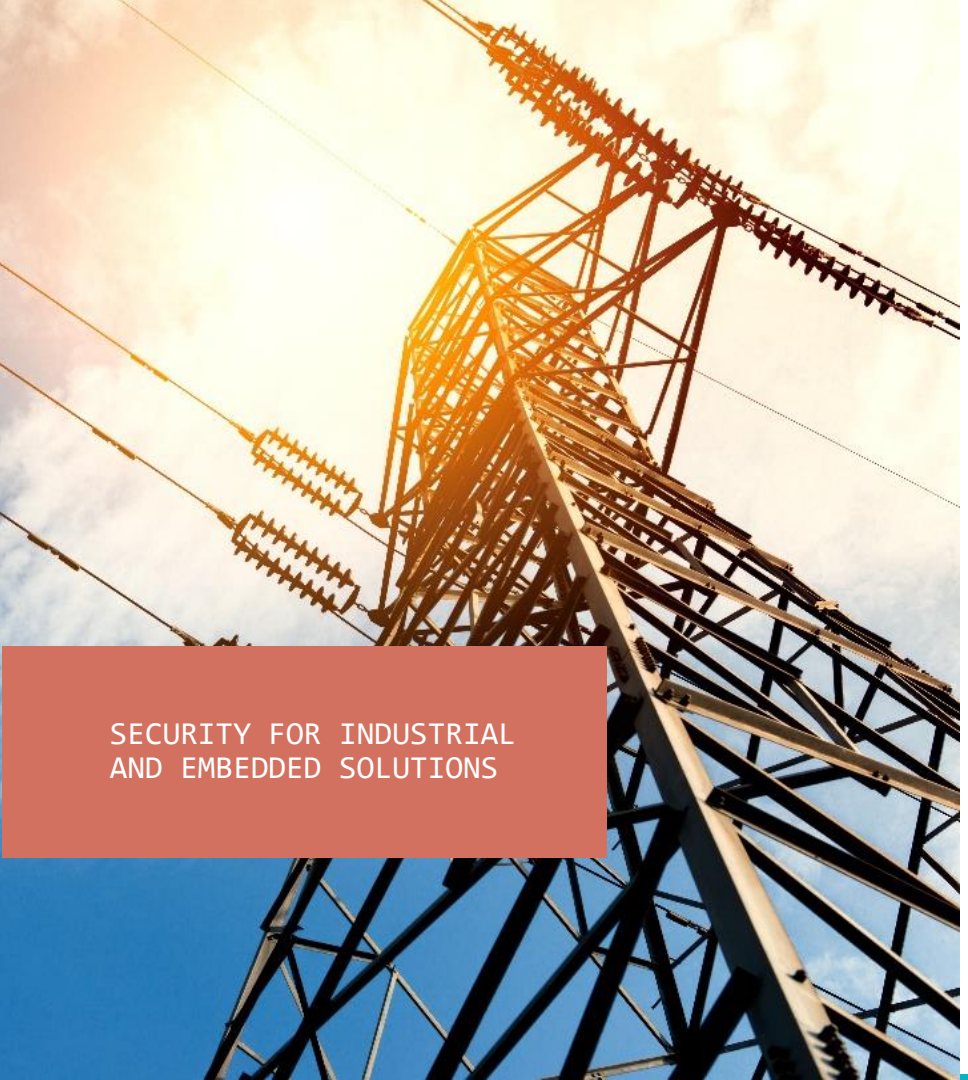
Встраиваемая криптография для промышленных систем

