Малы, да удалы. Встраиваемые СКЗИ ViPNet SIES

Алексей Власенко

Ведущий менеджер продуктов

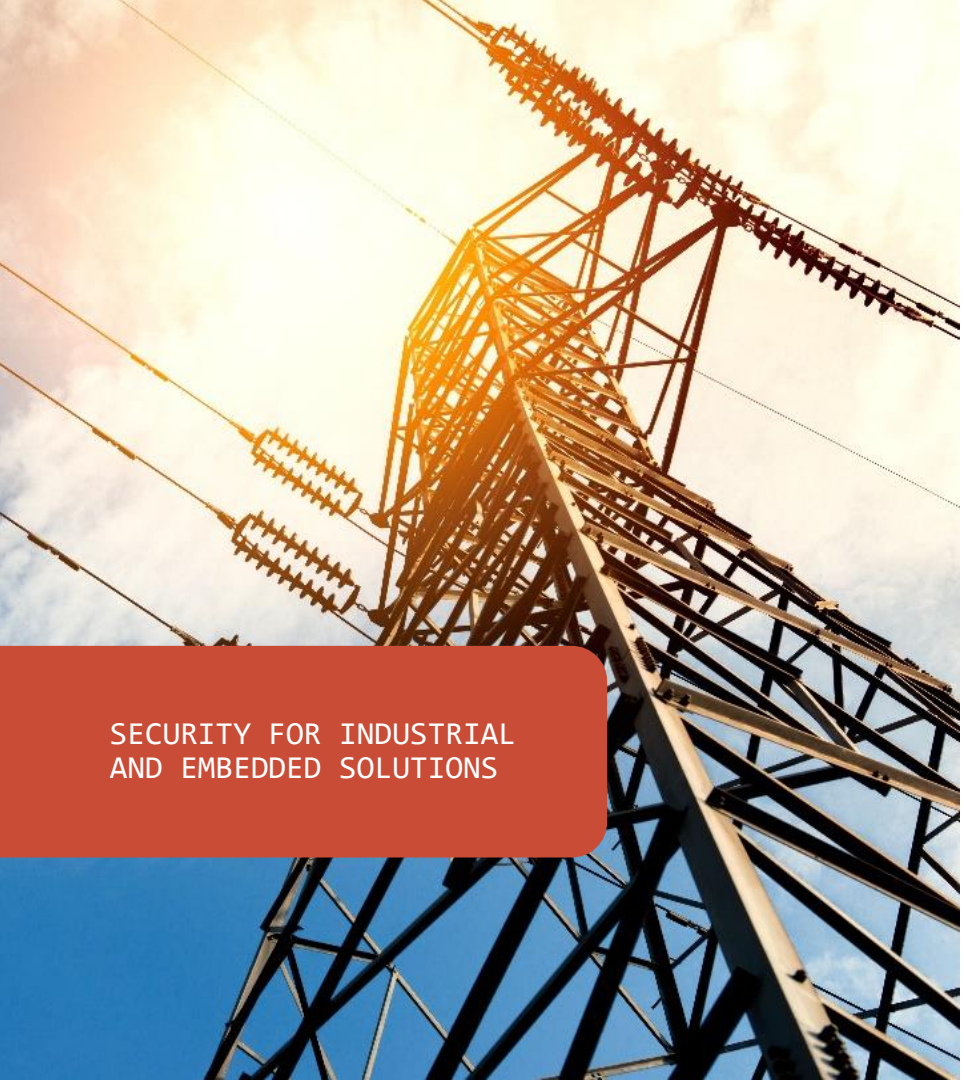
инфотекс ТЕХНОДЕСТ

Белый поток

Решение ViPNet SIES

Немного теории

инфотекс

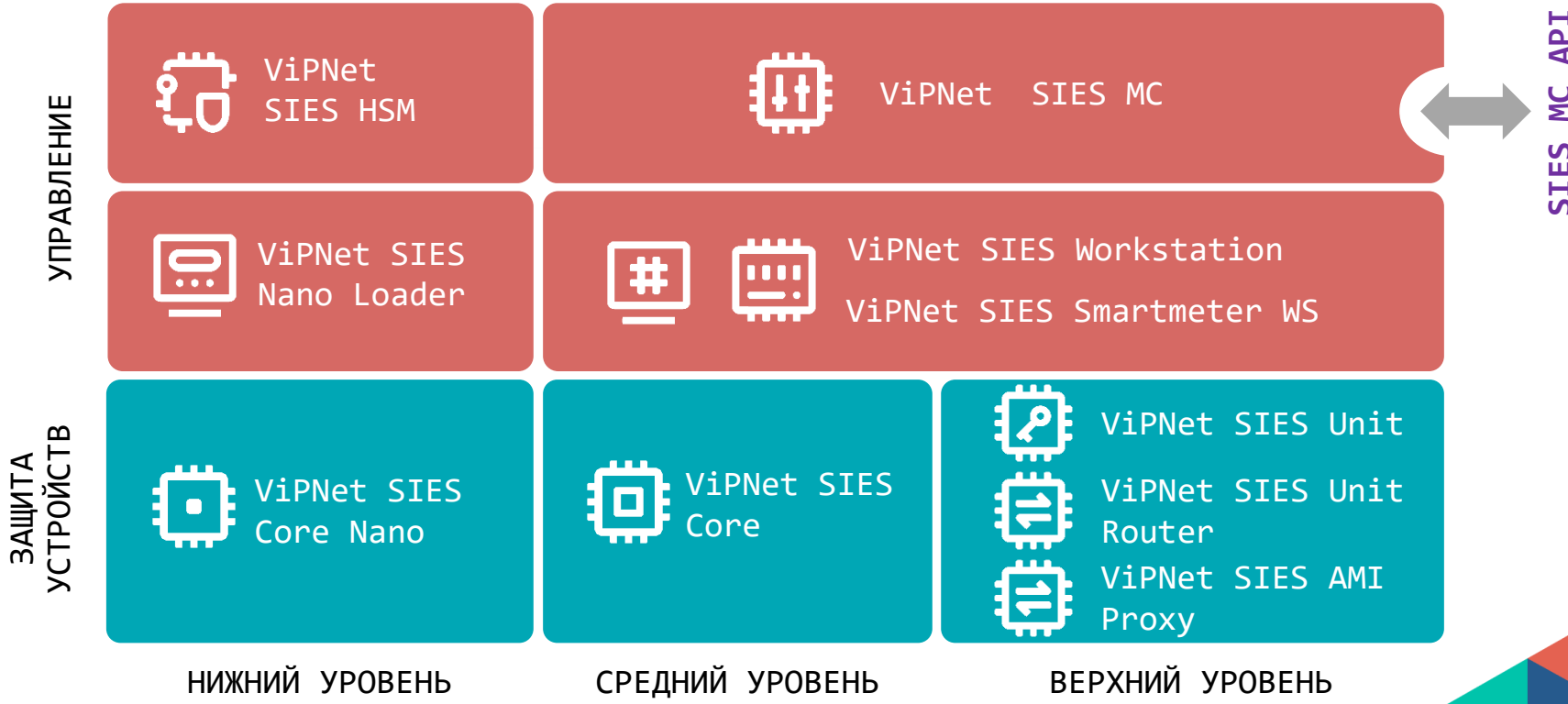


Решение ViPNet SIES

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

