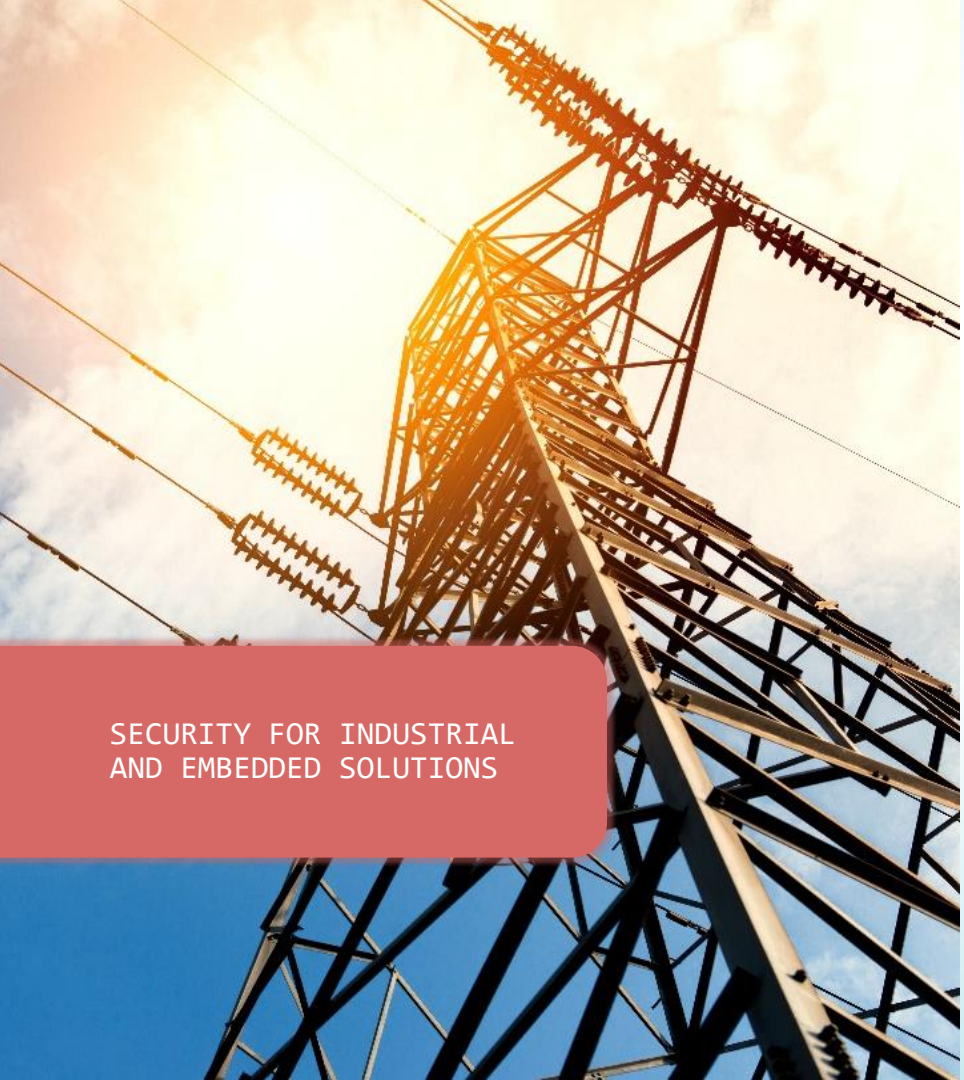
Встраиваемая криптография для промышленных систем. Новое в решении ViPNet SIES

