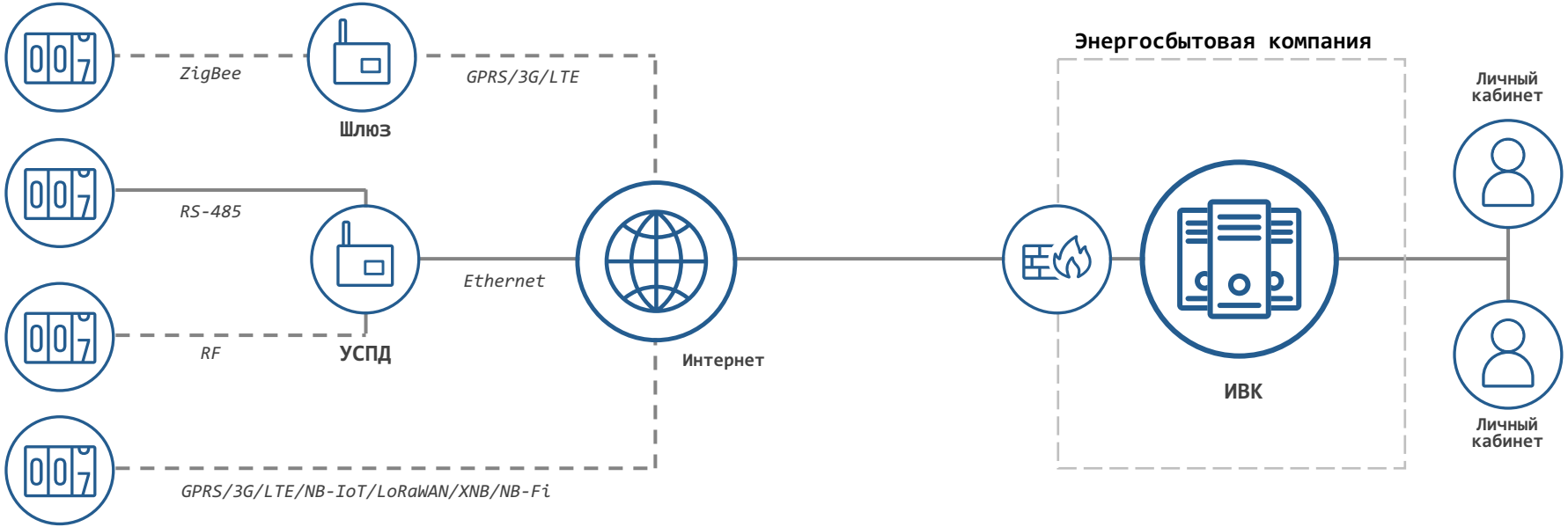
Решение ИнфоТеКС для защиты данных интеллектуальной системы учета

Алексей Власенко
менеджер продуктов

infotecs

Структура ИСУЭ



Приборы учета (ПУ) Уровень ИВКЭ Уровень ИВК

Сложности обеспечения ИБ ИСУЭ

- Большая распределенная система
- Элементы ИСУЭ, за исключением ИВК, расположены вне контролируемой зоны
- ИСУЭ по своей архитектуре является IIoT-системой и защищать ИСУЭ нужно как IIoT
- СЗИ и СКЗИ должны быть встроенными в компоненты ИСУЭ
- Большое количество протоколов и интерфейсов
- Большое количество разработчиков и производителей компонентов ИСУЭ

