

Криптография в каждый дом: ИСУЭ новое

Марина Сорокина

БОЛЬШОЙ
МОСКОВСКИЙ
ТЕХНО  **ФЕСТ**

Общие положения

Интеллектуальная система учета электрической энергии (мощности) – ИСУЭ



Постановление Правительства РФ
от 19 июня 2020 г. № 890
«О порядке предоставления
доступа к минимальному набору
функций интеллектуальных
систем учета электрической
энергии (мощности)»

Базовая модель угроз и нарушителя

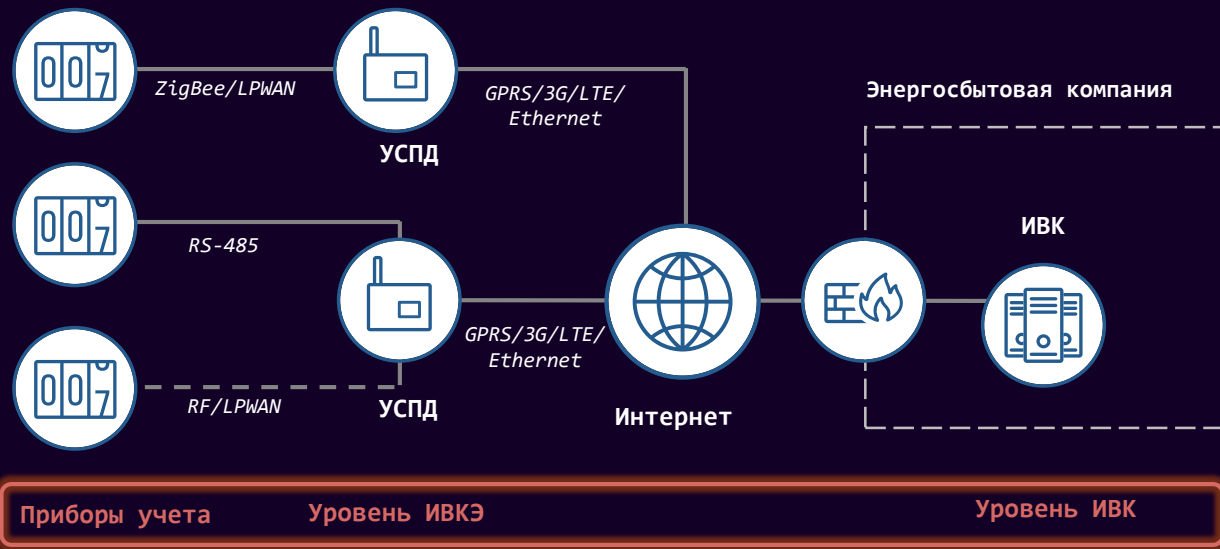
Базовая модель угроз
безопасности информации
интеллектуальной системы учета
электрической энергии (мощности)

<https://minenergo.gov.ru/upload/iblock/36f/Bazovaya-model-ugroz-s-izmeneniyami-ot-11.12.2024.pdf>