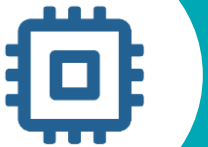
ПАК ViPNet SIES MC IoT
- До 2 млн устройств
- СКЗИ класса КС3

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

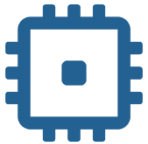
SIES-узлы

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

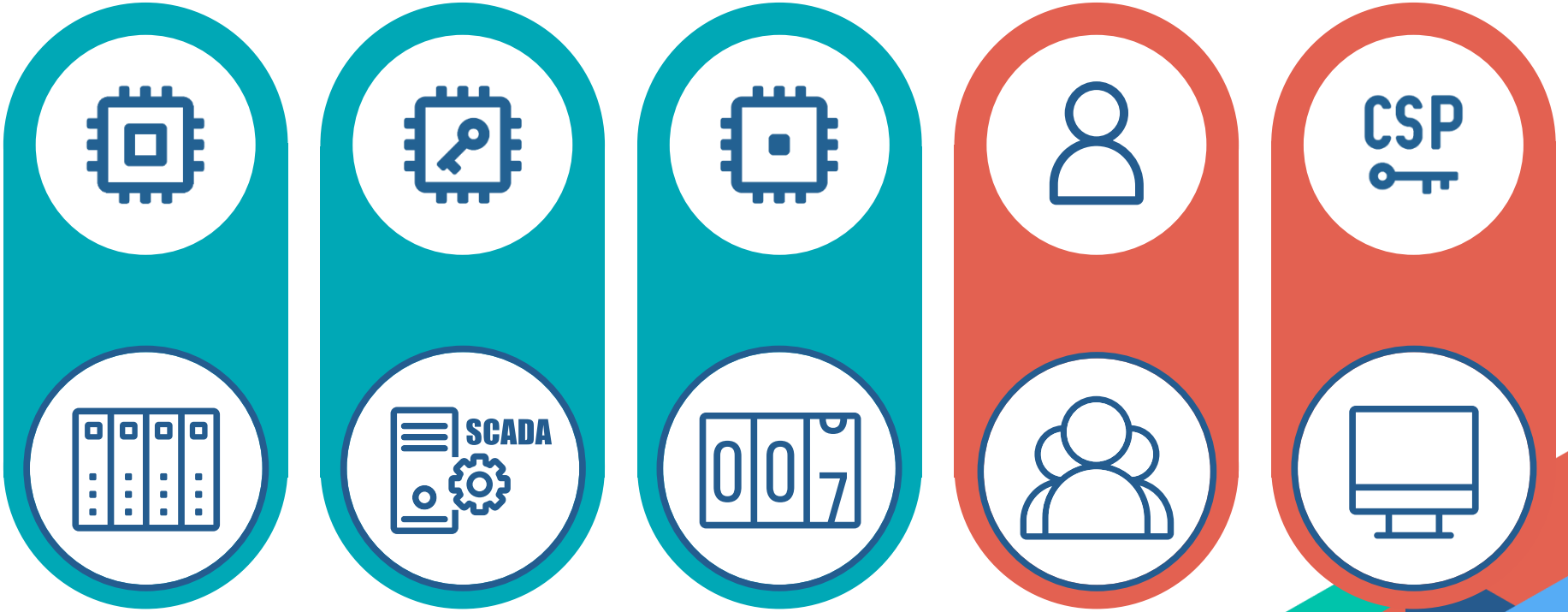
Токены/смарт-карты сервисного инженера, инженера КИП и др.