Алексей Власенко
Ведущий менеджер продуктов

Решение ViPNet SIES

Немного теории



SECURITY FOR INDUSTRIAL
AND EMBEDDED SOLUTIONS

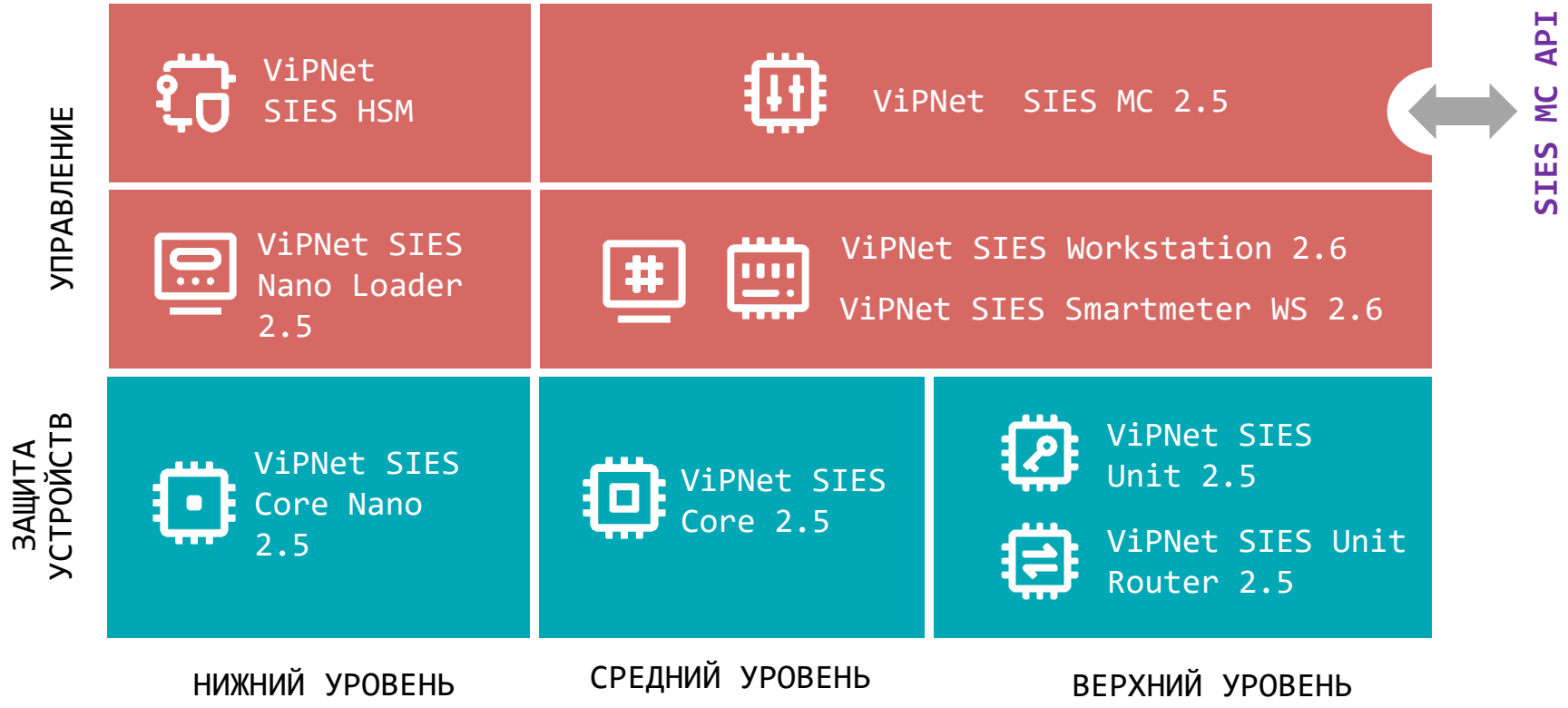
ТЕХНО 2024 infotecs ФЕСТ

Решение ViPNet SIES

Встраиваемые криптографические средства защиты информации:

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

Состав решения 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

ПАК ViPNet SIES MC IoT
- До 2 млн 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

SIES-узлы

СКЗИ, выполняющие прикладные криптографические операции с данными защищаемых устройств

ПАК ViPNet SIES Core

ПО ViPNet SIES Unit

ПАК ViPNet SIES Core Nano

СКЗИ Пользова-теля АСУ

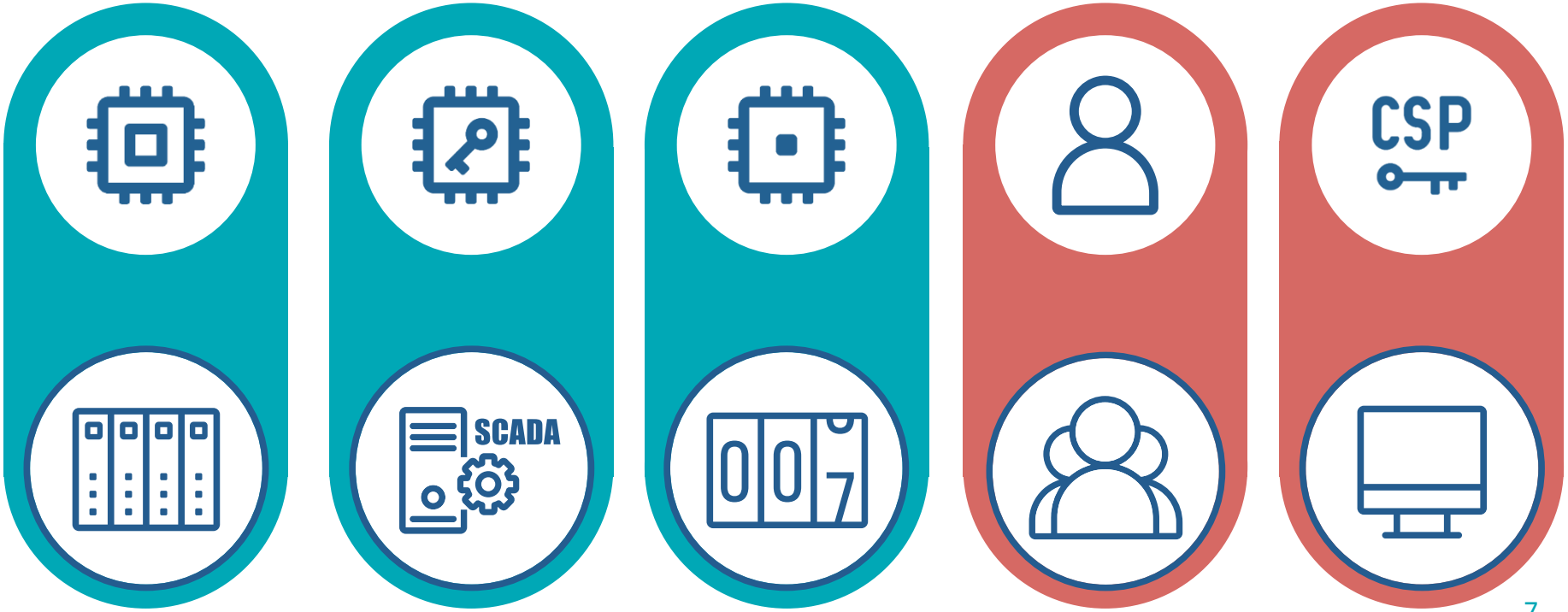
Токены/смарт-карты сервисного инженера, инженера КИП и др.