Алексей Власенко
ведущий менеджер продуктов

infotecs

Решение ViPNet SIES

Немного теории

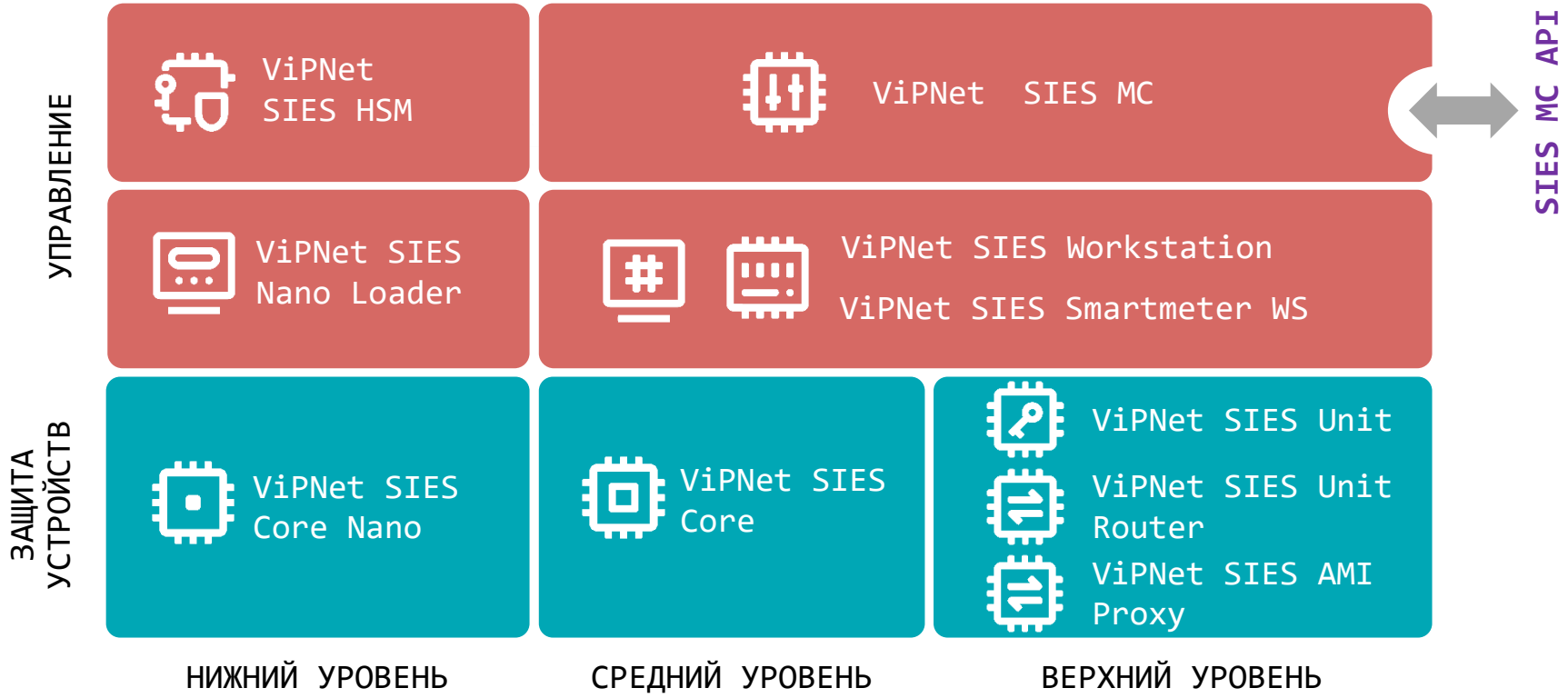


Решение ViPNet SIES

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

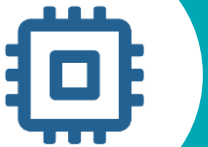
ПАК ViPNet SIES MC IoT
- До 2 млн устройств
- СКЗИ класса КС3

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

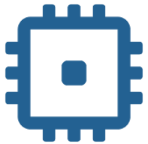
SIES-узлы

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

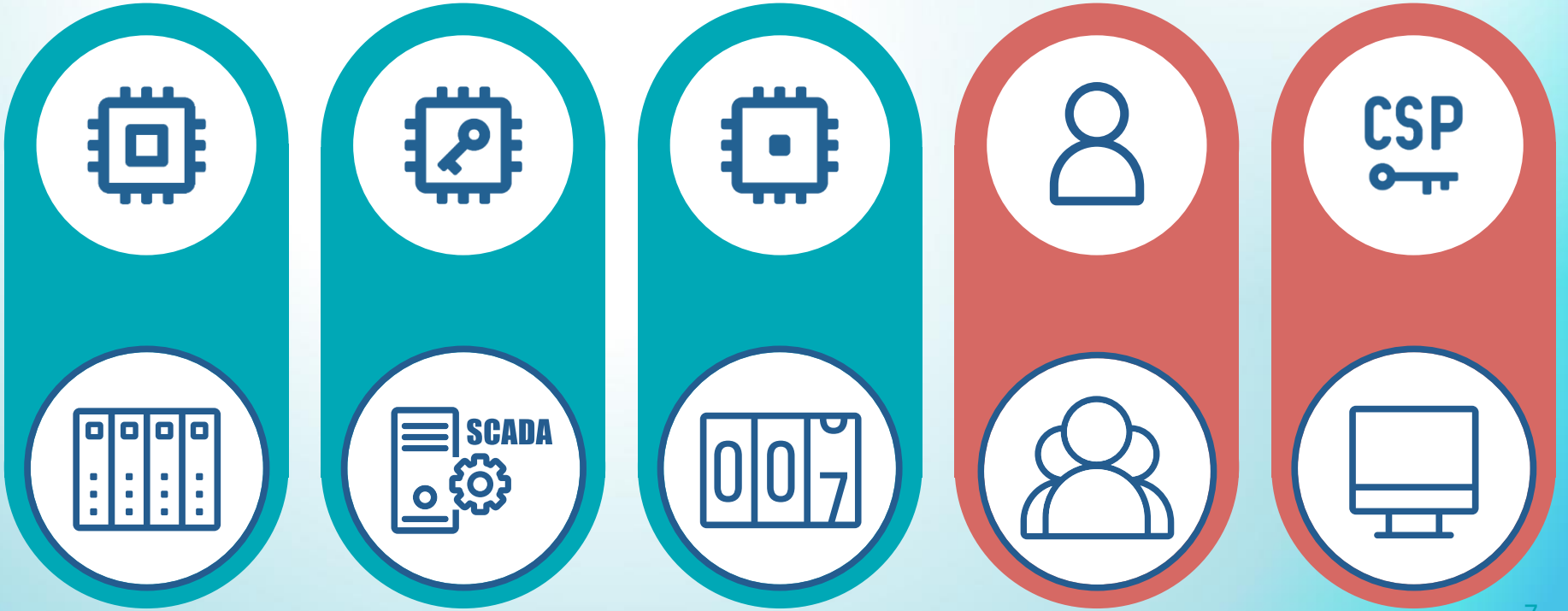
Токены/смарт-карты сервисного инженера, инженера КИП и др.