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

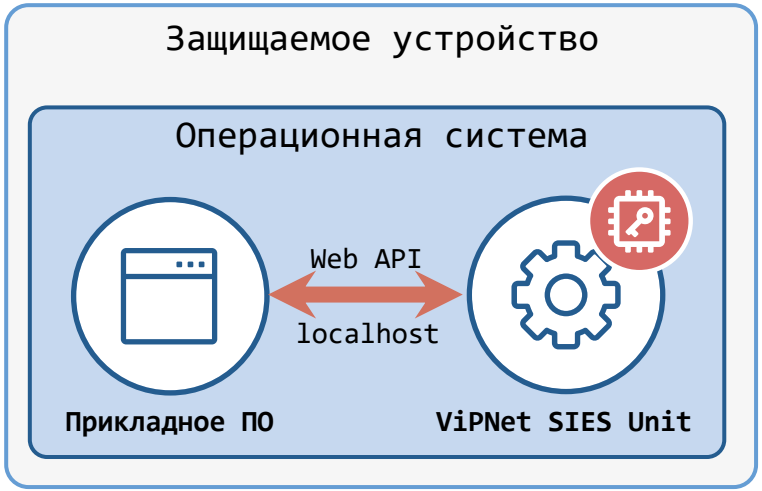
Функциональные особенности

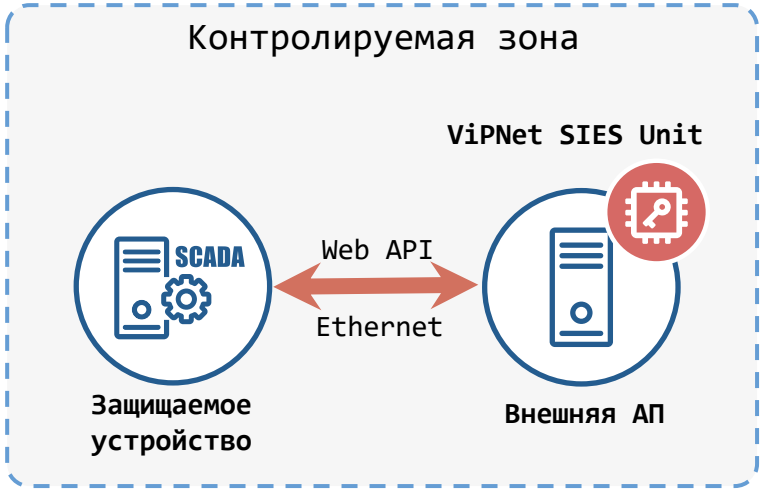
- Поддерживаемые архитектуры: x86-32, x86-64, ARM
- Поддерживаемые ОС: Windows, Linux, Astra Linux, Альт СП
- Установка на защищаемое устройство или выделенную платформу

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

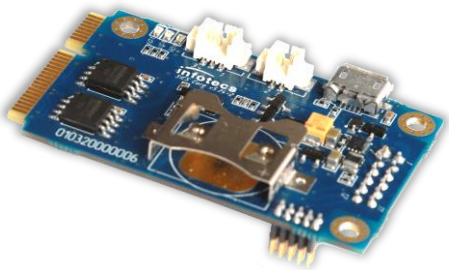
Функциональные особенности

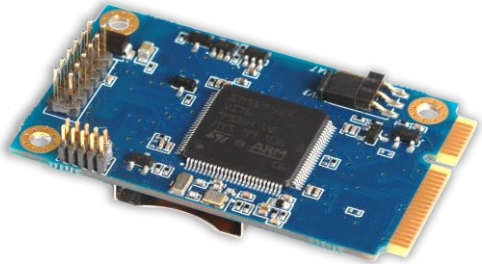
- Программный комплекс работает как служба ОС
- Поддержка резервирования (кластер ViPNet SIES Unit Router)
- Поддерживаемые архитектуры: x86-64
- Поддерживаемые ОС: Astra Linux, Альт СП