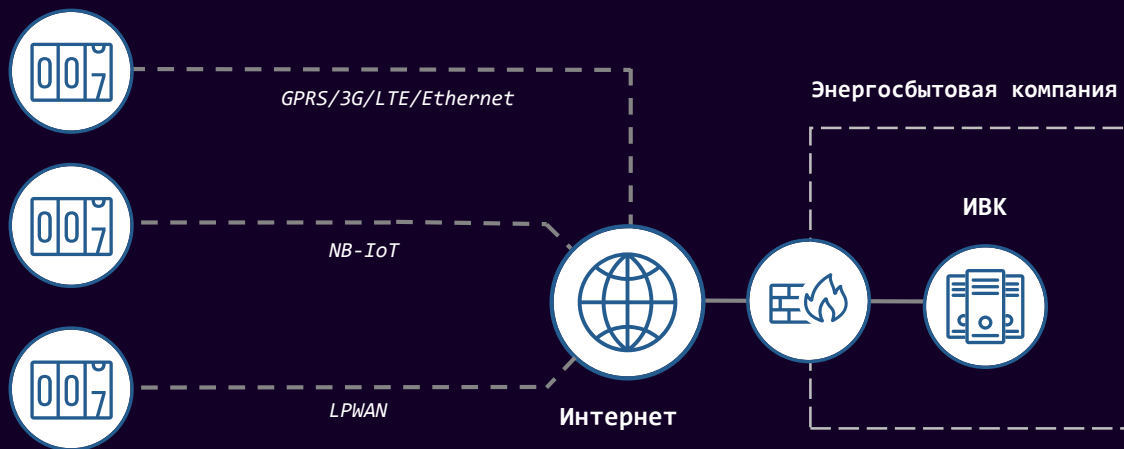


- Защита данных между ИВК-ИВКЭ обязательна
- Защита данных между ИВКЭ-ПУ и ИВК-ПУ – в зависимости от частной модели угроз безопасности информации
- В Базовую модель угроз и нарушителя добавлены типовые модели угроз. Типовая Модель угроз безопасности информации ИСУЭ Вариант 1 разработана ИнфоТеКС
- Типовая модель угроз безопасности ИнфоТеКС предполагает использование СКЗИ класса КСЗ; для сетевых компаний допустимо применение СКЗИ класса КС1

ИСУЭ с трехзвенной архитектурой:



ИСУЭ с двухзвенной архитектурой:



Приборы учета

Уровень ИВК

- Защита данных между ИВК - ПУ – в зависимости от частной модели угроз безопасности информации
- ИнфоТеКС разработана Типовая модель угроз безопасности информации для ИСУЭ с двухзвенной архитектурой, предоставляется по запросу
- Типовая модель угроз безопасности ИнфоТеКС предполагает использование СКЗИ класса КСЗ



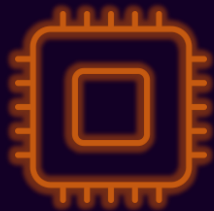
ИСУЭ как ОКТИ

ИСУЭ входит в перечень
типовых отраслевых
объектов ОКТИ,
функционирующих в сфере
энергетики
2023-08-08

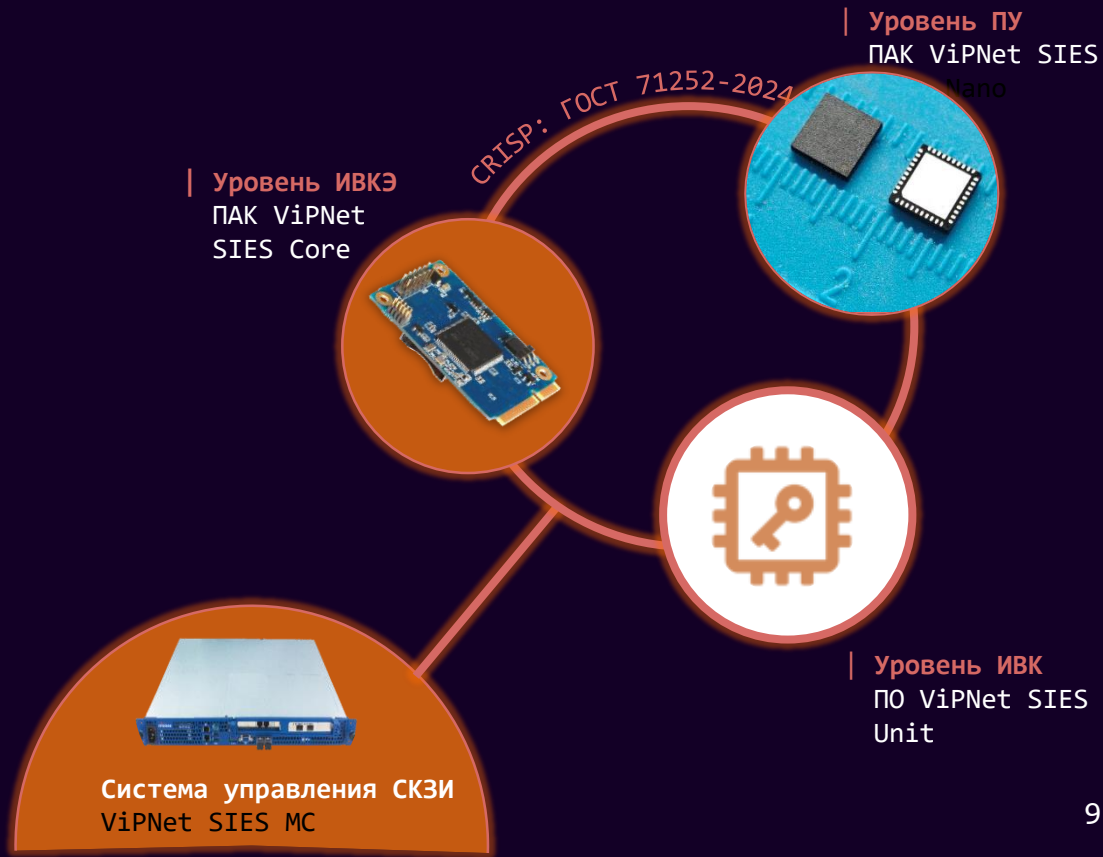
<https://minenergo.gov.ru/opensdata/7715847529-perechen-obektov-kii-2023>