Другой SIES-узел

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

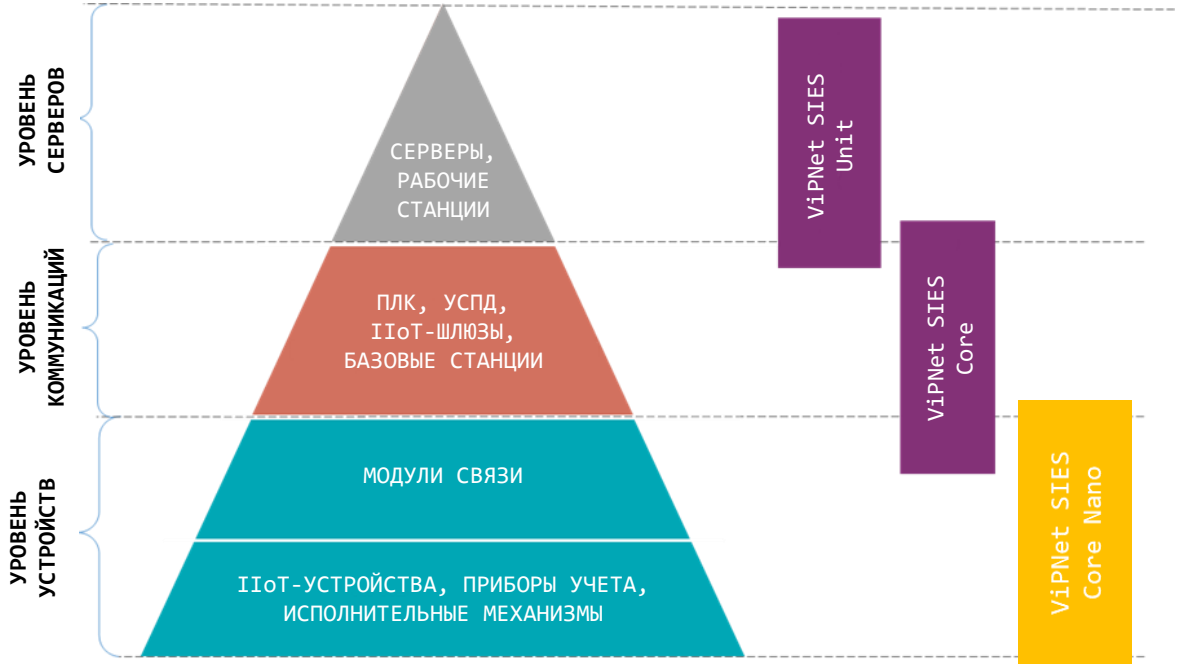
Защищаемые устройства

средства обработки информации, интегрированные с SIES-узлами



Защита данных от АСУ ТП до IIoT

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



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

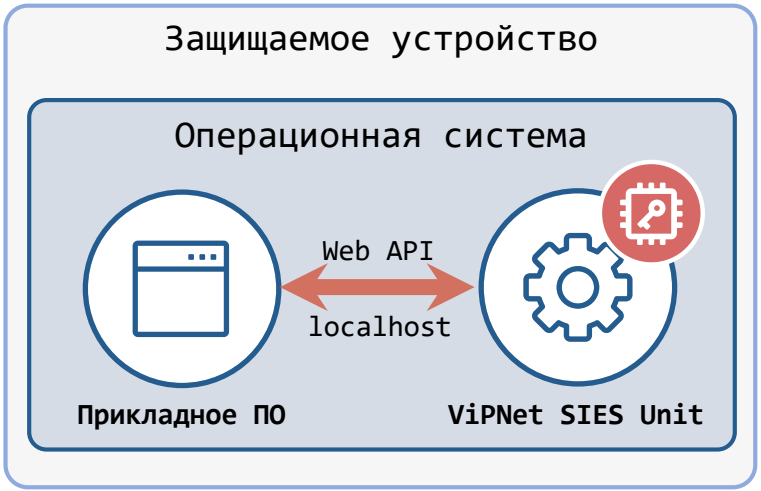
Функциональные особенности:

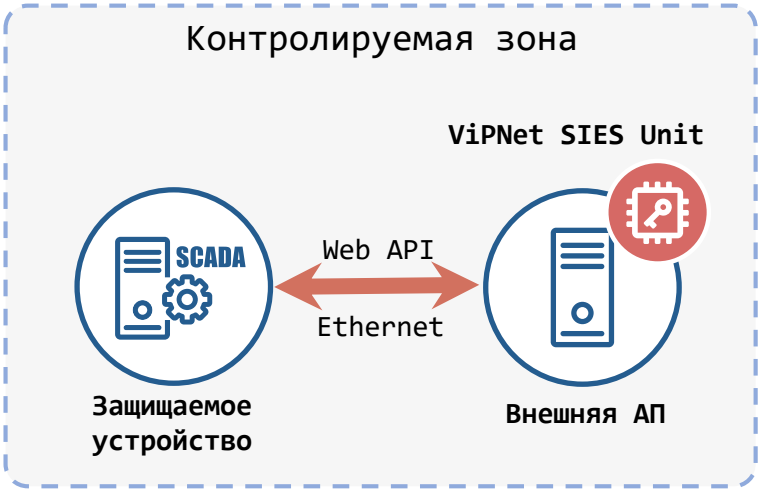
- Поддерживаемые архитектуры – x86-32, x86-64, ARM (armhf)
- Поддерживаемые ОС
  - Windows 10 (x86/64), Windows Server 2012 / 2012R2 / 2016,
  - Linux (Debian 10, 11 / Ubuntu 16, 18 / Astra Linux SE 1.6, 1.7 (Смоленск) / Альт8СП)
- Установка на защищаемое устройство или выделенную платформу
- Исполнения с поддержкой различного количества связей: 50, 500, 2000, 10 000, 100 000, 1 млн связей

Соответствие требованиям:

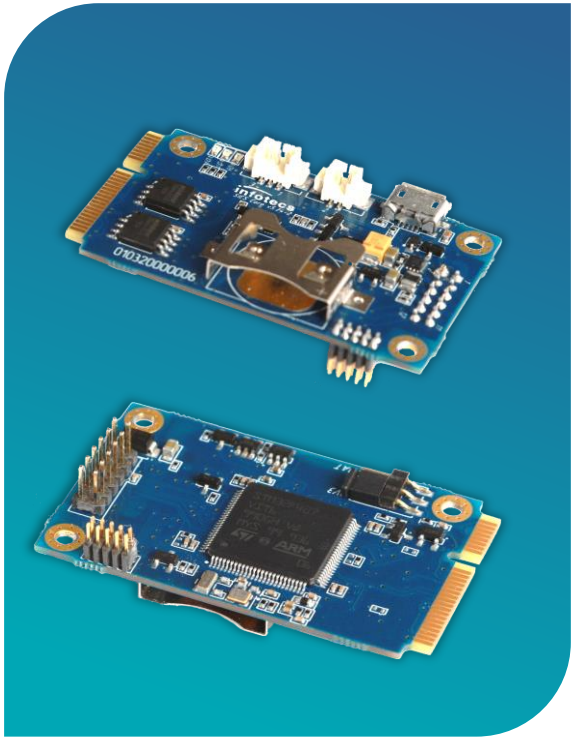
- СКЗИ класса КС1 и КС3

Интеграция ViPNet SIES Unit





ПАК ViPNet SIES Core



Встраивание:

- На аппаратном уровне – UART, USB, SPI
- На программном уровне – SIES Core API

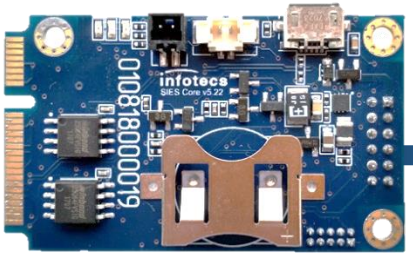
Функциональные особенности:

- Форм-фактор – плата PCI Express® Full-Mini Card (51 x 30 x 11,2 мм)
- Наличие SDK для Linux (ARM, x86), Windows, Baremetal (для устройств без ОС)
- Возможность эксплуатации вне контролируемой зоны при использовании ДНСД
- Рабочий диапазон температур -40^{0}C…+70^{0}C

Соответствие требованиям:

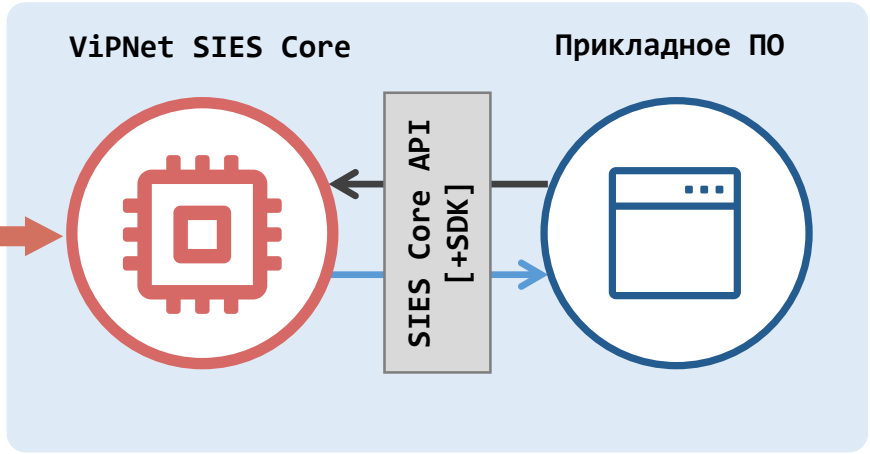
- СКЗИ класса КС3

Интеграция ViPNet SIES Core



ViPNet SIES Core

UART / USB / SPI



SIES Core SDK:

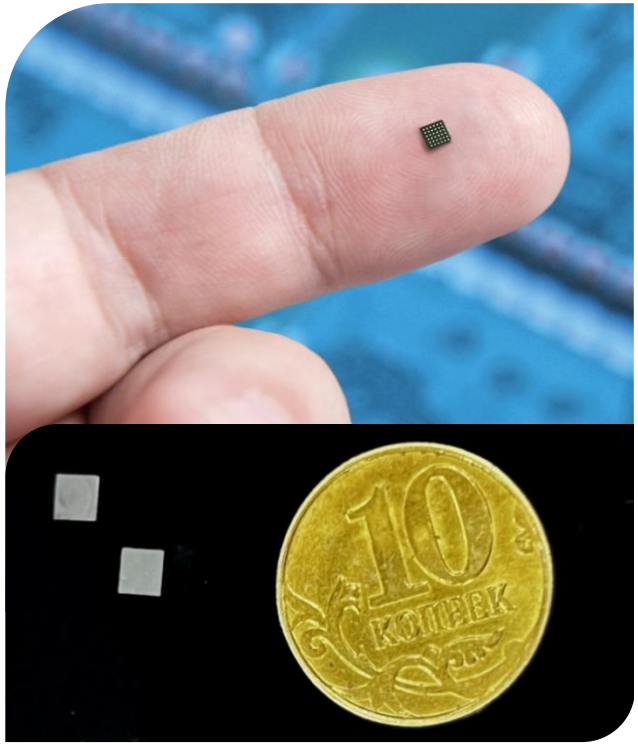
- x86-32/x86-64/ARM
- Windows
- Linux
- Baremetal (для устройств без ОС)

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

Данные

Защищенные данные

ПАК ViPNet SIES Core Nano



Встраивание:

- На аппаратном уровне – SPI
- На программном уровне – SIES Core Nano API

Функциональные особенности:

- 3 резервируемых ключа связи
- Хранение ключевой информации до 16 лет
- Рабочий диапазон температур -40^{0}C…+85^{0}C
- Форм-фактор – микросхема BGA36 3x3x0,4 мм

Соответствие требованиям:

- СКЗИ класса КС3
- Защита от атак инженерного проникновения (СКЗИ-НР)

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

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

СРЕДСТВО ГЕНЕРАЦИИ КЛЮЧЕЙ – SIES HSM

- К 1: симметричный ключ для обмена данными с устройством верхнего уровня (парная связь)
- К 2: симметричный ключ для обмена данными с устройством среднего уровня (парная связь)
- К 3: симметричный ключ для обмена данными с устройством (парная связь)
- К 4: симметричный ключ для собственных нужд ViPNet SIES Core Nano (парная связь)
- К 5: симметричный ключ для резервированной связи с верхним уровнем
- Служебный 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

* Протокол CRISP (ГОСТ Р 71252-2024) входит в перечень рекомендованных Минцифры России протоколов для ИСУЭ и IIoT

