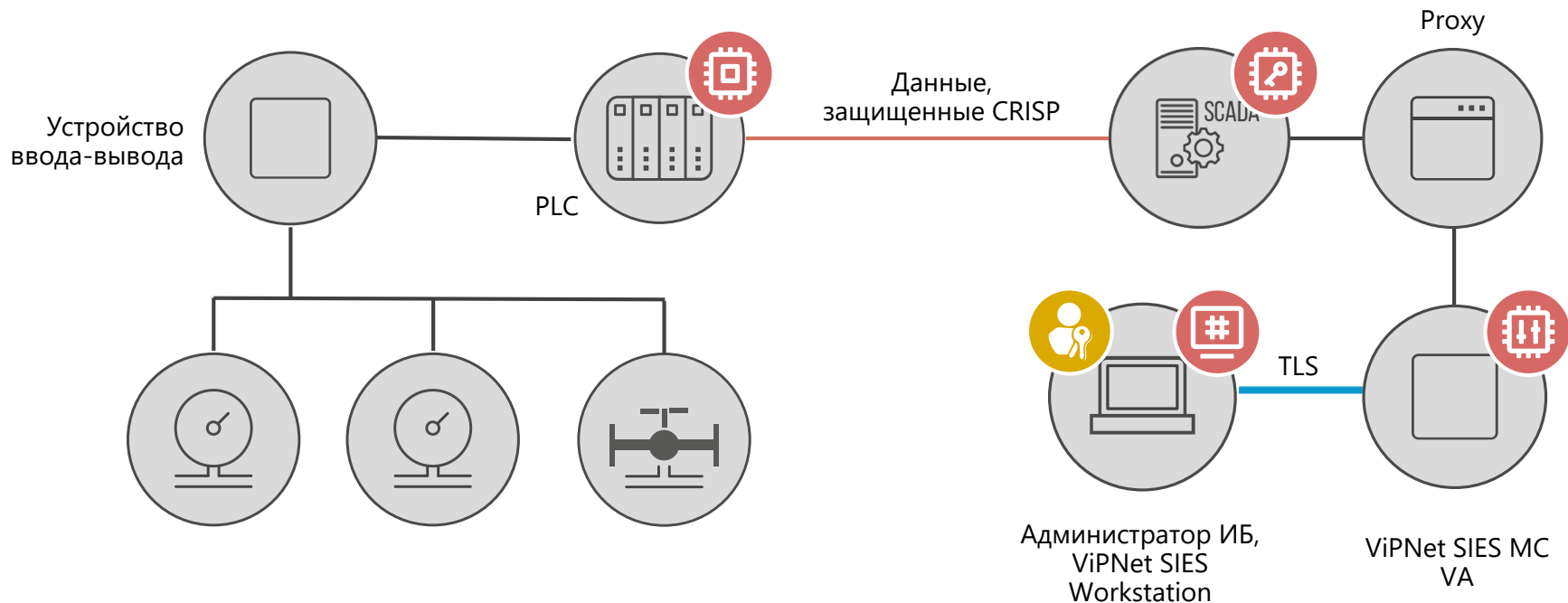
Разворачивание решения ViPNet SIES