Соответствие требованиям

- Не является СКЗИ и не подлежит обязательной сертификации

ViPNet SIES 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

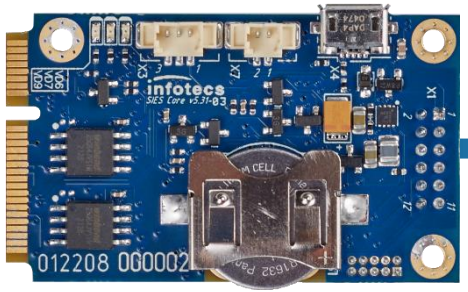
Функциональные особенности

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

Соответствие требованиям

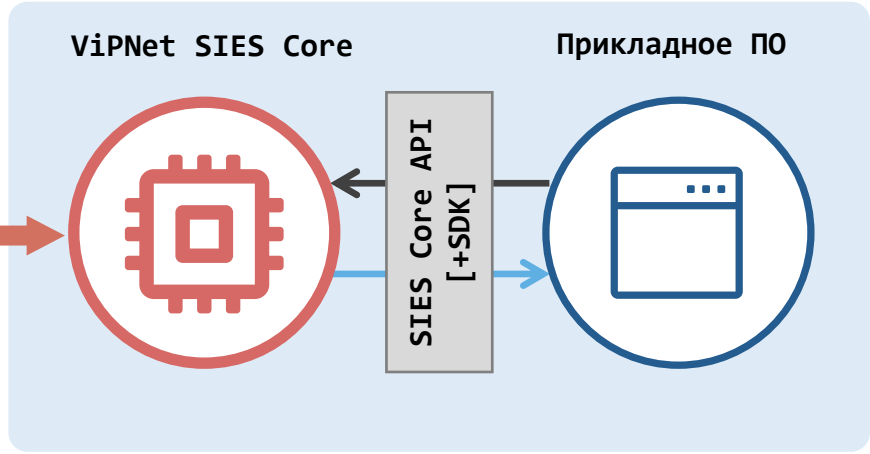
- СКЗИ класса КС3

Интеграция ViPNet SIES Core



ViPNet SIES Core

UART/USB/SPI/I2C

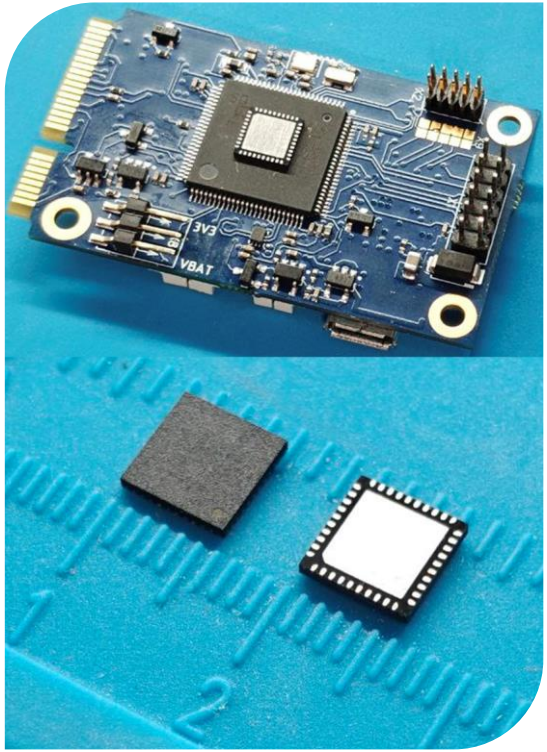


Защищаемое устройство
(ПЛК, УСПД, УСО, шлюз и т.п.)