Другой SIES-узел

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

Защищаемые устройства

Средства обработки информации, интегрированные с SIES-узлами



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

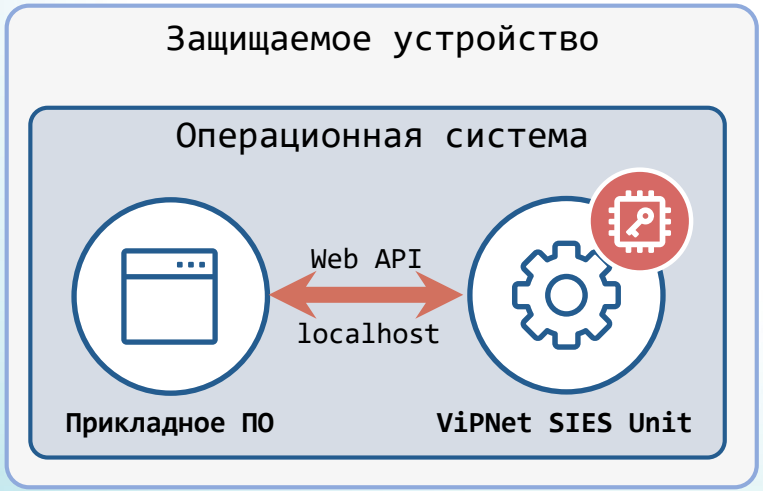
Функциональные особенности

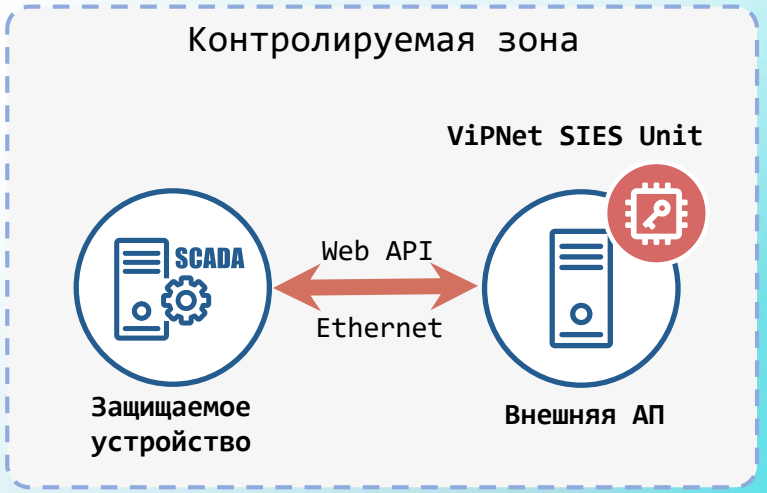
- Поддерживаемые архитектуры: x86-32, x86-64, ARM
- Поддерживаемые ОС: Windows, Linux, Astra Linux, Альт СП
- Установка на защищаемое устройство или выделенную платформу

Соответствие требованиям

- СКЗИ класса КС1 и КС3

Интеграция ViPNet SIES Unit





ViPNet SIES Unit Router

Функции

- Повышение производительности ViPNet SIES Unit
- Распределение запросов на выполнение криптографических операций между несколькими ViPNet SIES Unit
- Обеспечивает единую точку входа для подключения множества защищаемых устройств к нескольким ViPNet SIES Unit
- Автоматическая генерация таблицы маршрутизации запросов
- Резервирование ViPNet SIES Unit

Функциональные особенности

- Программный комплекс работает как служба ОС
- Поддержка резервирования (кластер ViPNet SIES Unit Router)
- Поддерживаемые архитектуры: x86-64
- Поддерживаемые ОС: Astra Linux, Альт СП

Соответствие требованиям

- Не является СКЗИ и не подлежит обязательной сертификации

ViPNet SIES AMI Proxy

Функции

- Обеспечение криптографической защиты данных для протоколов СПОДЭС/СПОДУС
- Автоматическое наложение и снятие криптографической защиты данных при помощи ViPNet SIES Unit
- Обеспечивает единую точку подключения к ИВК ИСУЭ по протоколам СПОДЭС/СПОДУС
- Обеспечивает совместимость продуктов ViPNet SIES с ИВК различных производителей, поддерживающих СПОДЭС/СПОДУС

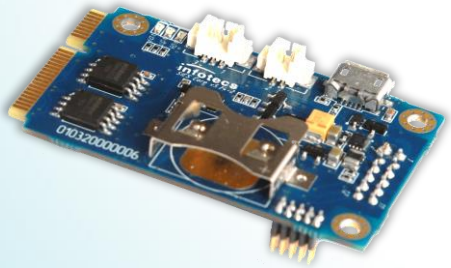
Функциональные особенности

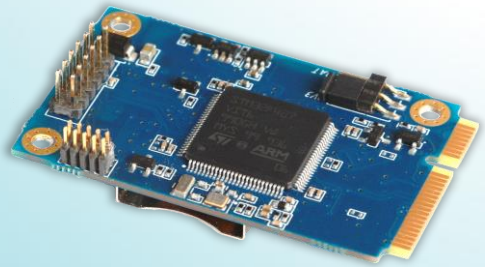
- Программный комплекс работает как служба ОС
- Стоит в разрыв связи перед ИВК ИСУЭ, перехватывая данные
- Прозрачный режим при взаимодействии ИВК с ИВКЭ и ПУ
- Поддерживаемые архитектуры: x86-64
- Поддерживаемые ОС: Astra Linux, Альт СП, Debian

Соответствие требованиям

- Не является СКЗИ и не подлежит обязательной сертификации

ViPNet SIES Core





Встраивание

- На аппаратном уровне – UART, USB, SPI, I2C
- Подключение – разъем PLD2, USB-micro, **Mini PCI-E**
- 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

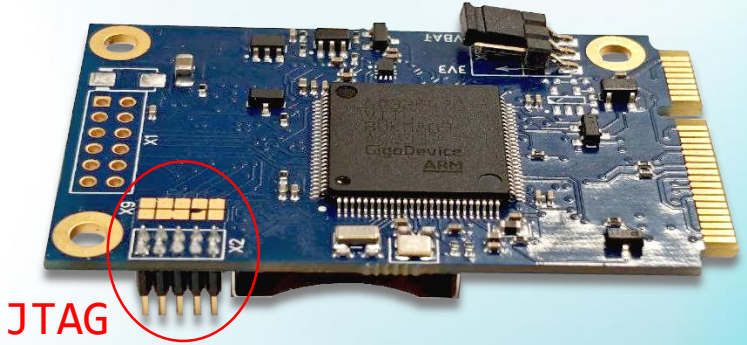
Функциональные особенности

- Форм-фактор – плата PCI Express® Full-Mini Card
- Поддержка ДНСД для эксплуатации вне контролируемой зоны
- Рабочий диапазон температур -40…+70^{0}C

Соответствие требованиям

- СКЗИ класса КС3

Исполнения ViPNet SIES Core



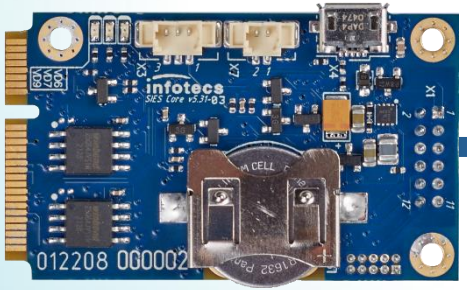
ViPNet SIES Core

- АП SIES Core I2 (STM32)
- АП SIES Core I4 (GD32)