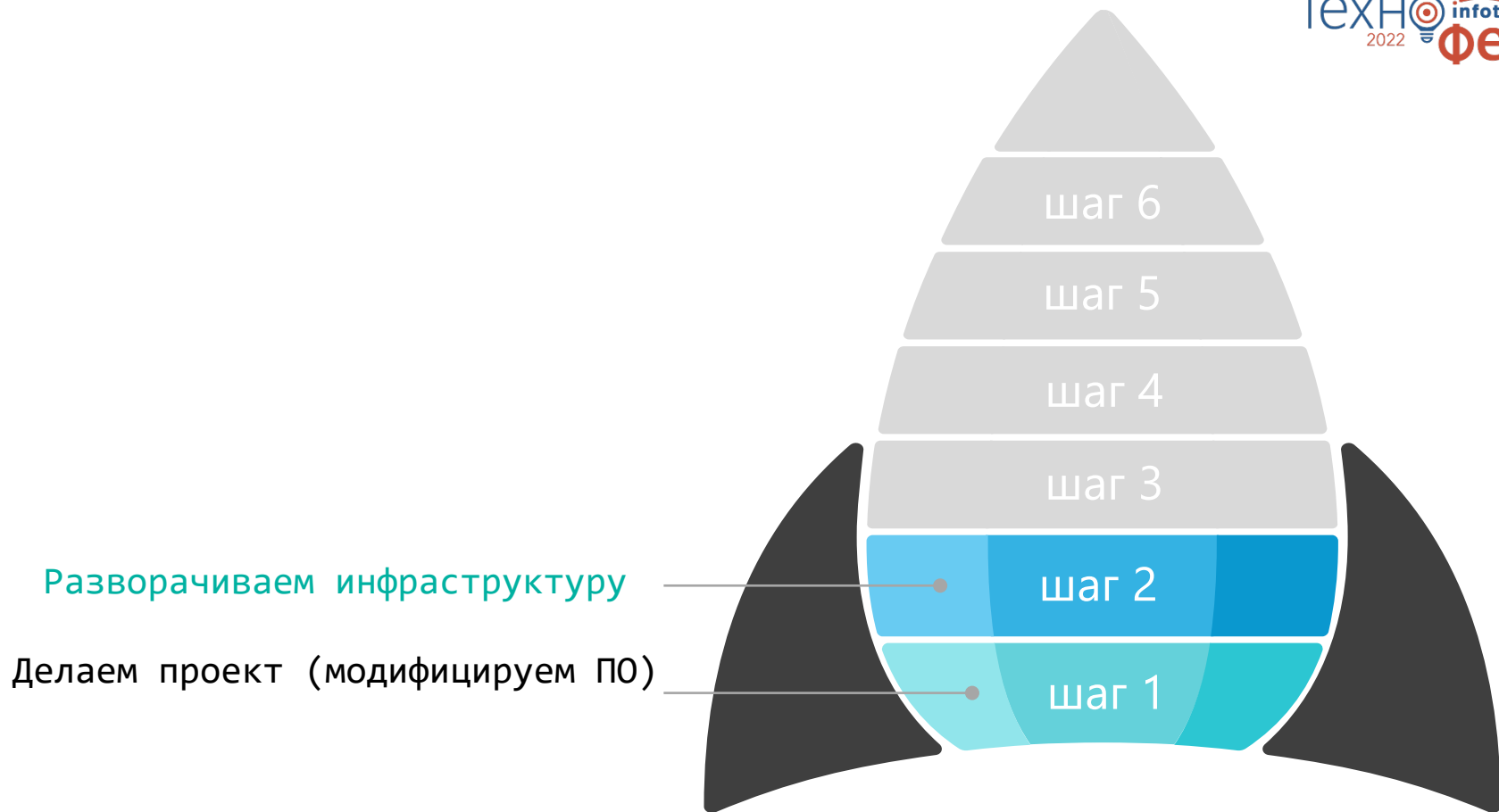


Делаем проект (модифицируем ПО)