Сложности применения СКЗИ в ИСУЭ

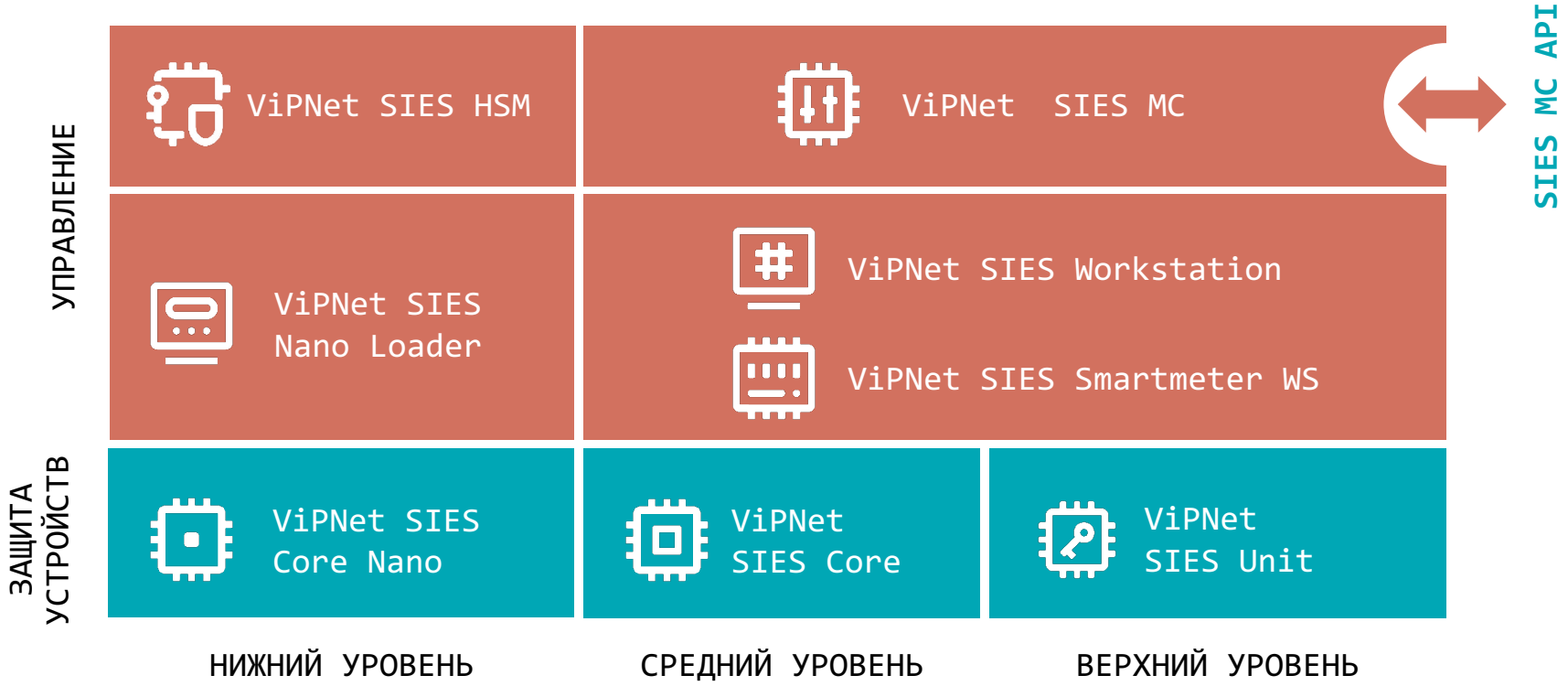
- СКЗИ должны быть встроенными
- СКЗИ применяются в условиях отсутствия контроля несанкционированного доступа
- СКЗИ используются для защиты данных по каналам, которые могут быть не TCP/IP
- СКЗИ должны функционировать на каналах с низкой пропускной способностью
- СКЗИ должны быть рассчитаны на работу в ИСУЭ с учетом ее количественных характеристик
- СКЗИ должны иметь централизованную схему управления
- СКЗИ должны функционировать в компонентах ИСУЭ с большим сроком службы