ViPNet SIES Core PCIe

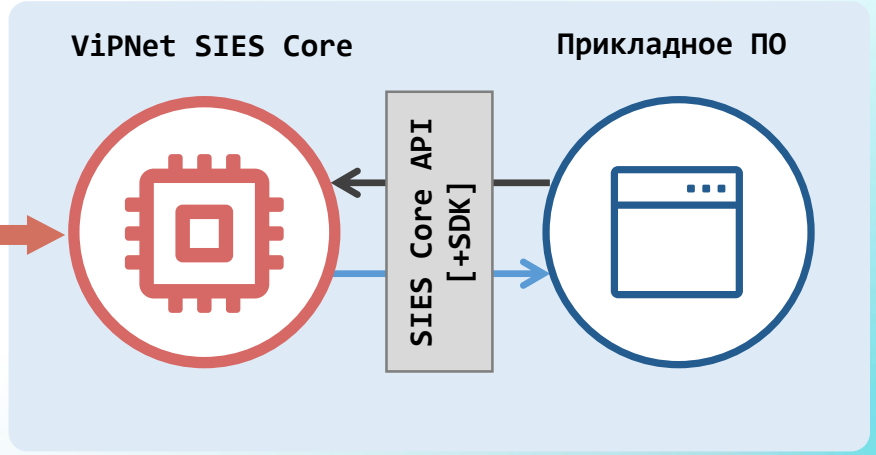
- АП SIES Core I5 (STM32)
- АП SIES Core I6 (GD32)

Интеграция ViPNet SIES Core



ViPNet SIES Core

UART/USB/SPI/I2C

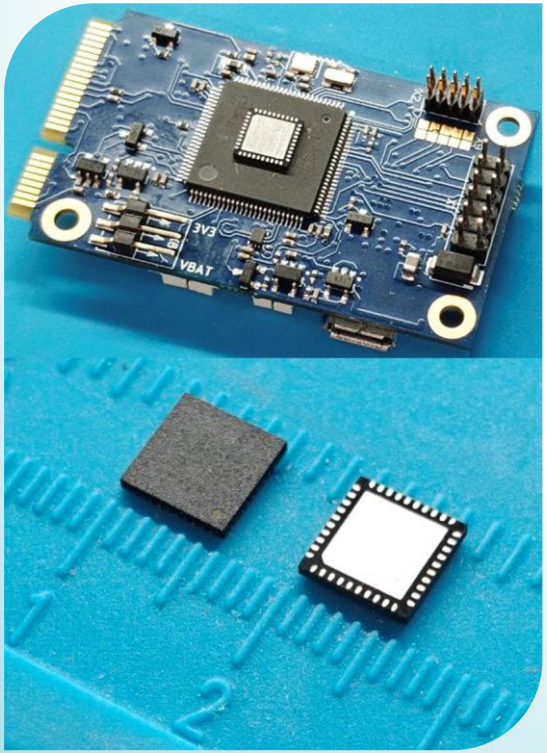


Защищаемое устройство
(ПЛК, УСПД, УСО, шлюз и т.п.)

Данные

Защищенные данные

ViPNet SIES Core Nano



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

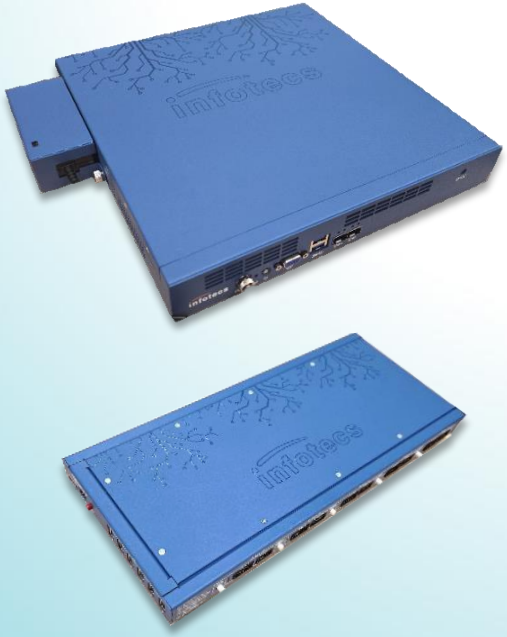
Криптографические функции
- Зашифрование/расшифрование (CRISP)
- Вычисление/проверка имитовставки (CRISP)
- Вычисление/проверка хэш-кода

Функциональные особенности
- 3 резервируемых ключа связи
- Хранение ключевой информации до 16 лет
- Рабочий диапазон температур -40^{0}C…+85^{0}C
- Форм-фактор – микросхема **QFN40**
- Эксплуатация вне контролируемой зоны

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

ViPNet SIES Nano Loader

автоматизированное рабочее место подготовки к эксплуатации ViPNet SIES Core Nano



Функции

- Проверка целостности ПО
- Загрузка ПО в ViPNet SIES Core Nano
- Контроль серийного номера ViPNet SIES Core Nano
- Запрос ключевой информации из ViPNet SIES HSM
- Загрузка ключевой информации в ViPNet SIES Core Nano
- Экспорт данных о подготовленных ViPNet SIES Core Nano

Функциональные особенности

- Форм-фактор: ViPNet SIES Nano Loader (настольный ПК) + ViPNet SIES Nano Array Adapter (оснастка для подключения ViPNet SIES Core Nano)
- Одновременная подготовка до 10 ViPNet SIES Core Nano