Проект пивоваренного завода в защищенном виде





Развертывание инфраструктуры



Назначение администратора ИБ



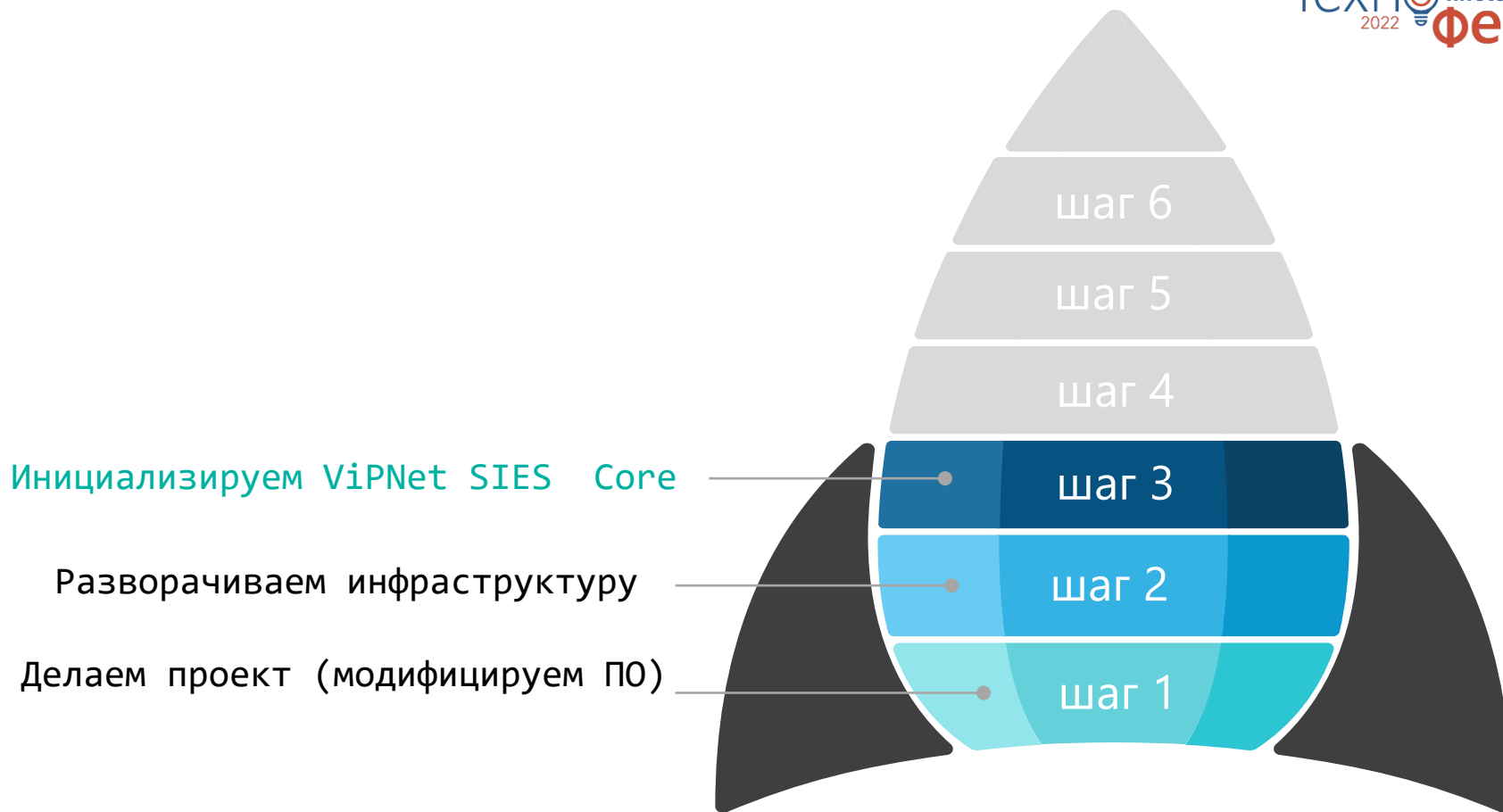
Инициализация ПАК ViPNet SIES MC