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

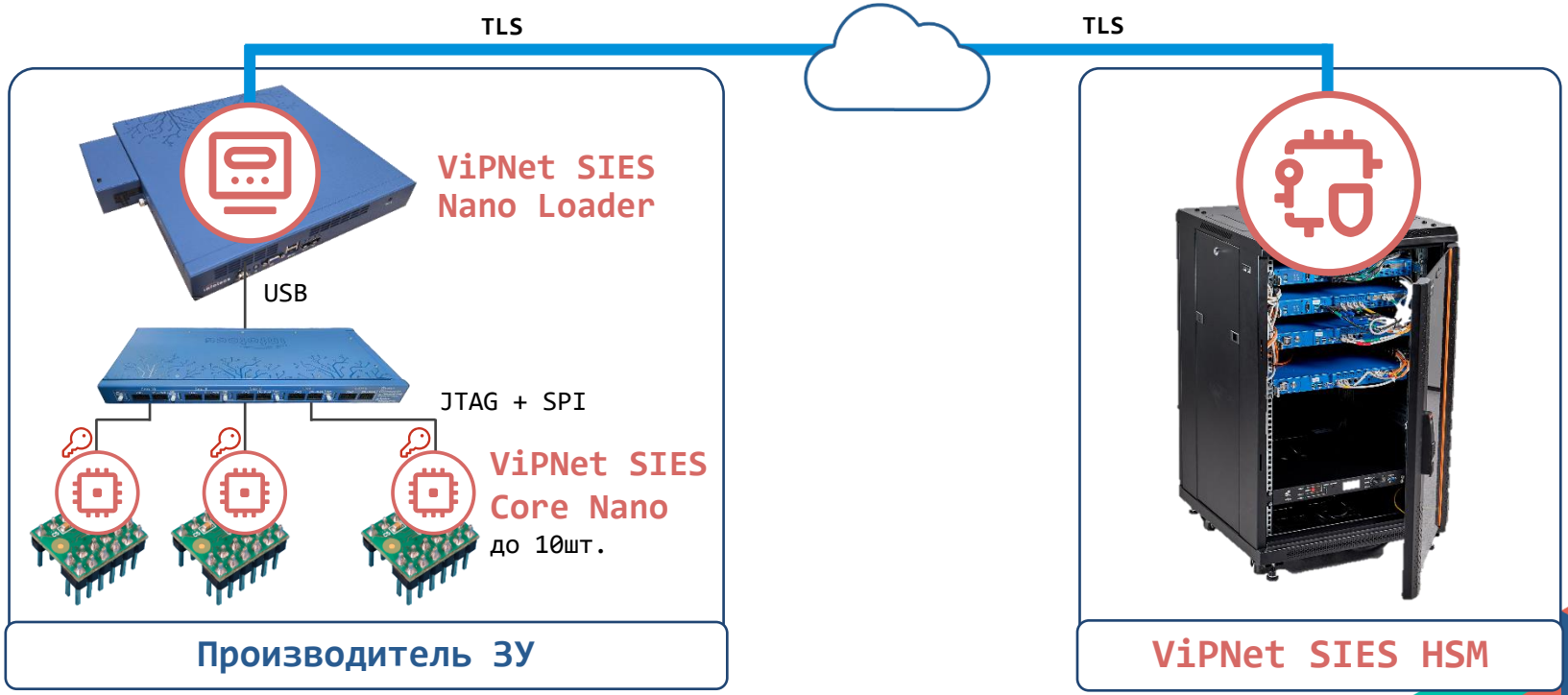
Функциональные особенности

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

Соответствие требованиям

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

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

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

Как упростить встраивание?