Соответствие требованиям

- СКЗИ класса КС3

Комплекс ViPNet SIES HSM

Исполнение 1: стандартное исполнение

Исполнение 2: исполнение с резервированием

Долговременное защищенное хранение ключевой информации ViPNet SIES Core Nano

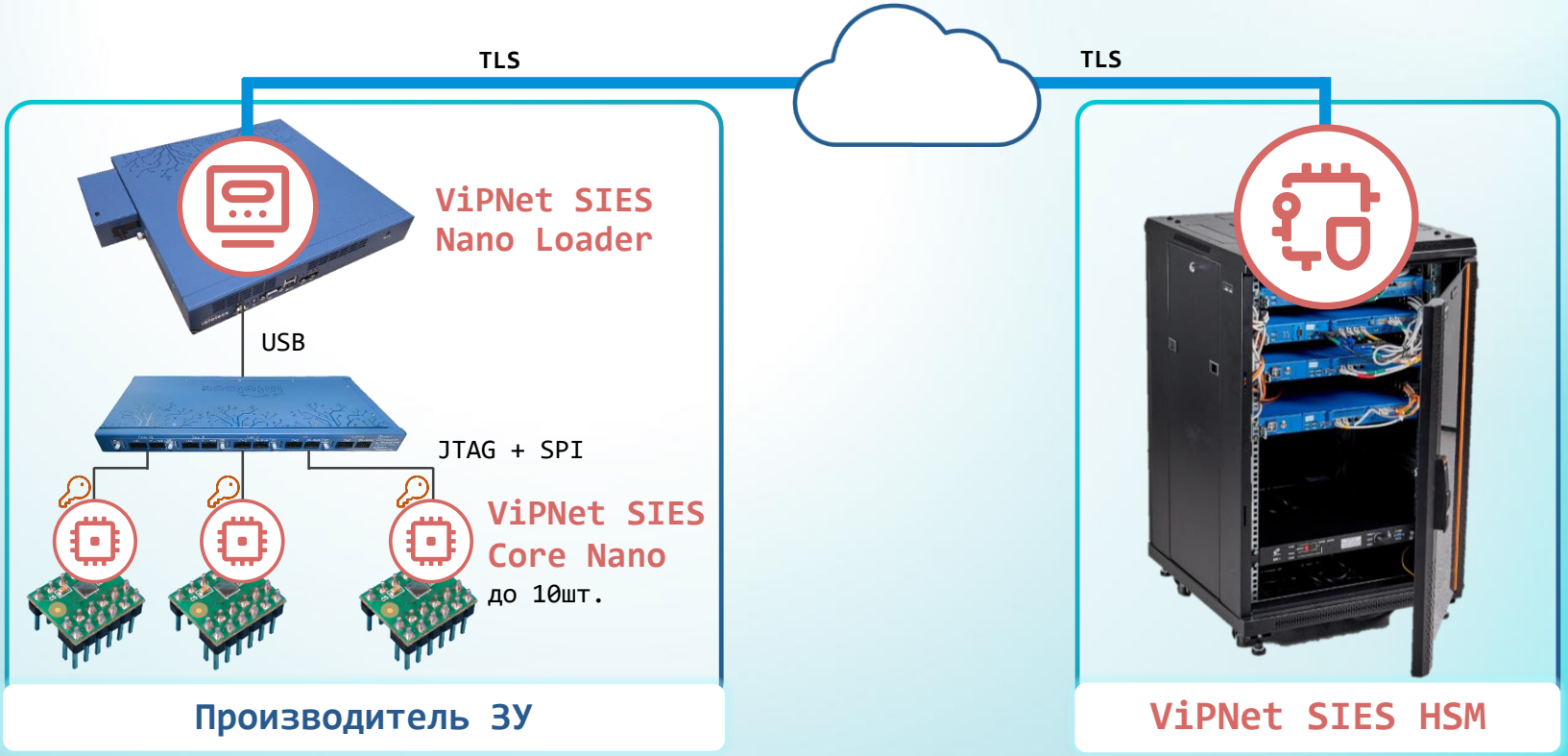
Регистрация производителей устройств и их АРМ ViPNet SIES Nano Loader

Генерация и предоставление ключевой информации по запросу ViPNet SIES Nano Loader

Предоставление ключевой информации по запросу ViPNet SIES MC

Хранение БД соответствия серийного номера устройства, СКЗИ и загруженных ключей

Производство устройств с ПАК ViPNet SIES Core Nano



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

Ключи загружаются на заводе, изготавливающем устройство, с помощью ViPNet SIES Nano Loader

Средство генерации ключей – ViPNet 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

ViPNet SIES Core Nano: временные и групповые ключи

Генерация и смена ключей во время эксплуатации

Загрузка через ViPNet SIES MC

Временные симметричные ключи для обмена данными между устройствами со сроком действия до 1 года (до 20 ключей)

Средство генерации ключей – ViPNet SIES MC

Групповой (мультивещательный) ключ со сроком действия до 16 лет

Средство генерации ключей – ViPNet SIES HSM

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

Работа с защищаемыми устройствами и SIES-узлами

Задачи

- Добавление SIES-узла в ViPNet SIES MC
- Регистрация защищаемого устройства в ViPNet SIES MC
- Создание связей между защищаемыми устройствами
- Изменение связей между защищаемыми устройствами
- Изменение атрибутов SIES-узлов и защищаемых устройств

Для большого количества устройств

- Получение карты сети из внешней ИС
- Регистрация защищаемых устройств в ViPNet SIES MC на основе карты сети

Продукты и средства работы с SIES-узлами

- ViPNet SIES Workstation
- ViPNet SIES Smartmeter WS
- ViPNet SIES MC Mapper

ViPNet SIES Workstation

программный комплекс для АРМ инициализации и локального обслуживания SIES-узлов

Инициализация ViPNet SIES Core

- Настройка интерфейса сопряжения с защищаемым устройством: выбор SPI или UART, настройка параметров UART
- Загрузка первичной ключевой информации
- Настройка служебной ключевой системы
- Регистрация SIES-узла в ViPNet SIES MC

Инициализация ViPNet SIES Unit

- Загрузка первичной ключевой информации
- Настройка служебной ключевой системы
- Регистрация SIES-узла в ViPNet SIES MC

Обслуживание ViPNet SIES Core

- Управление ViPNet SIES Core в режимах штатный, конфигурирование, блокировка
- Трансляция защищенных служебных конвертов от ViPNet SIES MC

ViPNet SIES Smartmeter WS

программный комплекс для автоматизированного ввода в эксплуатацию защищаемых устройств (ЗУ) с ViPNet SIES Core в информационных системах (ИС) с топологией «звезда»

Функции

- Автоматическая инициализация ViPNet SIES Core, ассоциация с ЗУ и регистрация в ViPNet SIES MC
- Автоматическое создание связей между ЗУ и центральным сервером с ViPNet SIES Unit, загрузка прикладной ключевой информации в ViPNet SIES Core
- Активация ДНСД после подготовки ЗУ с ViPNet SIES Core
- Формирование отчетов о подготовленных ЗУ с ViPNet SIES Core

Функциональные особенности

- Поддержка парных и резервированных связей
- Возможность поточной работы с 8 ЗУ и ViPNet SIES Core
- Поддержка ОС Linux и Windows

ViPNet SIES MC Mapper

ПО для автоматического создания карты взаимодействия защищаемых устройств в центре управления ViPNet SIES MC

Функции

- Импорт карты сети из внешней ИС в ViPNet SIES MC
- Регистрация ViPNet SIES Core Nano в ViPNet SIES MC
- Регистрация защищаемых устройств в ViPNet SIES MC и ассоциация с ViPNet SIES Core Nano
- Автоматическое создание связей между ЗУ с ViPNet SIES Core Nano и центральным сервером на основе карты сети

Как упростить встраивание?