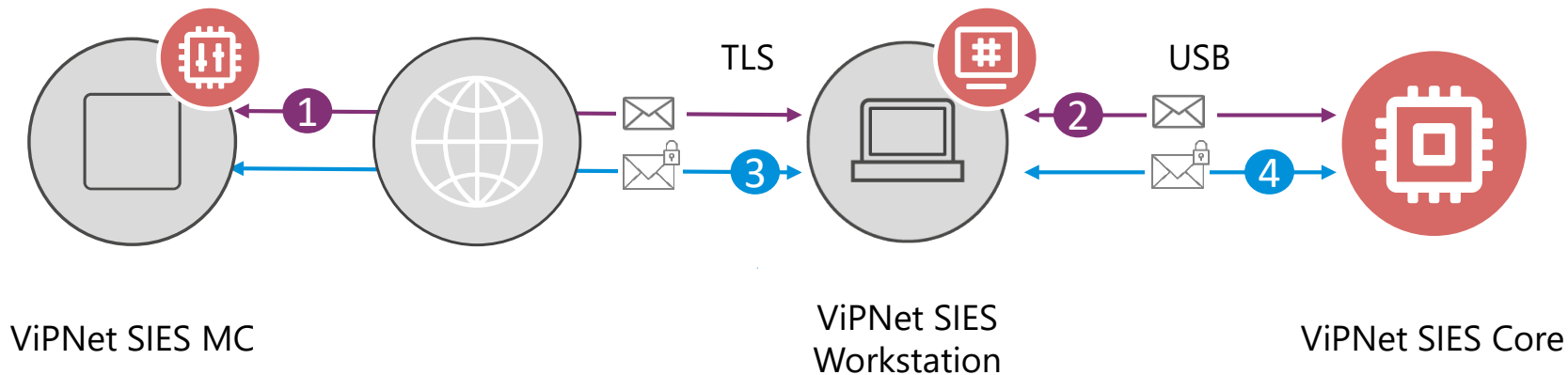
Настройка рабочего места администратора ИБ



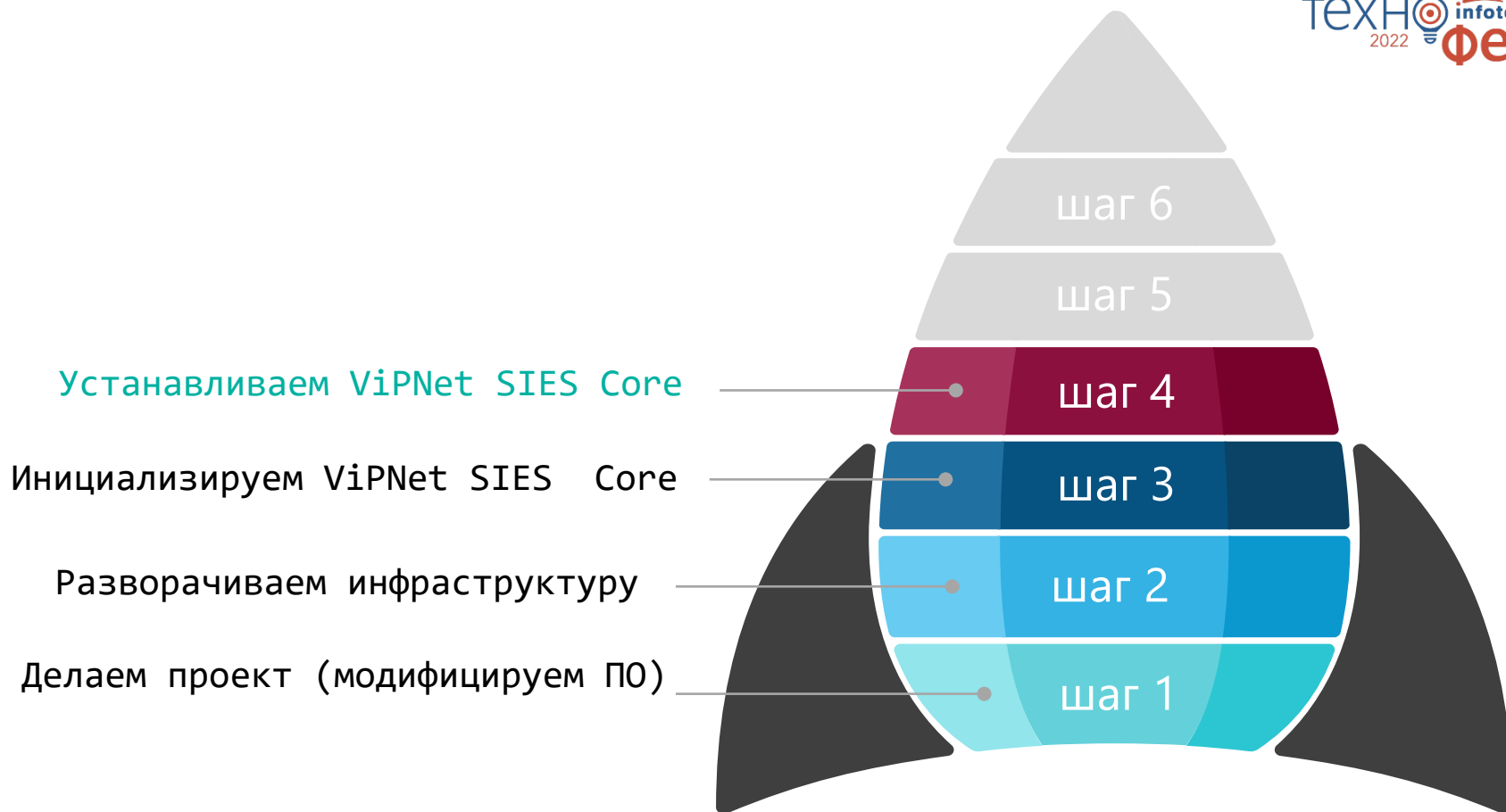
Установка SIES Proху для проброса управляющих команд