Расширения и инструменты для разработчиков

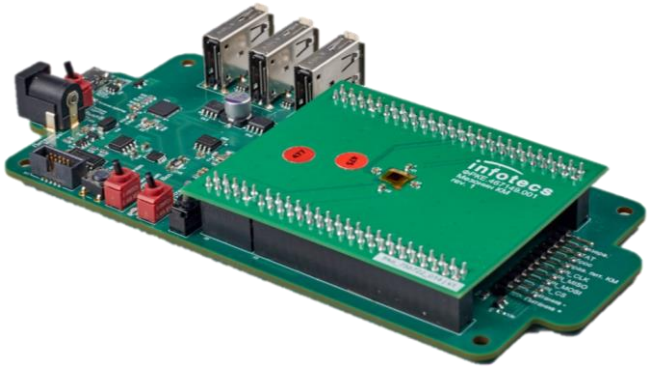
инфотекс

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



Предназначен 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

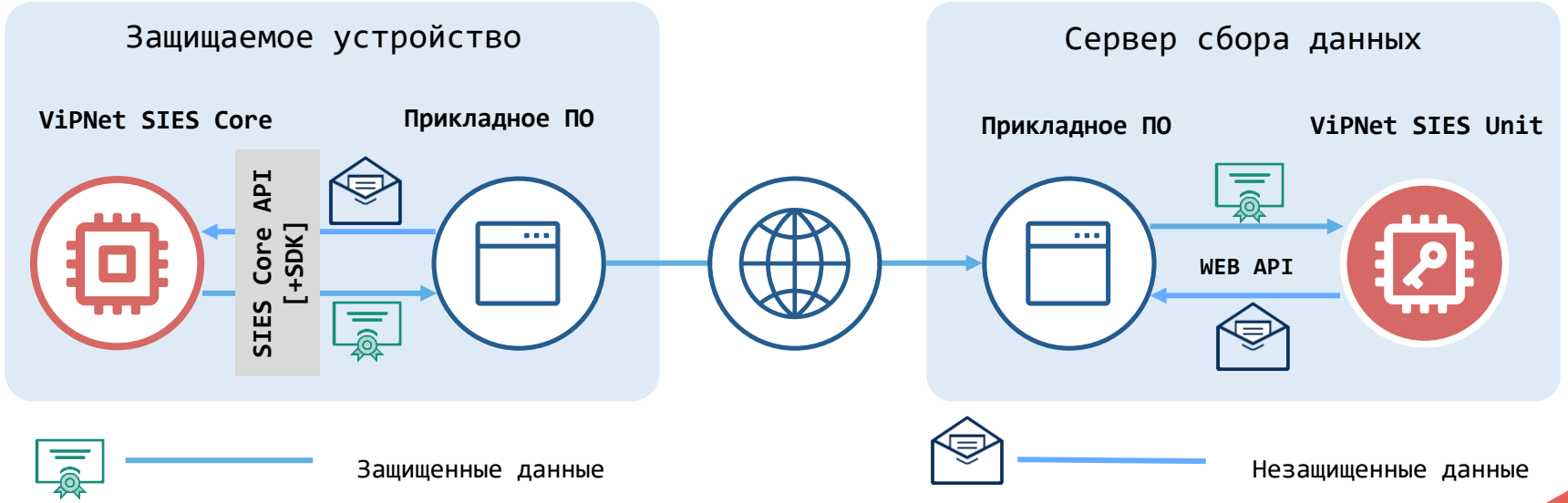
инфотекс

Криптографические сервисы для защищаемых устройств

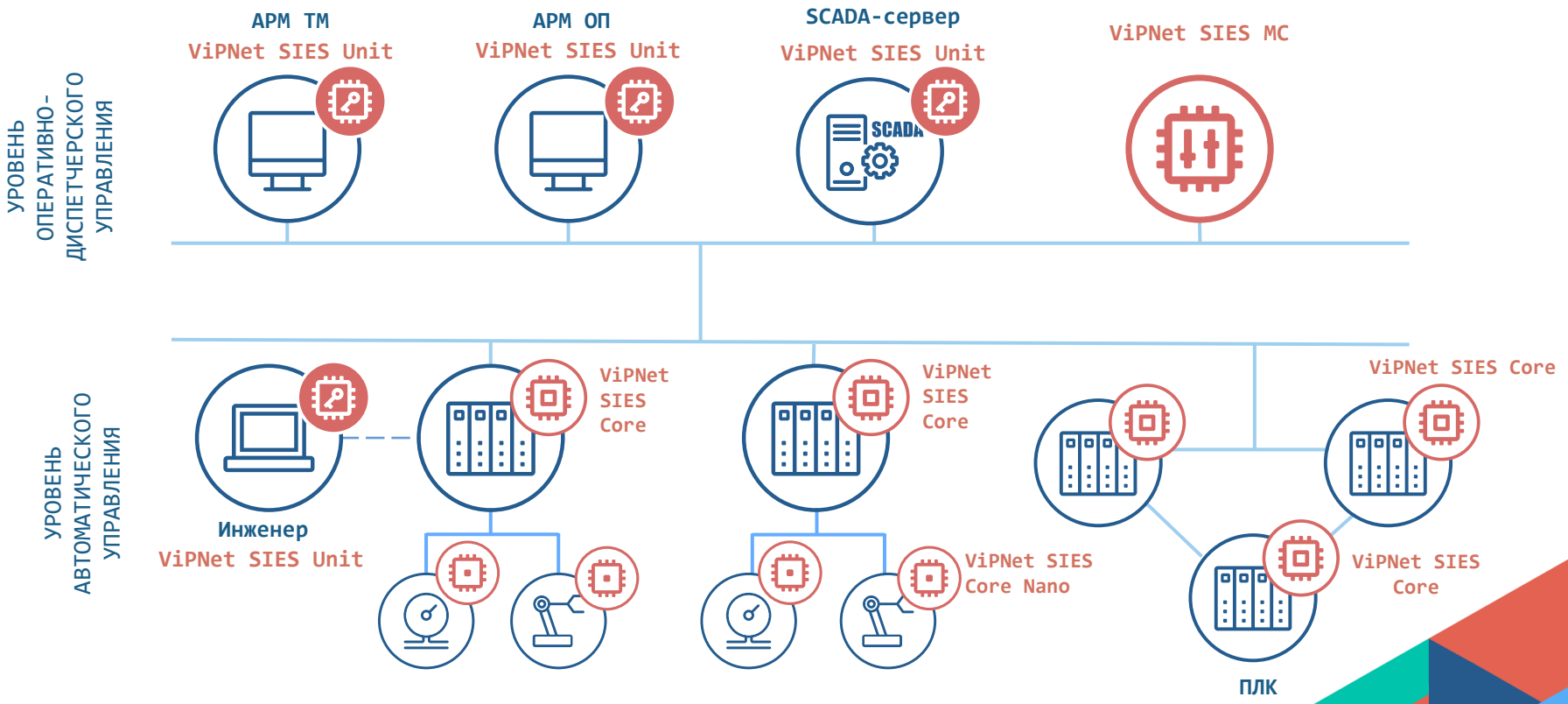
Компоненты решения ViPNet SIES позволяют реализовывать следующие сценарии обеспечения информационной безопасности защищаемых устройств:

- 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

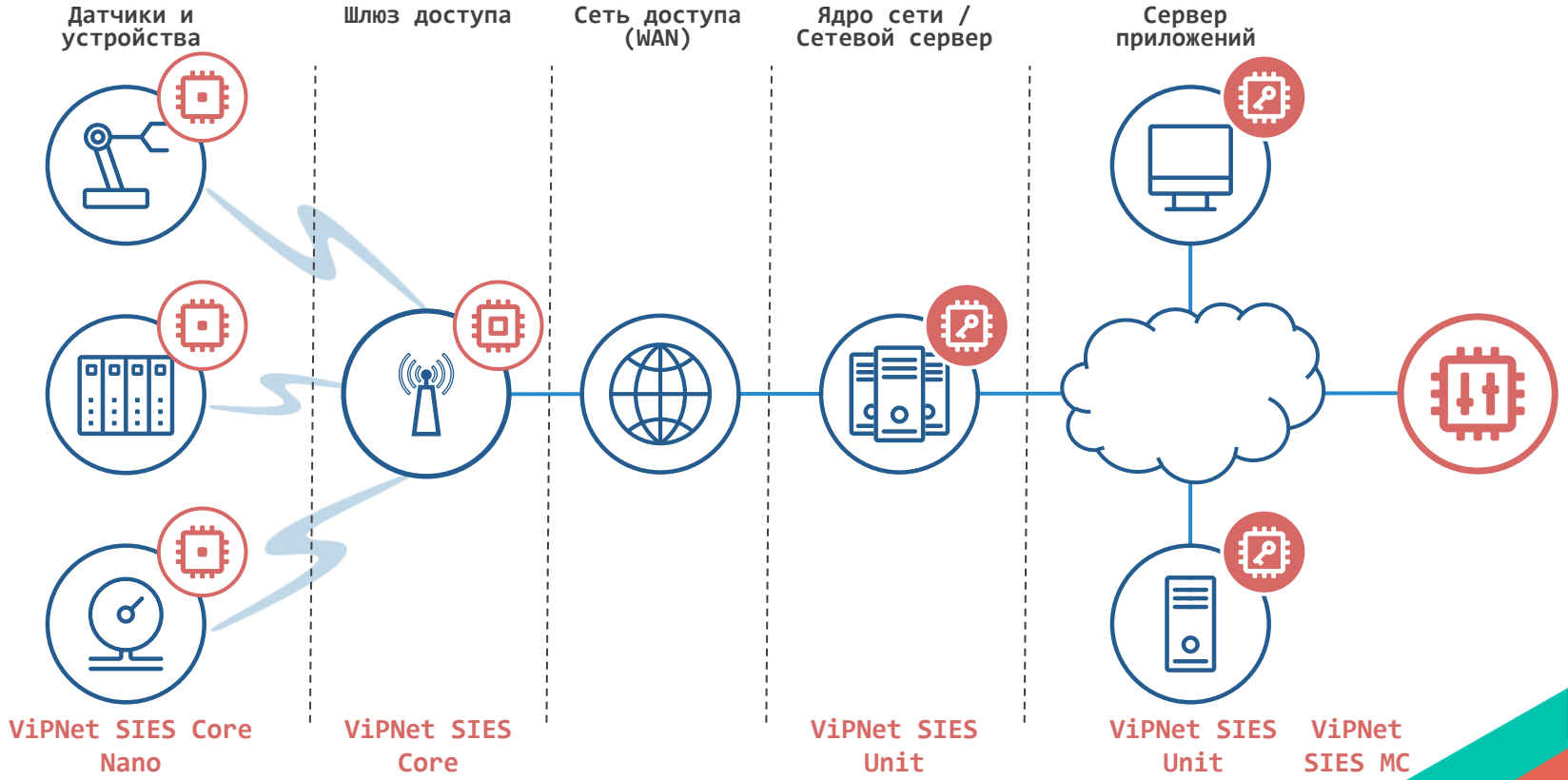
Защита коммуникаций с помощью ViPNet SIES