Расширения и инструменты для разработчиков

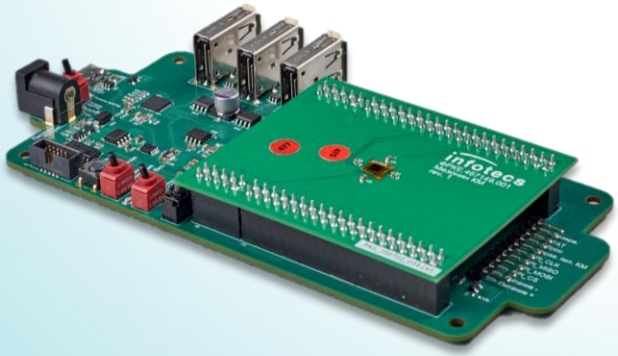
Комплект разработчика ViPNet SIES Development kit

Исполнение 1	Исполнение 2	Исполнение 3	Исполнение 4
ViPNet SIES Core (2 модуля)	ViPNet PKI Client с TLS Unit	ViPNet SIES Core (2 модуля)	ViPNet PKI Client с TLS Unit
ViPNet SIES Core SDK	ViPNet SIES Unit	ViPNet SIES Core SDK	ViPNet SIES Unit
ViPNet SIES Workstation	ViPNet SIES MC VA	ViPNet SIES Workstation	Подключение к ИнфоТеКС ViPNet SIES MC
ViPNet SIES Unit		ViPNet SIES Unit	
ViPNet PKI Client с TLS Unit		ViPNet PKI Client с TLS Unit	
ViPNet SIES MC VA		Подключение к ИнфоТеКС ViPNet SIES MC	

Паспорт, комплект пользовательской и эксплуатационной документации

Комплект разработчика ViPNet SIES Core Nano DevKit

для разработчиков защищаемых устройств, ведущих работы по встраиванию ViPNet SIES Core Nano



Состоит из

- модуля SIES Core Nano Adapter;
- мезонинной платы с распаянным SIES Core Nano

Комплект разработчика позволяет

- ознакомиться с возможностями продукта ViPNet SIES Core Nano;
- разработать и отладить ПО защищаемого устройства для взаимодействия с ViPNet SIES Core Nano;
- реализовать сценарии защиты информации защищаемого устройства;
- подготовить стенд для проверки реализованных сценариев защиты информации;
- разработать конструкторскую, доработать пользовательскую и эксплуатационную документацию с учётом использования СКЗИ

Инструменты для встраивания в защищаемые устройства

- **SIES Core/Unit SDK** – готовые библиотеки для устройств с ОС Windows, Linux с архитектурами x86-32, x86-64, ARM
- **SIES Core/Core Nano SDK Baremetal** – компилируемые библиотеки в исходных кодах для устройств без ОС
- **ViPNet SIES Core Agent** – сервис для ARM устройств с ОС Linux, обеспечивающий взаимодействие с центром управления ViPNet SIES MC
- **ViPNet SIES Core Service** – сервис для защиты протоколов СПОДЭС/СПОДУС в ARM устройствах (УСПД) с ОС Linux