Инициализация ViPNet SIES Core

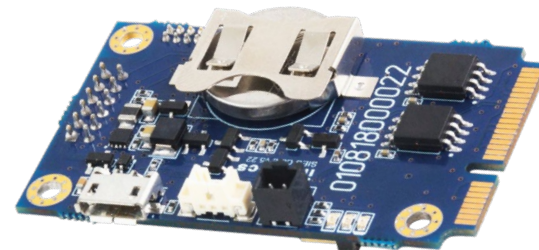
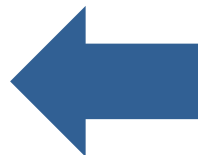


- Начало инициализации
- Завершение инициализации

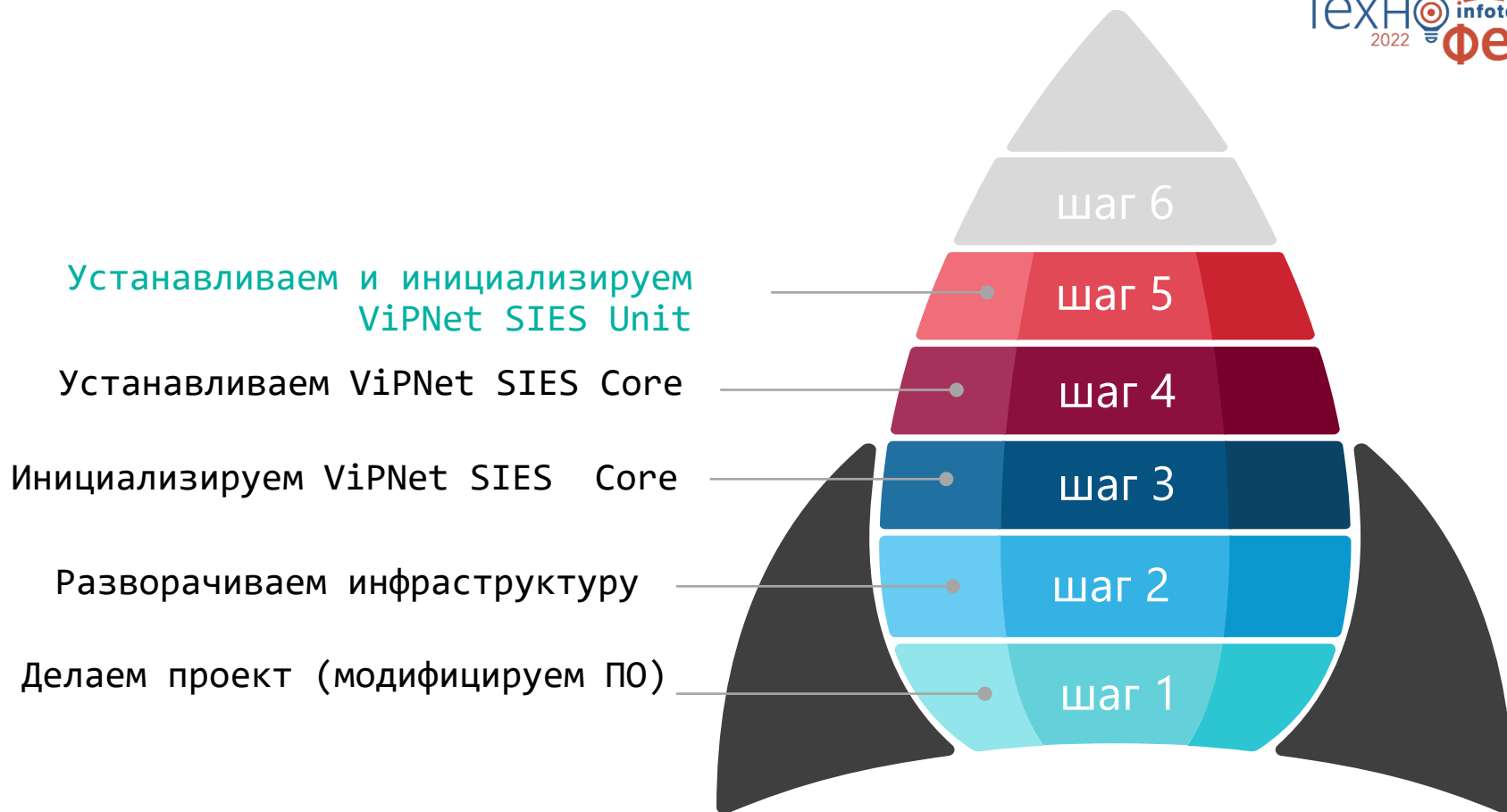


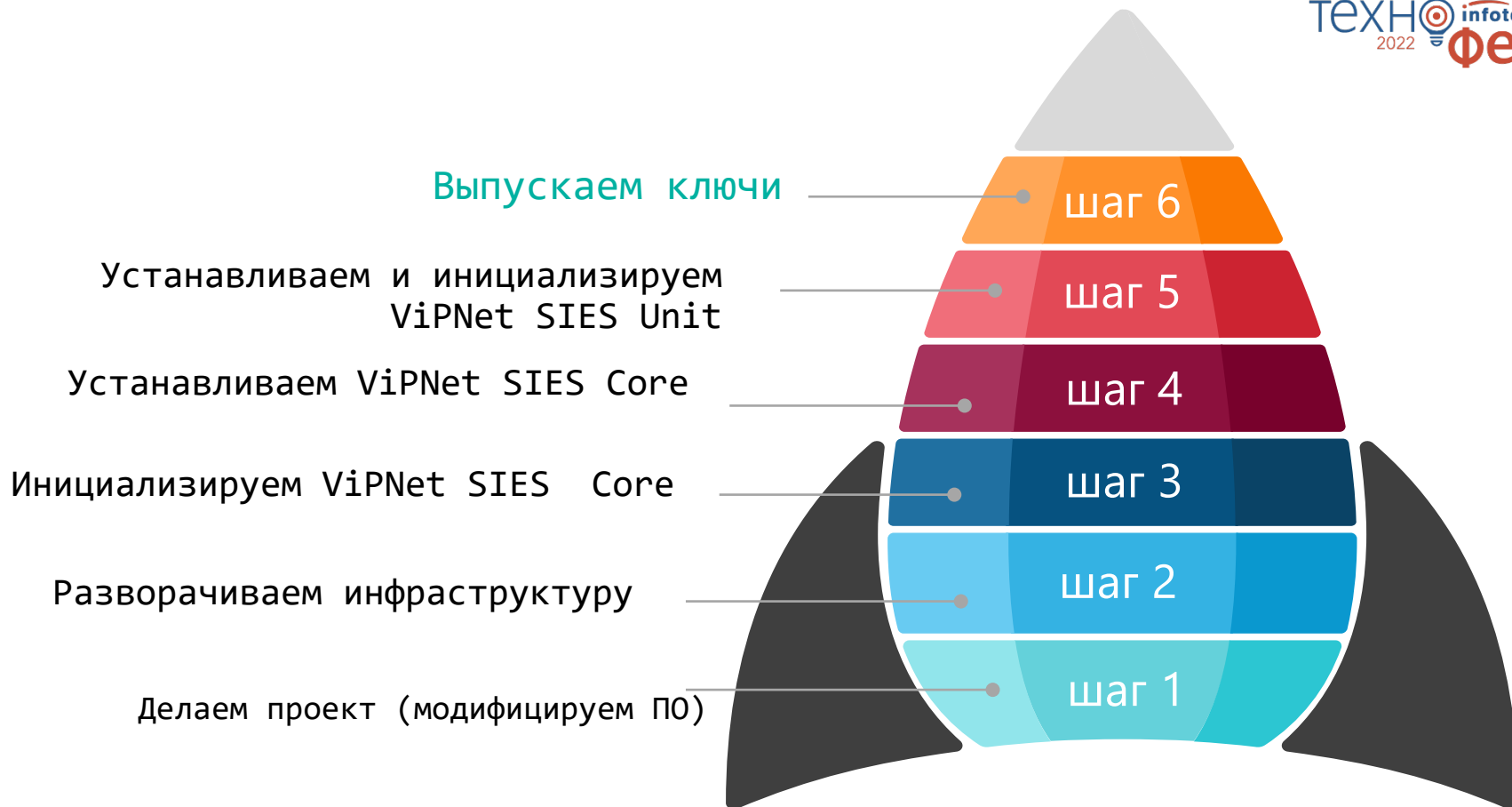