Решение ViPNet SIES для ИСУЭ

Решение ViPNet SIES для ИСУЭ



Встраиваемые СКЗИ
ViPNet SIES



Возможные сценарии обеспечения ИБ для УСПД/шлюза/базовой станции и ПУ

Защита коммуникаций ИСУЭ (точка-точка и резервированные связи):

- Обеспечение целостности по протоколу CRISP* (ГОСТ 71525-2024)
- Шифрование по протоколу CRISP* (ГОСТ 71525-2024)
- Шифрование (в формате CMS)**
- Электронная подпись для команд и данных (в формате CMS)**

Защита устройства уровня ИВКЭ и ПУ:

- Доверенное удаленное и локальное обновление ПО*
- Доверенное конфигурирование* (в том числе через конфигуратор)
- Авторизация пользователя**
- Доверенная загрузка
- Черный ящик для хранения журнала устройства

* Сценарии, рекомендованные к реализации ИнфоТеКС

** Только для устройств с СКЗИ ViPNet SIES Core

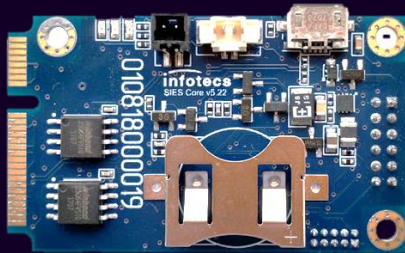


для ИНТЕГРАЦИИ в УСПД / шлюз

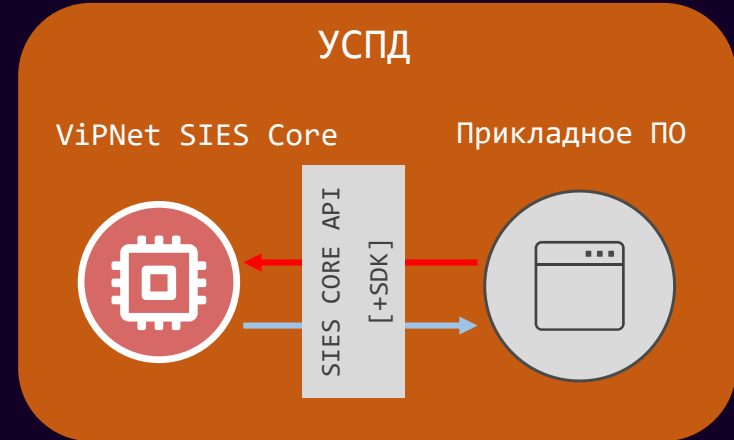
- Форм-фактор – плата PCI Express® Full-Mini Card (51 x 30 x 11,2 мм)
- Интеграция на аппаратном уровне – USB, UART, SPI
- Интеграция на программном уровне – SIES Core API
- Рабочий диапазон температур – -40...+70 °C
- Возможность использования вне контролируемой зоны при подключении тампер контактов
- Наличие SDK под Linux (ARM, x86), Windows, RTOS
- Сертификат СКЗИ класса КСЗ по требованиям ФСБ России