Применение в промышленных системах

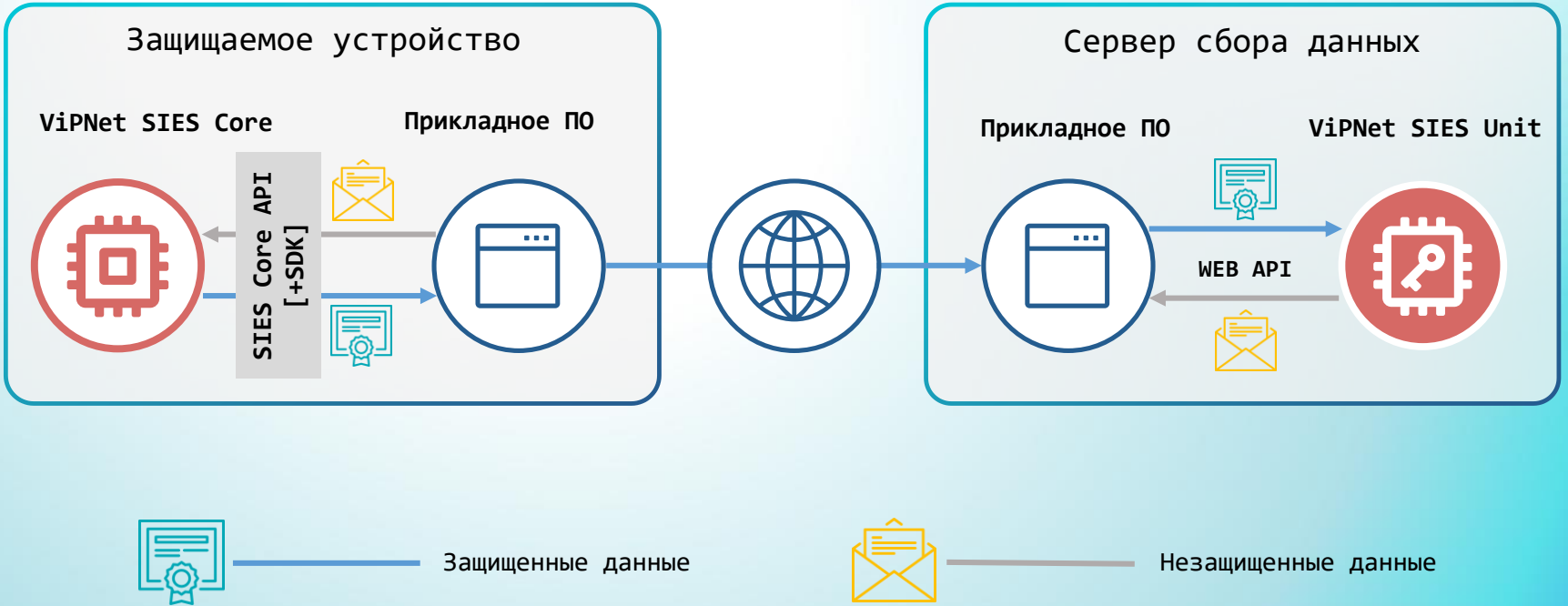
Что и как можно защитить

Криптографические сервисы для защищаемых устройств

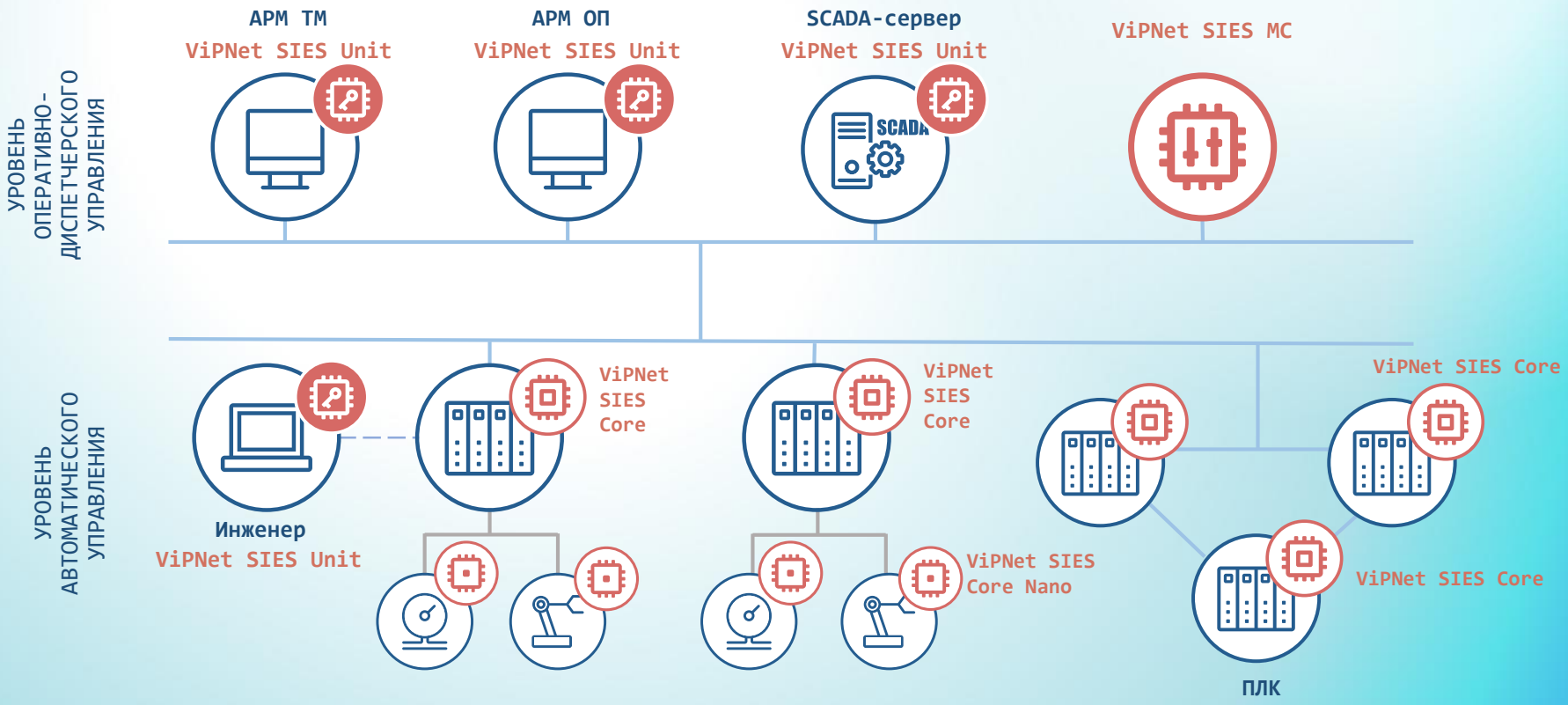
Компоненты решения ViPNet SIES позволяют реализовывать следующие сценарии обеспечения информационной безопасности защищаемых устройств:

- 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

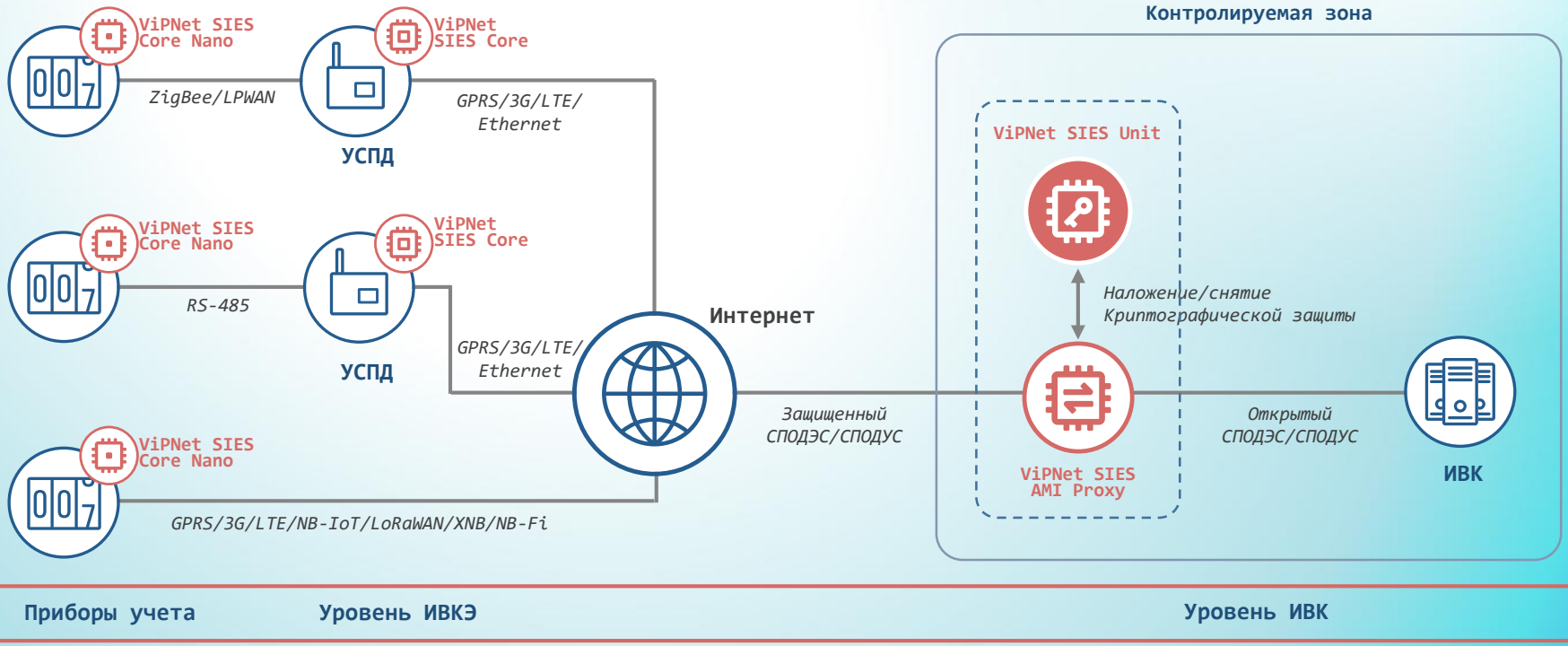
Защита коммуникаций с помощью ViPNet SIES



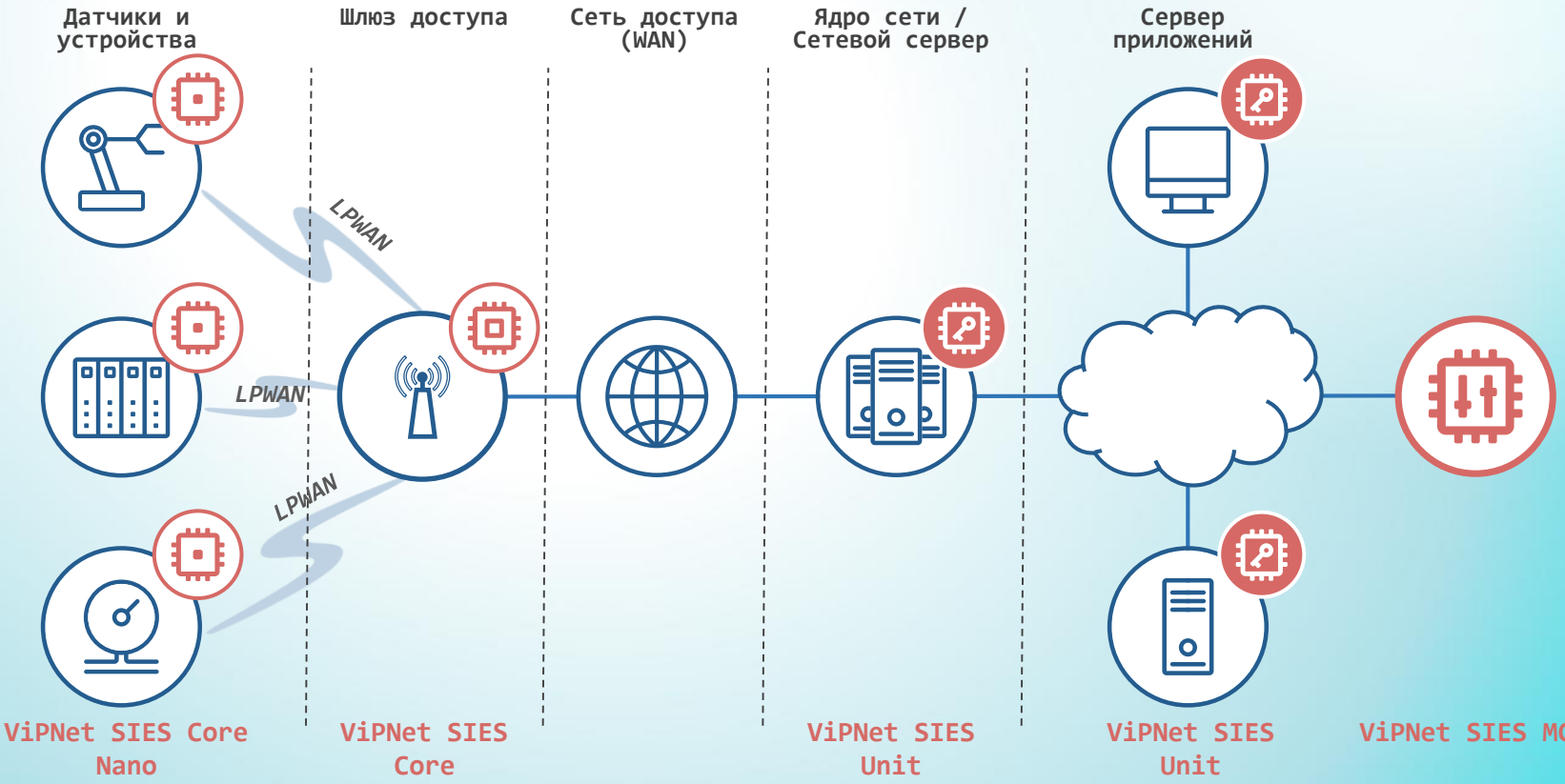
Защищенная АСУ ТП



Защита данных в ИСУЭ



Защита данных в IIoT-системе



Масштабирование ViPNet SIES Unit

Масштабирование ViPNet SIES Unit

Масштабирование ViPNet SIES Unit

Подписывайтесь
на наши соцсети,
там много интересного

infotecs