infotecs

Решение ViPNet SIES

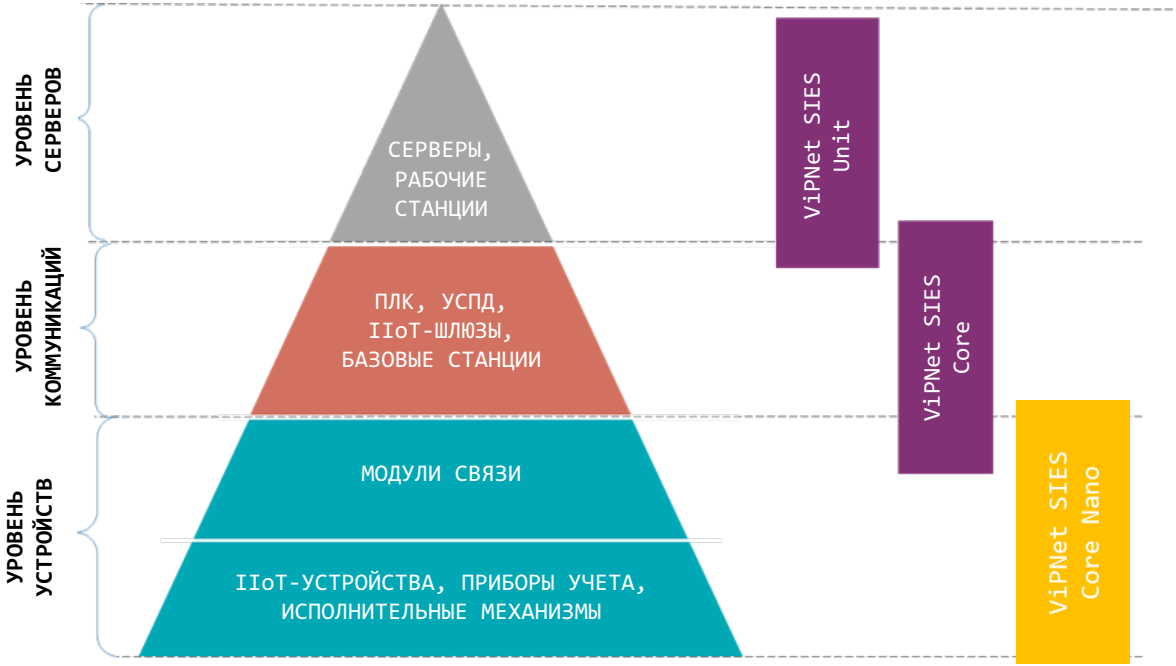
встраиваемые СКЗИ

Состав решения ViPNet SIES

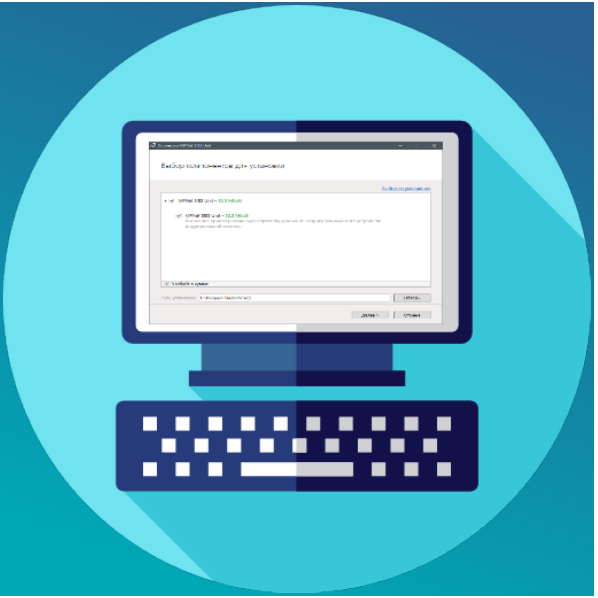


Защита данных от АСУ ТП до IIoT

СКЗИ для всех уровней АСУ ТП 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

Криптографические функции:

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

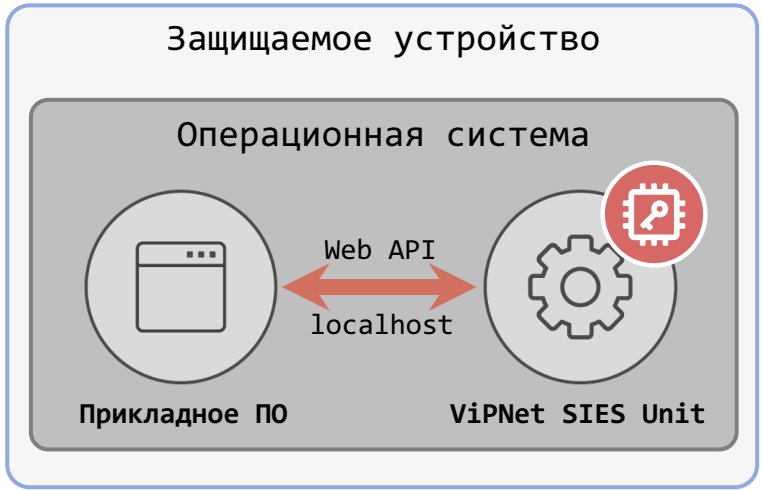
Функциональные особенности:

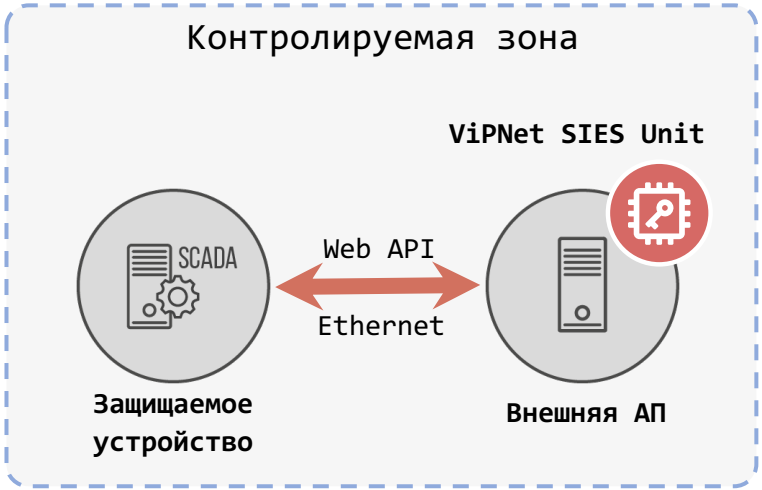
- Поддерживаемые архитектуры – x86-32, x86-64, ARM (armhf)
- Поддерживаемые ОС – Windows, Linux (Debian 9.8, 10/ Ubuntu 16, 18/Astra Linux SE 1.6, 1.7 Смоленск)
- Установка на защищаемое устройство или выделенную платформу

Соответствие требованиям:

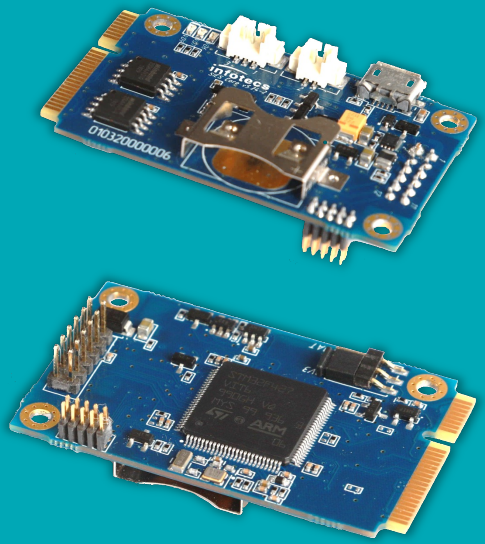
- СКЗИ класса КС1 и КС3

Интеграция ViPNet SIES Unit





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

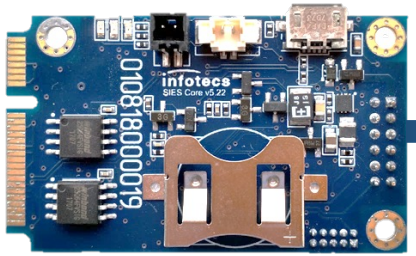
Функциональные особенности:

- 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:

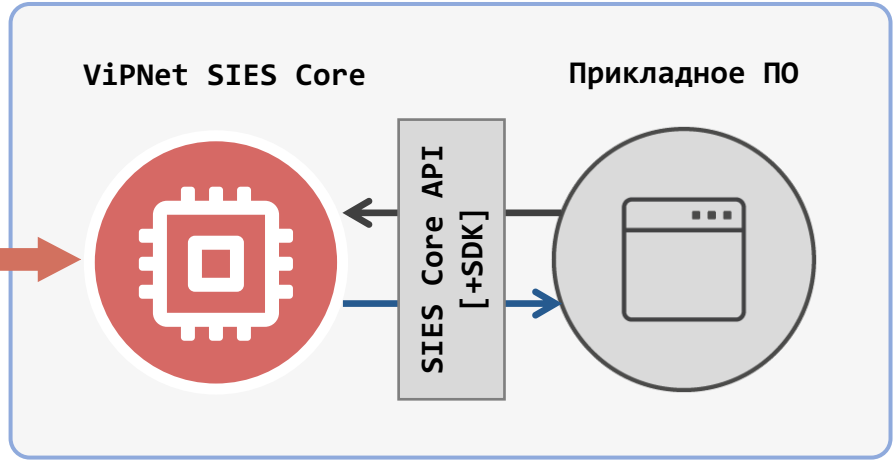
- СКЗИ класса КС3

Интеграция ViPNet SIES Core



ViPNet SIES Core

UART / USB / SPI



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

SIES Core SDK:

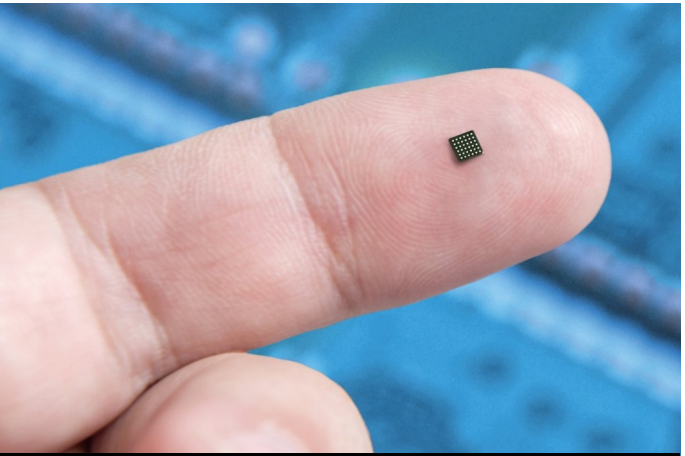
- x86-32/x86-64/ARM
- Windows
- Linux
- Baremetal (для устройств без ОС)

Данные

Защищенные данные

ViPNet SIES Core Nano

infotecs



Встраивание:

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

Криптографический протокол CRISP:

- Зашифрование/расшифрование (CRISP)
- Вычисление/проверка имитовставки (CRISP)
- Вычисление/проверка хэш-кода

Функциональные особенности:

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

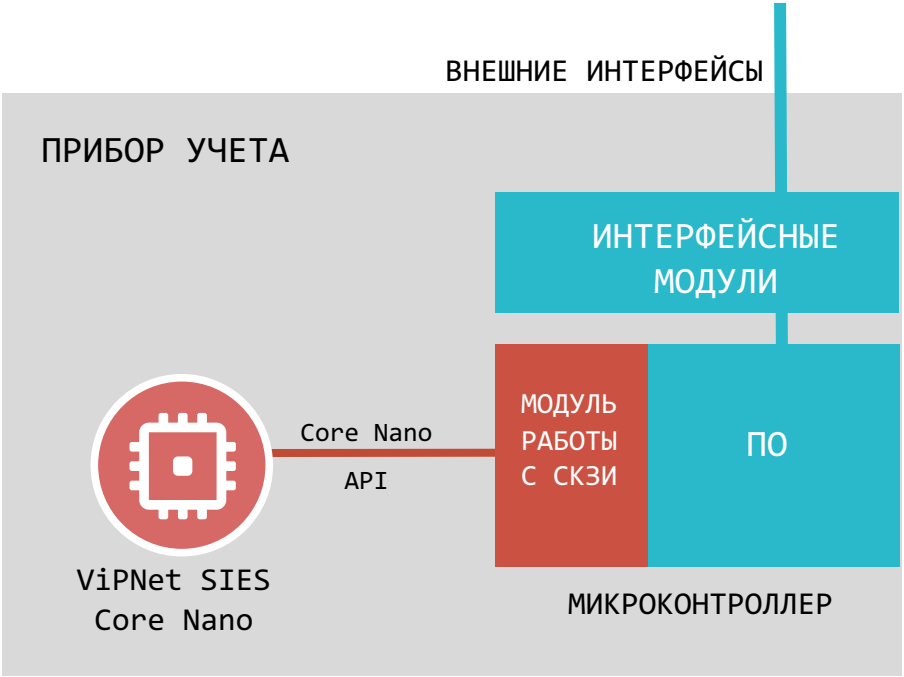
Соответствие требованиям:

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

Встраивание ViPNet SIES Core Nano в приборы учета

Интеграция на аппаратном уровне – SPI

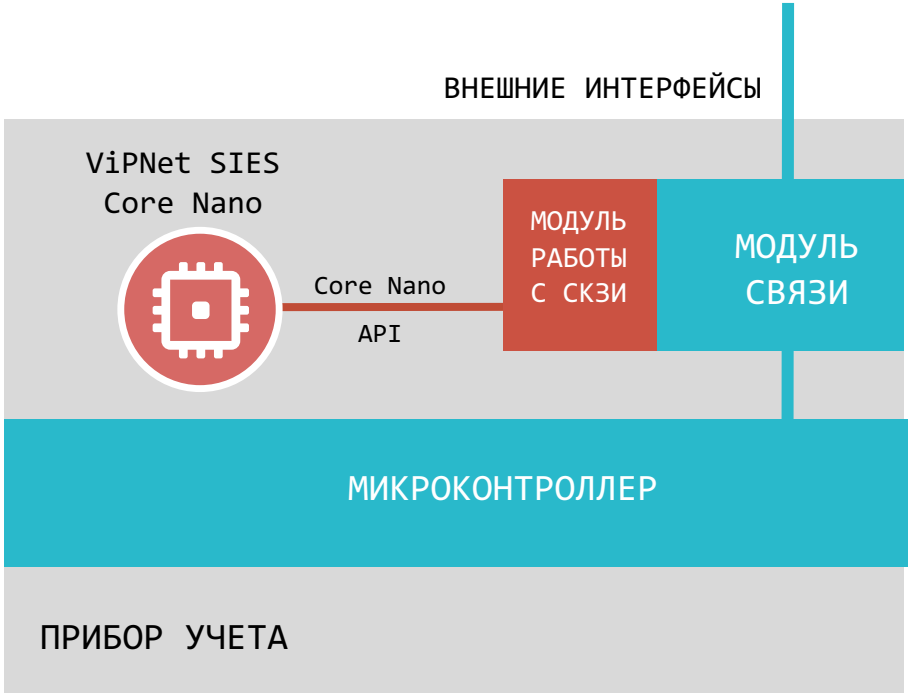
Интеграция на программном уровне – Core Nano API