ПАК ViPNet SIES Core

Интеграция ViPNet SIES Core в УСПД/коммуникационный шлюз/ базовую станцию



UART / USB / SPI



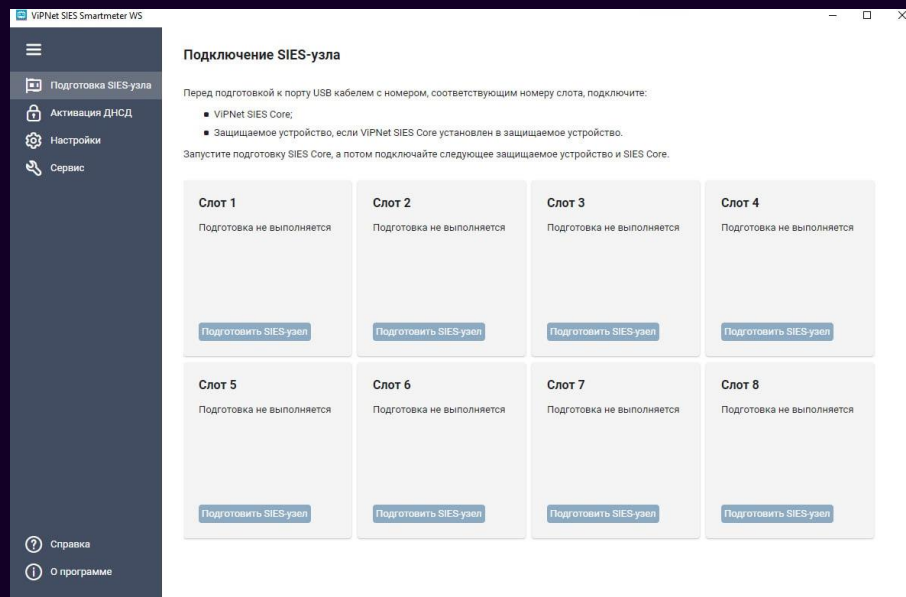
СКЗИ встраиваются в устройства ИВКЭ на этапе разработки устройства
Установка и/или монтаж СКЗИ осуществляется при производстве
устройств ИВКЭ
Инициализация происходит при вводе в эксплуатацию

— Защищенные данные
— Незащищенные данные

Массовый ввод в эксплуатацию УСПД с ViPNet SIES Core

ViPNet SIES Smartmeter WS – АРМ для автоматического поточного ввода в эксплуатацию УСПД с SIES Core:

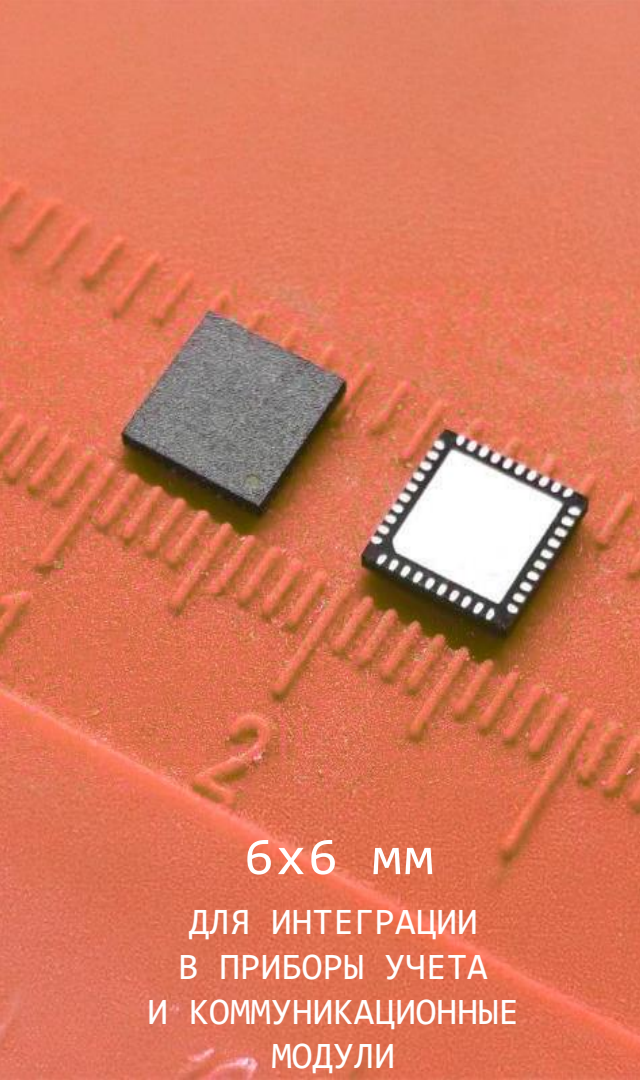
- Массовая инициализация ViPNet SIES Core (до 8 шт одновременно)
- Автоматизация ввода в эксплуатацию (привязка с защищаемому устройству, создание связей по типу звезда или звезда с резервированием, загрузка ключей, активация ДНСД)
- Гибкая конфигурация настроек и сохранение настроек в файле конфигурации
- Возможность ввода информации сканером штрихкодов
- Возможность интеграции со сторонней системой для ввода данных по УСПД
- Возможность загрузки данных об УСПД из файла