Защита адресных и групповых сообщений

Бессесионный криптографический протокол

Минимальные накладные расходы (overhead)и минимальная нагрузка на сеть

Универсальный стандартизированный протокол защиты любых протоколов ИСУЭ

Применение в промышленных системах

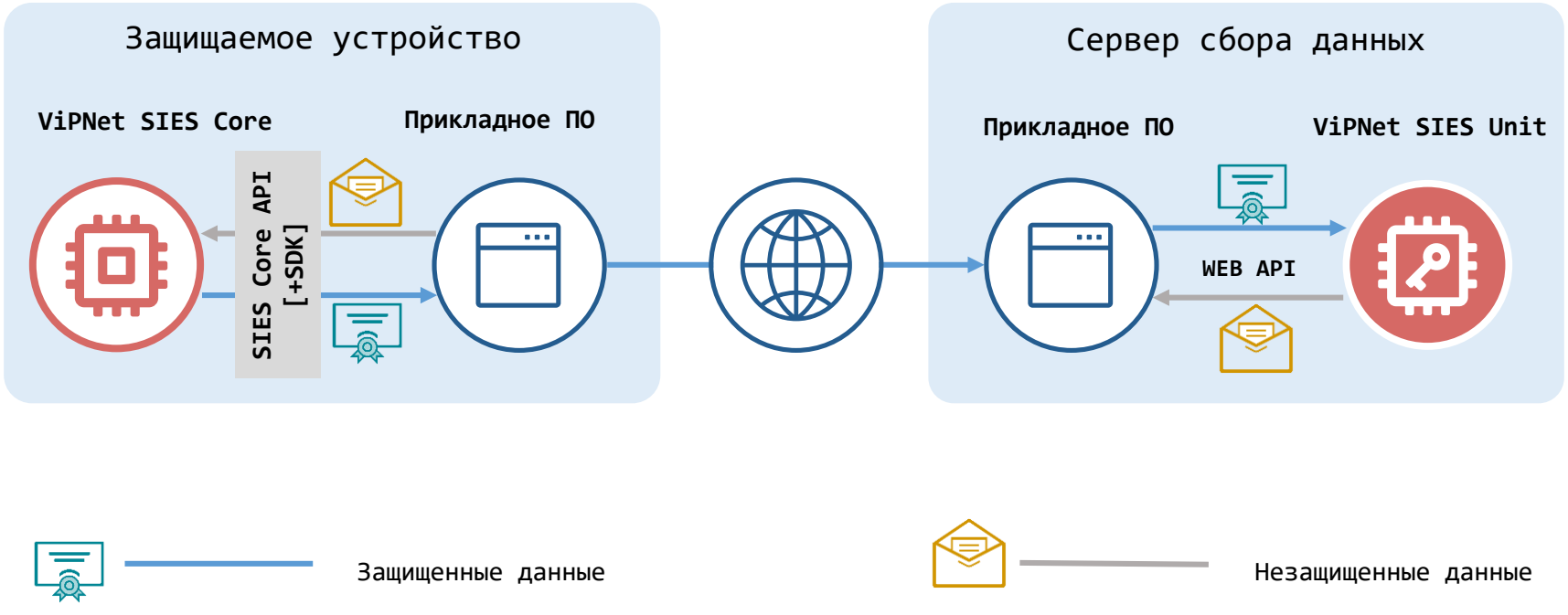
Что и как можно защитить

Криптографические сервисы для защищаемых устройств

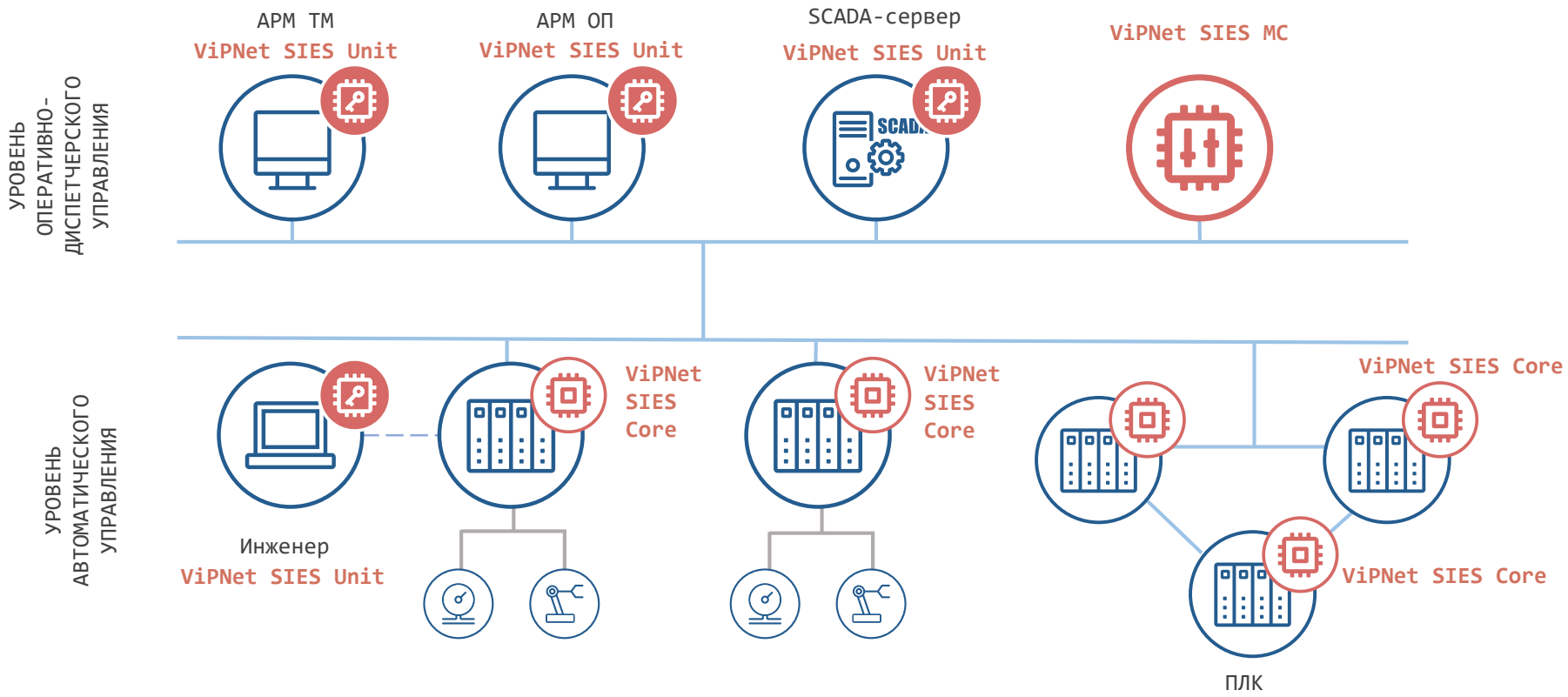
Компоненты решения ViPNet SIES позволяют реализовывать следующие сценарии обеспечения информационной безопасности защищаемых устройств:

- Защита данных при передаче по каналам связи вне зависимости от типа сети
- Доверенное обновление защищаемого устройства
- Доверенное локальное и дистанционное конфигурирование защищаемого устройства
- Локальная и дистанционная аутентификация пользователей защищаемого устройства