Встраивание ViPNet SIES Core Nano в модули связи ПУ

Интеграция на аппаратном уровне – SPI

Интеграция на программном уровне – Core Nano API



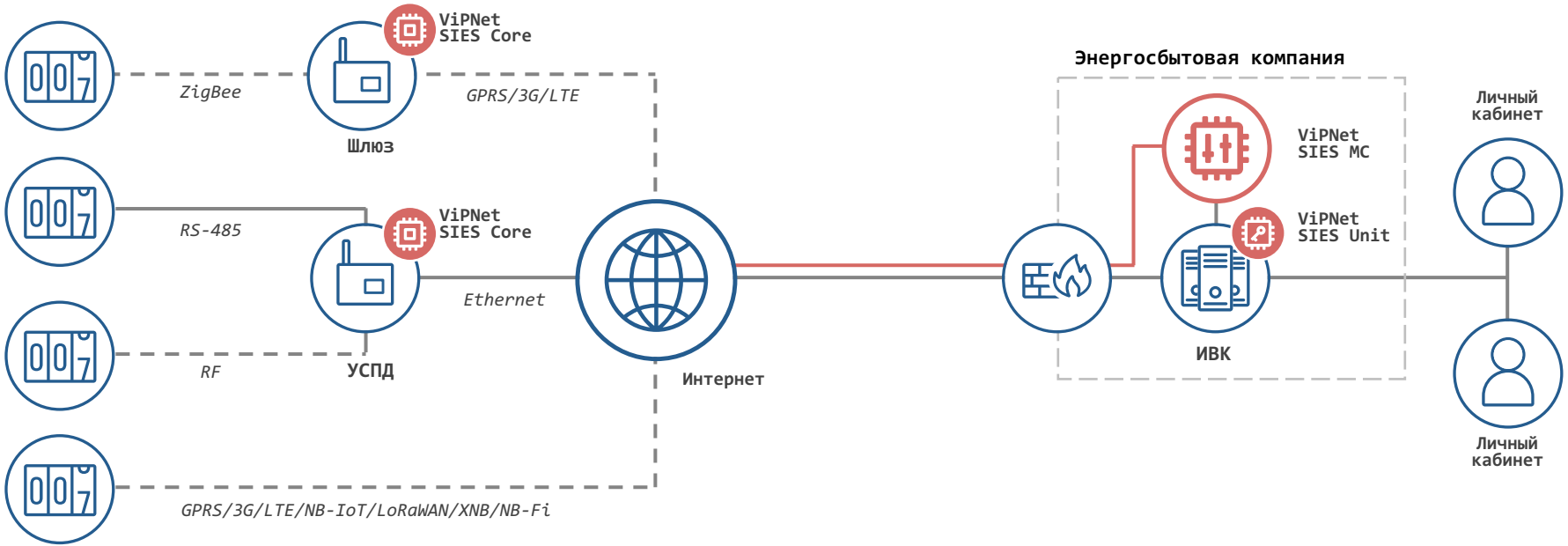
Центр управления ViPNet SIES MC

- 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

Защита данных ИСУЭ с помощью ViPNet SIES

Защита данных ИСУЭ с ViPNet SIES

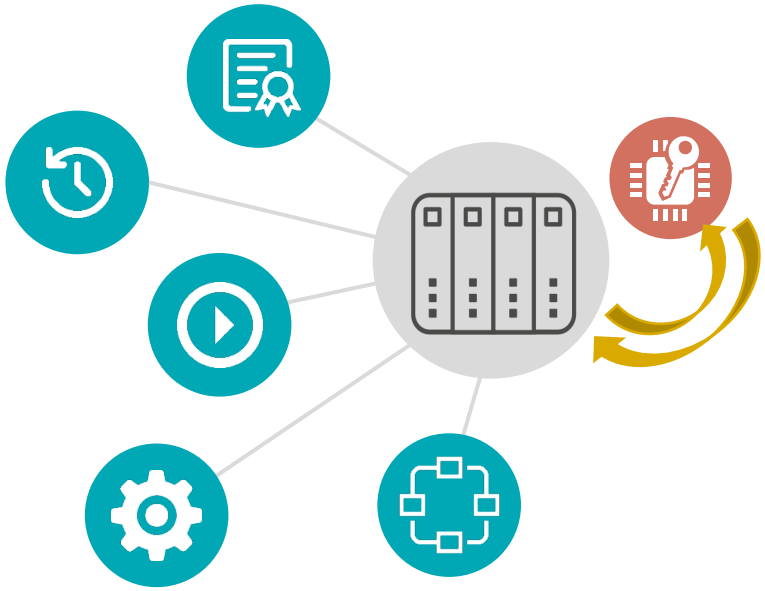


Приборы учета (ПУ) Уровень ИВКЭ Уровень ИВК

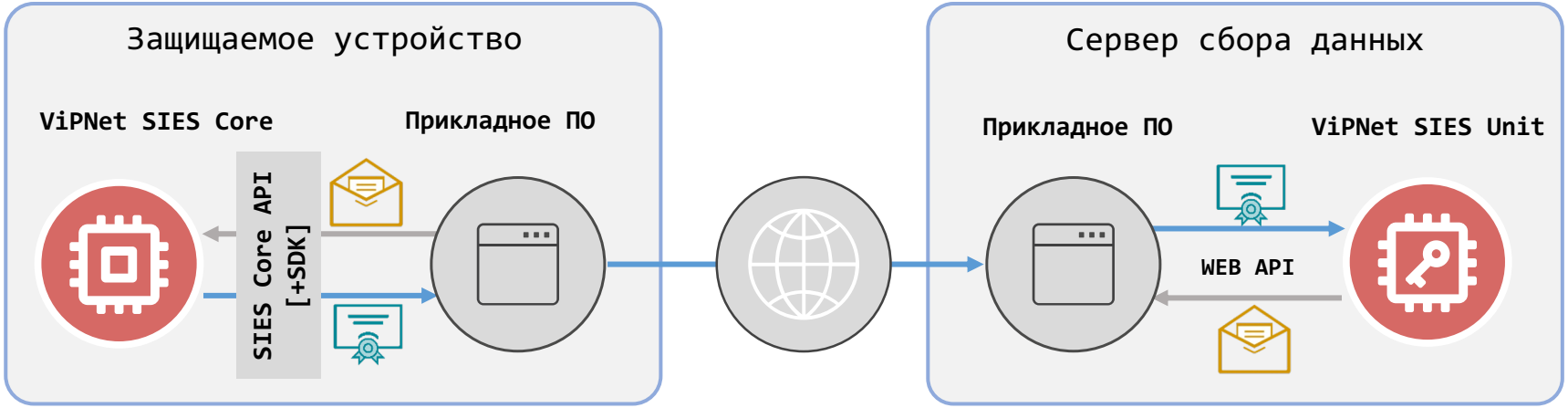
Защита информации в ИСУЭ с помощью ViPNet SIES

ViPNet SIES Core и ViPNet SIES Unit позволяют реализовывать следующие сценарии безопасности для УСПД и ИВК:

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



Защита коммуникаций с помощью ViPNet SIES



Защищенные данные

Незащищенные данные

Защита данных с помощью протокола CRISP

- Целостность
- Конфиденциальность (опционально)
- Защита от навязывания повторных сообщений
- Аутентификация источника сообщений