Массовый ввод в эксплуатацию УСПД с ViPNet SIES Core



ПАК ViPNet SIES Core Nano



6x6 мм

для ИНТЕГРАЦИИ
в ПРИБОРЫ УЧЕТА
и КОММУНИКАЦИОННЫЕ
МОДУЛИ

Встраивание:

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

Криптографический протокол CRISP:

- Зашифрование/расшифрование
- Создание имитовставки/ проверка имитовставки

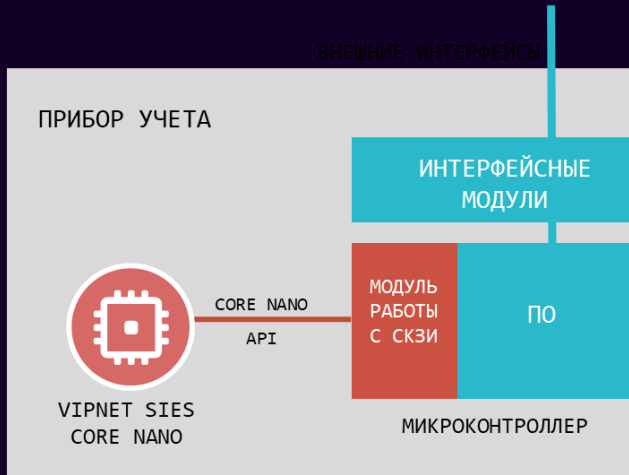
Функциональные особенности:

- Хранение ключевой информации 16 лет без смены
- Рабочий диапазон температур -40...+85 °C
- Форм-фактор – микросхема в корпусе QFN40

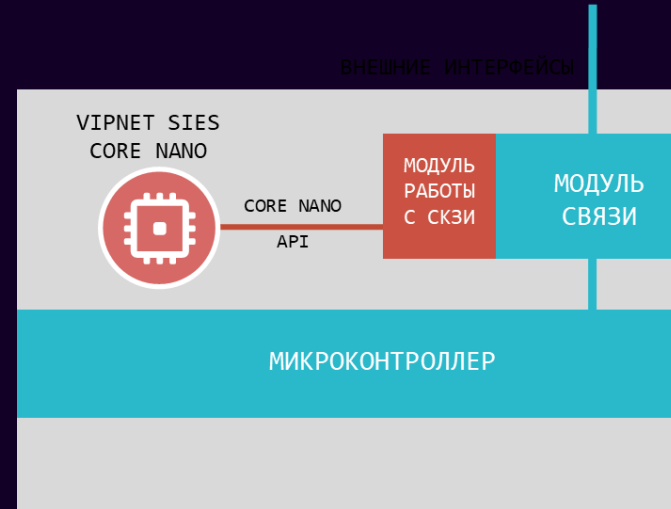
Сертификация:

- СКЗИ-НР и СКЗИ класса КСЗ

Встраивание VIPNet SIES Core Nano в прибор учета



ВСТРАИВАНИЕ В ПРИБОР УЧЕТА



ВСТРАИВАНИЕ В МОДУЛЬ СВЯЗИ

СКЗИ встраиваются в ПУ на этапе разработки устройства, монтаж СКЗИ на плату осуществляется при производстве ПУ. Ключевая информация в СКЗИ заливается на заводе при производстве ПУ. При вводе в эксплуатацию не требуется проведения никаких действий с СКЗИ

ПАК ViPNet SIES Nano Loader



АП ViPNet SIES Nano Loader



МОДУЛЬ SIES Nano Adapter



МОДУЛЬ SIES Nano Array Adapter

АРМ ввода ключей ПАК ViPNet SIES Core Nano

Состоит из:

- ViPNet SIES Nano Loader
- модуля SIES Nano Adapter (единичное обслуживание) или SIES Nano Array Adapter (массовый режим)

Позволяет:

- Подключиться к технологической оснастке для прошивки SIES Core Nano и загрузки в него ключей
- Запросить ключи SIES Core Nano в SIES HSM и экспортировать их в защищенном виде
- Загрузить ключи в SIES Core Nano
- Загрузить отчет о загрузке ключей и информацию о серийном номере SIES Core Nano и серийном номере защищаемого устройства

СКЗИ класса КСЗ+

Производство ПУ (инициализация ПАК ViPNet SIES Core Nano)



ViPNet SIES HSM

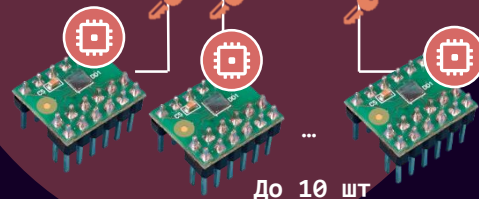
TLS



Завод

ViPNet SIES
Nano Loader

ViPNet SIES
Nano Array



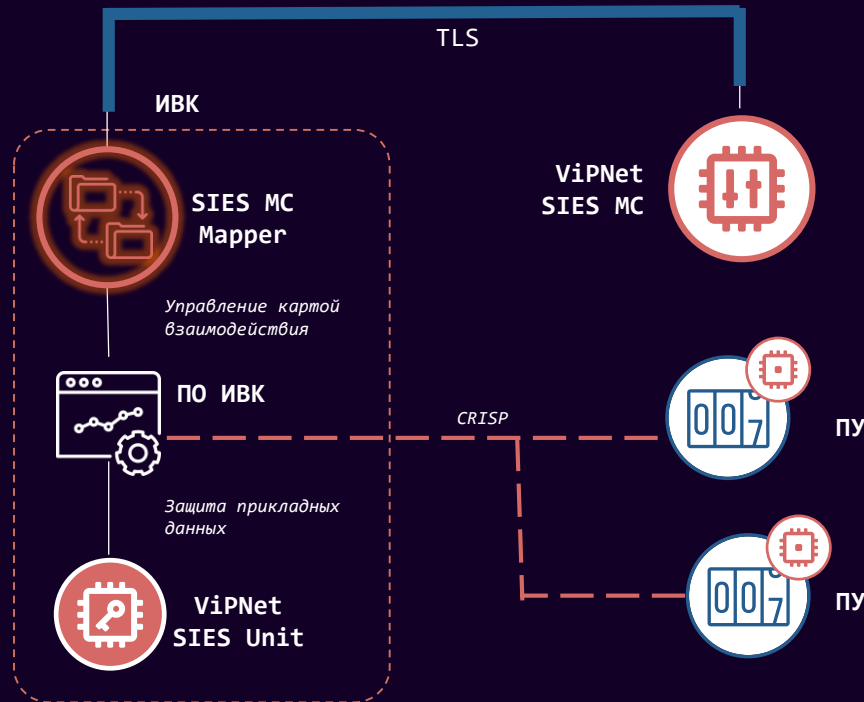
ViPNet SIES
Core Nano в
составе ПУ

- Генерация и загрузка ключей в крипточип
- Ведение базы соответствия серийного номера ПУ, крипчипа и загруженных ключей