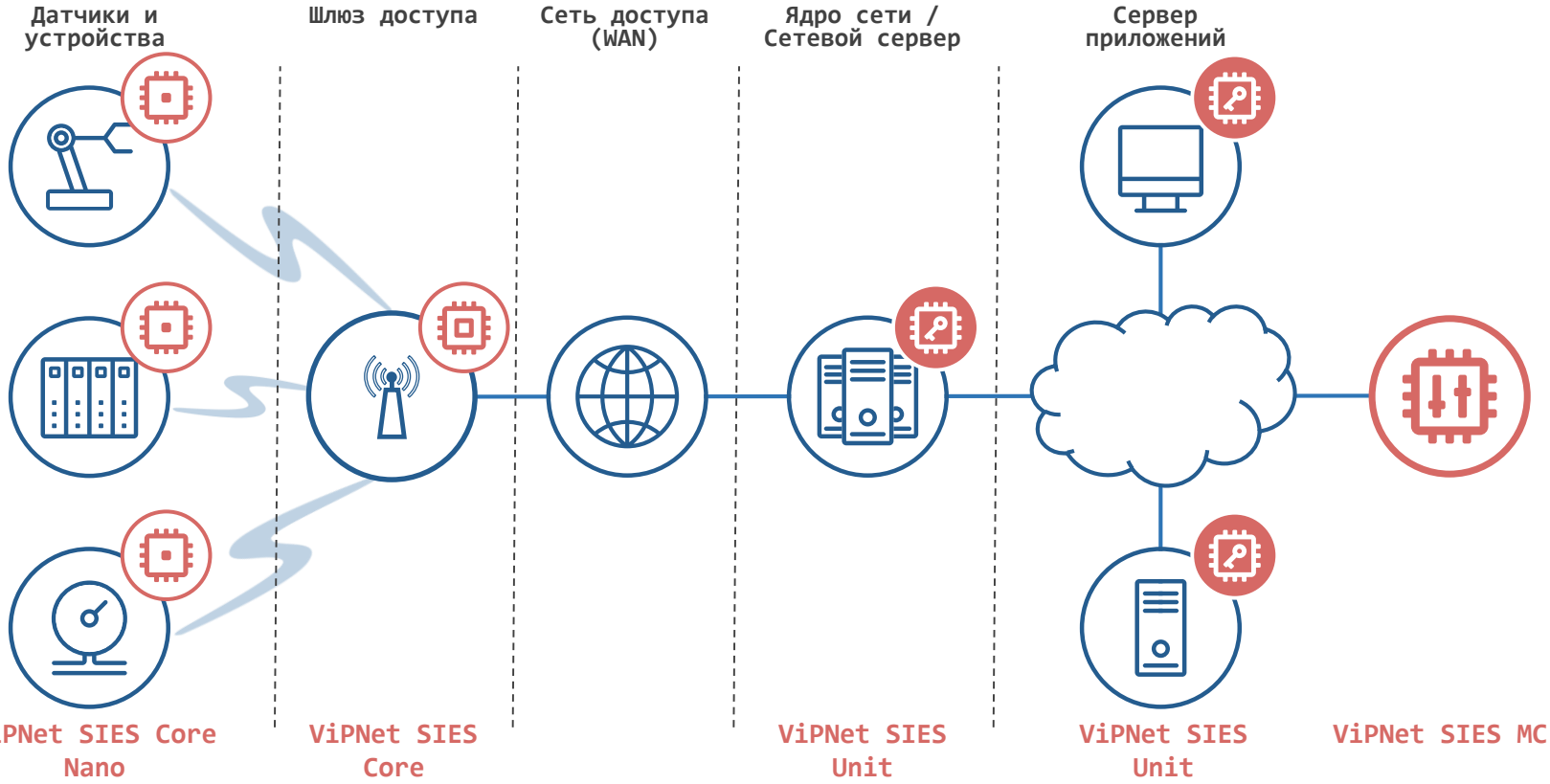
Защита коммуникаций с помощью ViPNet SIES