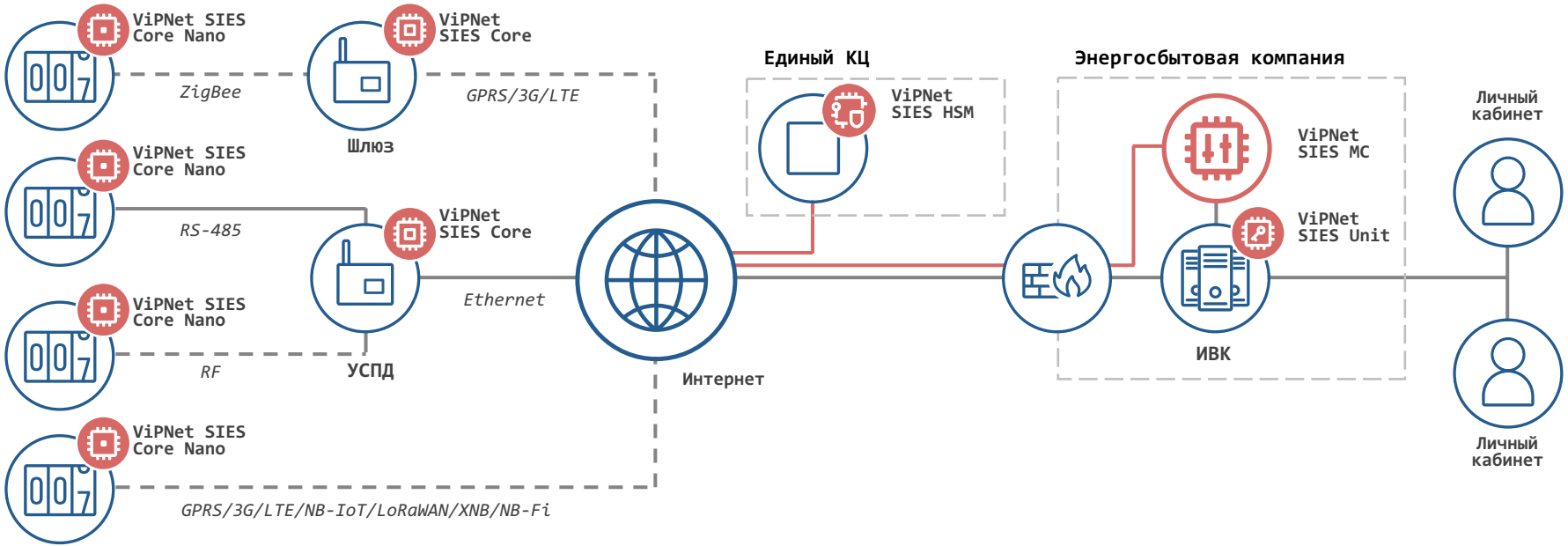
* Протокол CRISP (Р 1323565.1.029-2019) входит в перечень рекомендованных Минцифрой протоколов для ИСУЭ

infotecs

- Защита адресных и групповых сообщений
- Бессесионный криптографический протокол
- Минимальные накладные расходы (overhead)и минимальная нагрузка на сеть
- Универсальный стандартизированный протокол защиты любых протоколов ИСУЭ

RS-485 GSM PLC ETHERNET XNB EXTENDED NARROWBAND ZigBee LoRaWAN RF NB-IoT

Защита данных в ИСУЭ до уровня ПУ



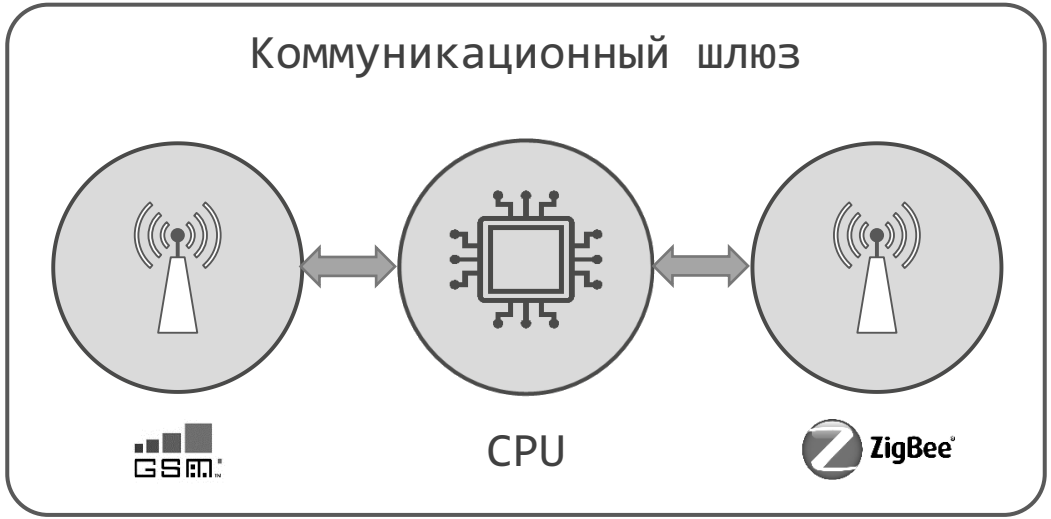
Приборы учета (ПУ) Уровень ИВКЭ Уровень ИВК

Встраивание ViPNet SIES Core в компоненты ИСУЭ

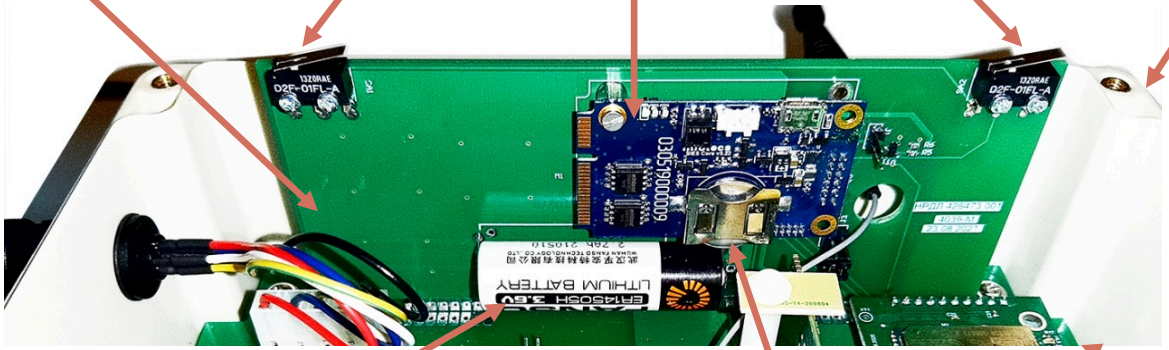
Этапы встраивания СКЗИ

- Подготовка к встраиванию СКЗИ
- Встраивание СКЗИ в защищаемое устройство
- Проведение испытаний защищаемого устройства с встроенным СКЗИ
- Оценка влияния защищаемого устройства на СКЗИ
- Обеспечение требований и условий работы с СКЗИ
- Производство