Интеграция SIES MC с ИВК: автоматизация ввода в эксплуатацию ЗУ

VipNet SIES MC Mapper – утилита для интеграции VipNet SIES MC с ИВК для автоматической регистрации ПУ и УСПД и построения карты взаимодействия между устройствами в системе:

- Регистрация защищаемых устройств в VipNet SIES MC (ПУ и УСПД) по информации из ИВК
- Внесение изменений в атрибуты защищаемых устройств (ПУ и УСПД) по информации из ИВК
- Автоматическое добавление VipNet SIES Core Nano в VipNet SIES MC при добавлении нового защищаемого устройства, если то содержит внутри себя крипточип; ассоциация его с защищаемым устройством
- Построение взаимодействия (связей) в VipNet SIES MC между ПУ, УСПД, ИВК по информации из ИВК



ПО ViPNet SIES Unit

ИВК И АРМ КОНФИГУРАТОР

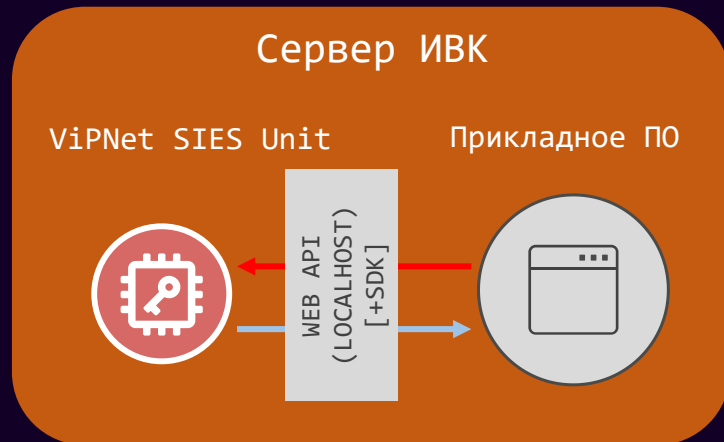
ДЛЯ ИНТЕГРАЦИИ В ИВК
И АРМ КОНФИГУРАТОР



- Интеграция по RESTAPI (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 и АЛТ 8 СП
- Поддержка архитектуры процессора 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, 100 000, 1 М связей
- Сертификат СКЗИ класса КС1 и КС3 по требованиям ФСБ России