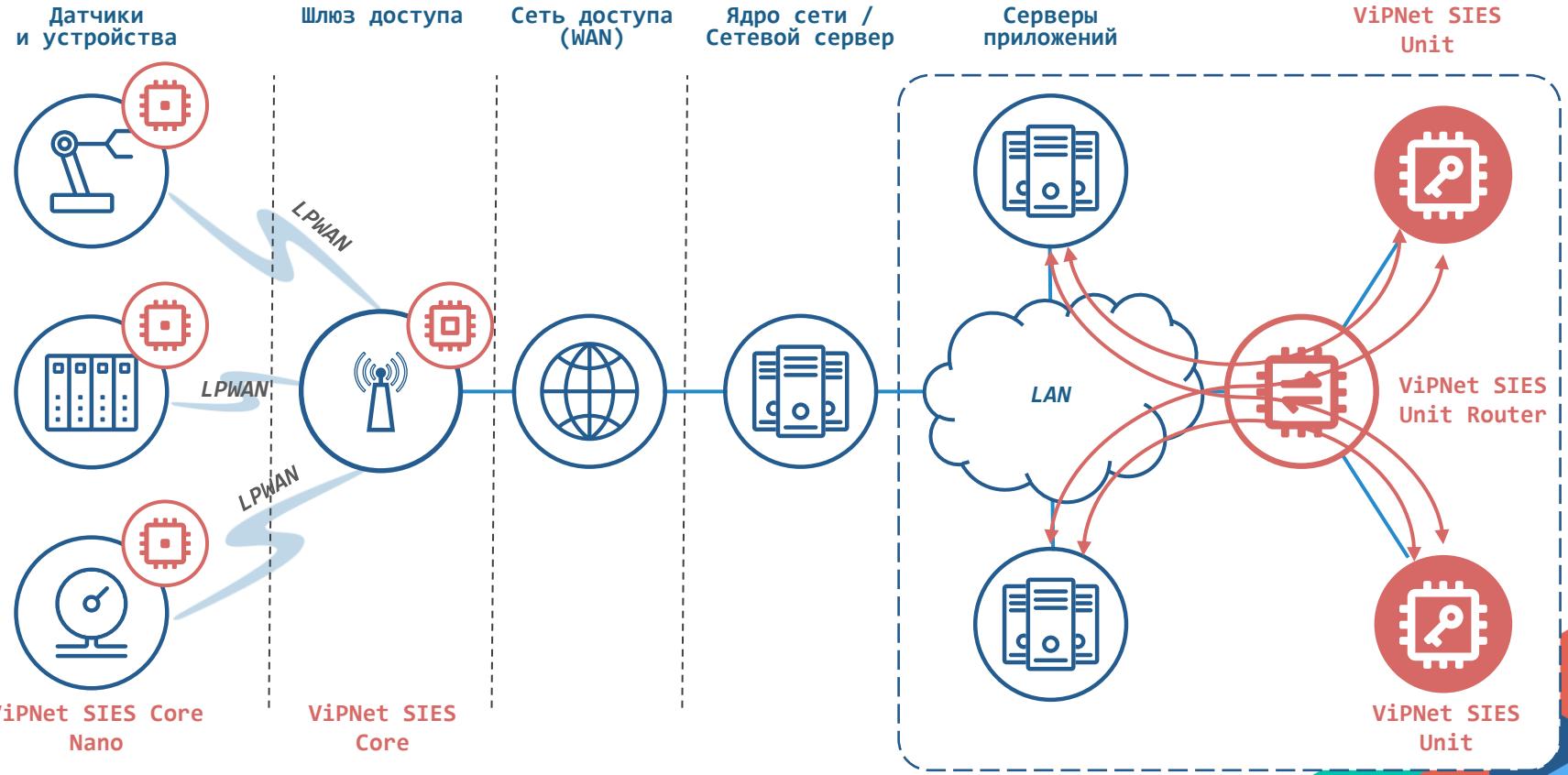
Защищенная АСУ ТП



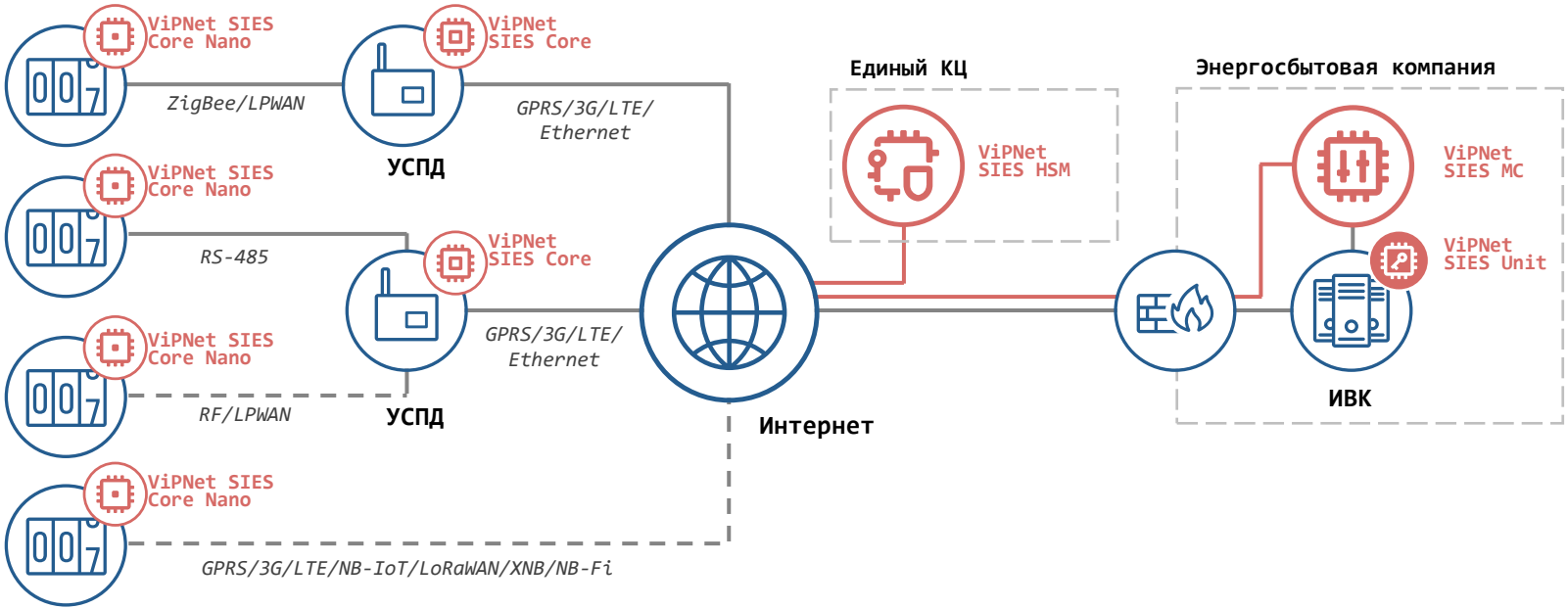
Защита данных в IIoT-системе



Масштабирование ViPNet SIES Unit



Защита данных в ИСУЭ



Приборы учета | Уровень ИВКЭ | Уровень ИВК

САНКТ ПЕТЕРБУРГ

инфотекс

ТЕХНОФЕСТ

Академия инфотекс · Учебный центр инфотекс · AMPIRE · TELEOFIS · КОМФОРТЕЛ оператор связи бизнес-класса · РУТОКЕН компания ИНФОТЕКС · TS Solution · AXOFT

Подписывайтесь на наши соцсети