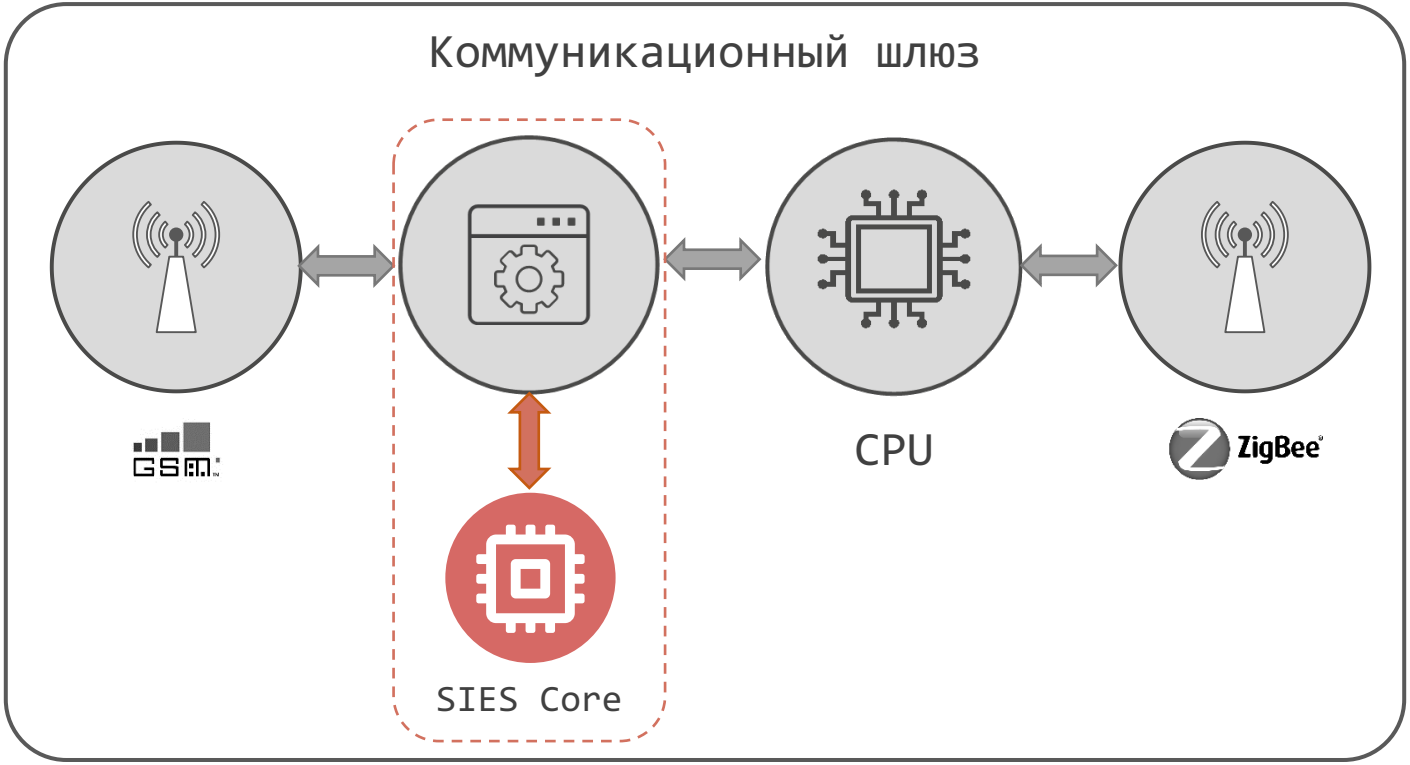
Коммуникационный шлюз НТЦ НАРТИС



Интеграция с модулем СКЗИ



Интеграция с модулем СКЗИ



Оценка влияния

- Подготовка ТЗ на оценку влияния
- Согласование ТЗ на оценку влияния с испытательной лабораторией
- Согласование ТЗ на оценку влияния с ФСБ России
- Передача материалов и стенда в исследовательскую лабораторию для проведения работ по оценке влияния
- Направление исследовательской лабораторией результатов исследований на экспертизу в ФСБ России
- Получение результатов экспертизы в ФСБ России

Решение ViPNet SIES для ИСУЭ

Соответствие Базовой МИУН ИСУЭ и требованиям первого этапа по внедрению СКЗИ в ИСУЭ

Защита информации с помощью рекомендованного Министерством цифрового развития криптографического протокола CRISP

Законченное решение со всеми необходимыми элементами – компоненты для внедрения в УСПД, компоненты для интеграции с ИВК, центр генерации ключей

infotecs

Спасибо за внимание!

Алексей Власенко

Менеджер отдела развития продуктов

e-mail: Aleksey.Vlasenko@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

t.me/infotecs_news

rutube.ru/channel/24686363