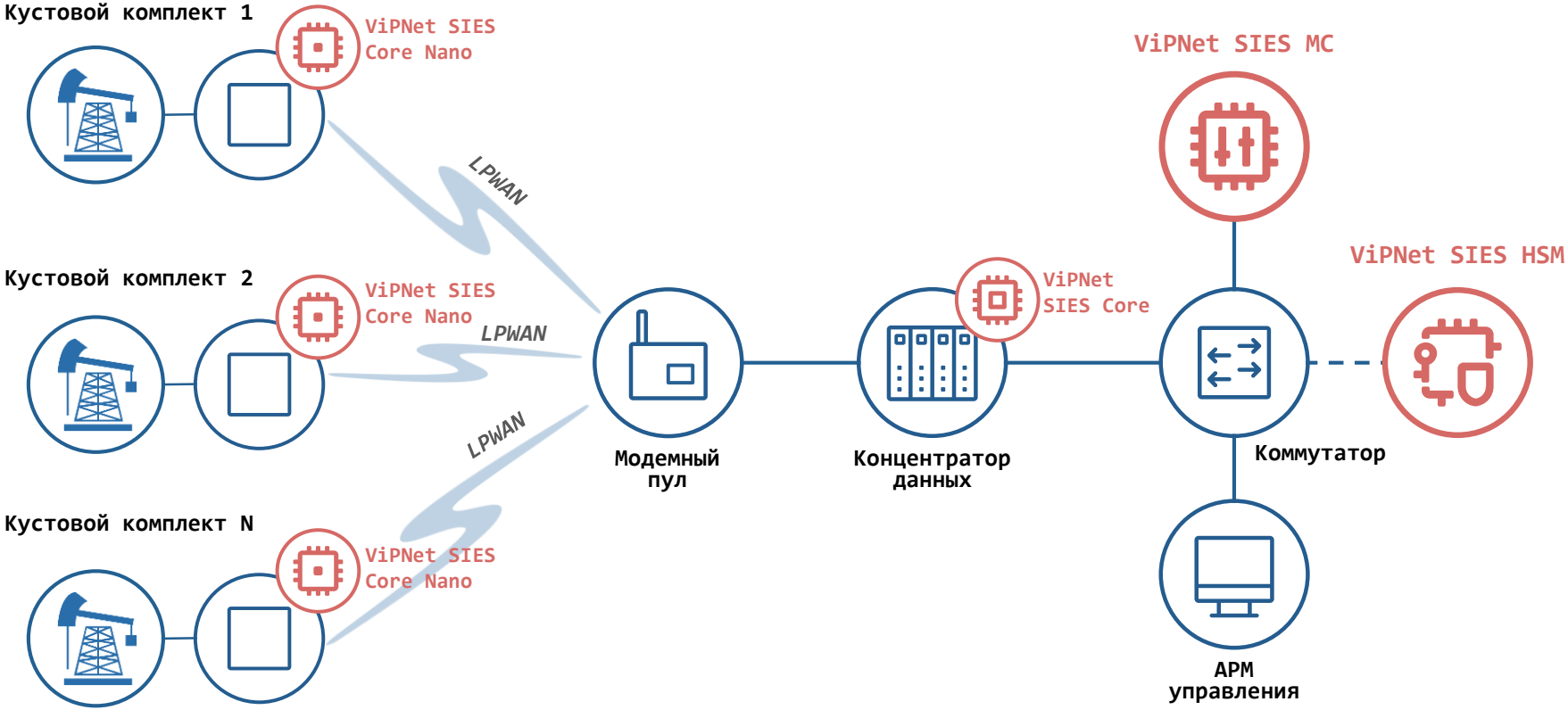
Защищенная АСУ ТП



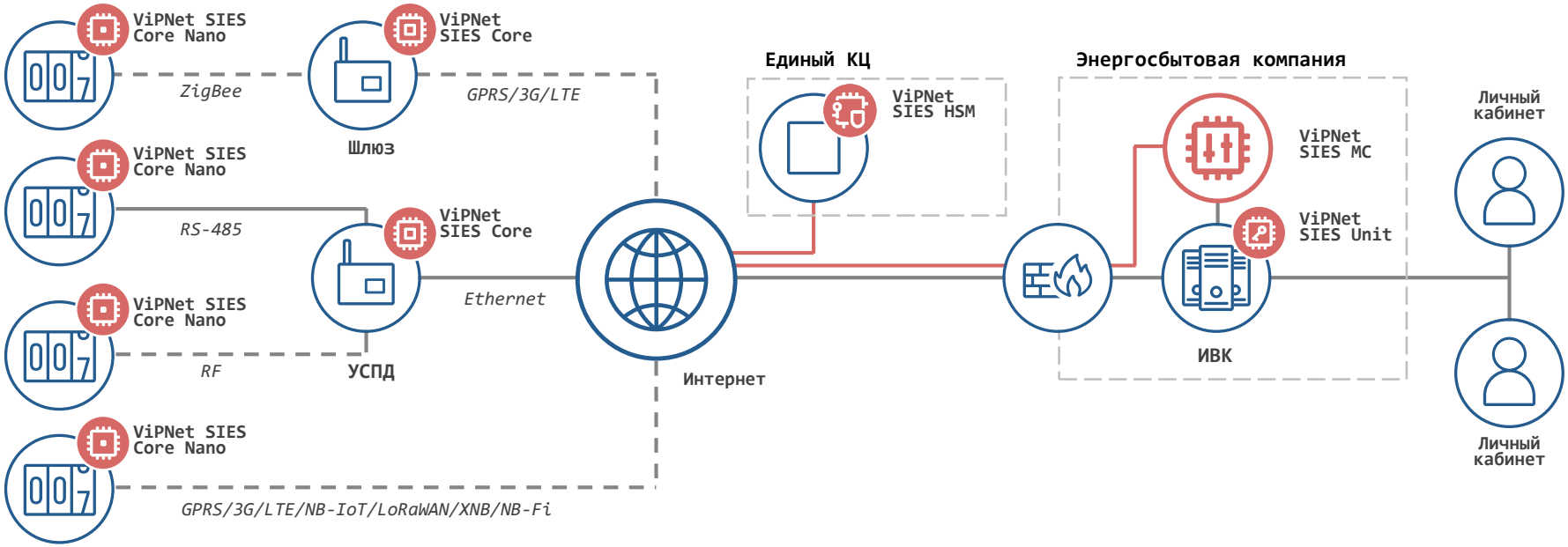
Защита данных в IIoT-системе



Защита данных в АССД



Защита данных в ИСУЭ



ТЕХНО 2024 infotecs ФЕСТ

Ответы на вопросы

Подписывайтесь на наши соцсети