Установка ПАК VIPNet SIES Core в ПЛК

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

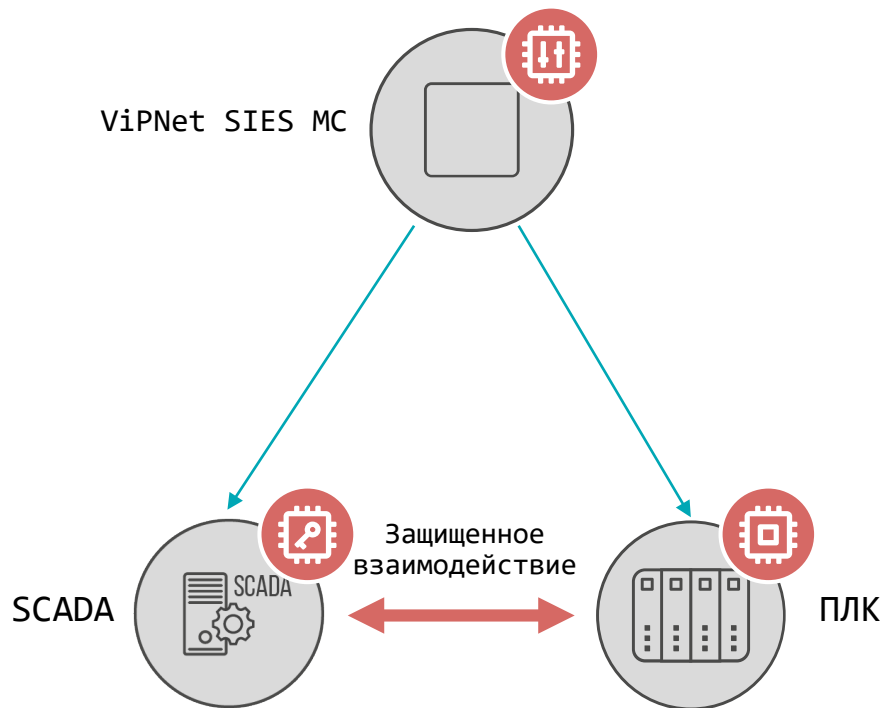


- На аппаратном уровне – USB
- На программном уровне – SIES Core API + SDK (RATP+прикладной протокол)





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.



ТЕХНО infotecs
2022 ФЕСТ

Спасибо за внимание!

Алексей Власенко

Aleksey.Vlasenko@infotecs.ru

Подписывайтесь на наши соцсети



vk.com/infotecs_news



t.me/infotecs_news



rutube.ru/channel/24686363