Интеграция ViPNet SIES Unit

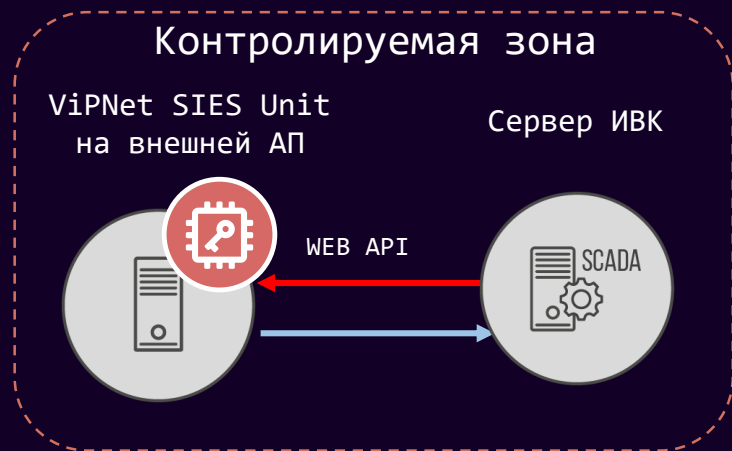
ВАРИАНТ 1



— Защищенные данные

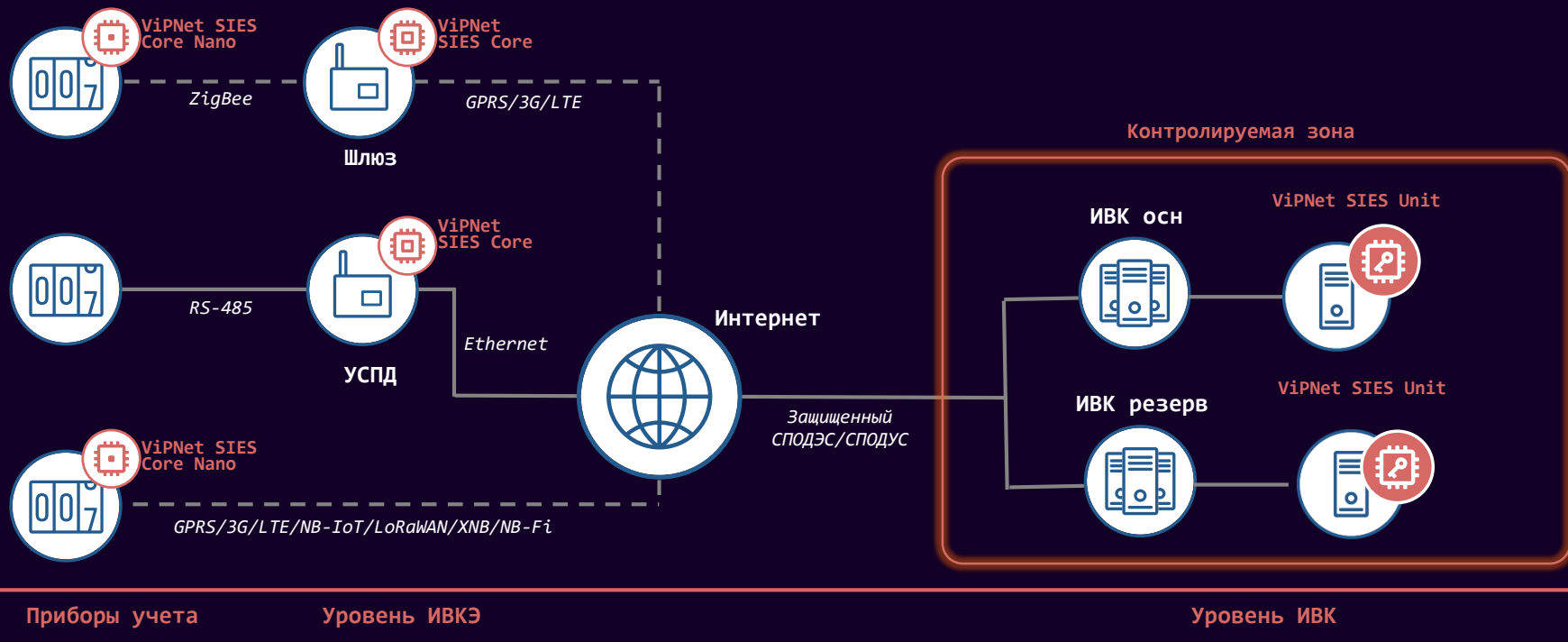
← — Незащищенные данные

ВАРИАНТ 2



СКЗИ устанавливаются в инфраструктуру на этапе ввода в эксплуатацию

Резервирование ViPNet SIES Unit





ВАРИАНТ ПОСТАВКИ ViPNet SIES Unit

на 500 связей

на 2К связей

на 10К связей

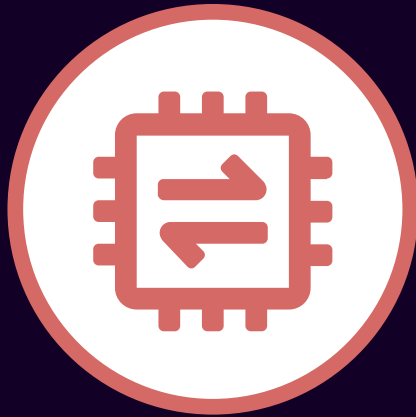
На 100К связей

На 1М связей

Высоконагруженный ИВК

- Использовать ViPNet SIES Unit на отдельном сервере
- Выбирать сервер под ViPNet SIES Unit исходя из рекомендаций по нагрузке
- Использовать gRPC в качестве интерфейса взаимодействия с ViPNet SIES Unit
- Выбрать высокопроизводительный вариант поставки ViPNet SIES Unit – 10К–1М связей
- Настроить ViPNet SIES Unit на работу в режиме с буферизацией
- Использовать ViPNet SIES Unit Router для «разбивки ViPNet SIES Unit на два сервера»

VIPNet SIES Unit Router: масштабирование SIES Unit



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

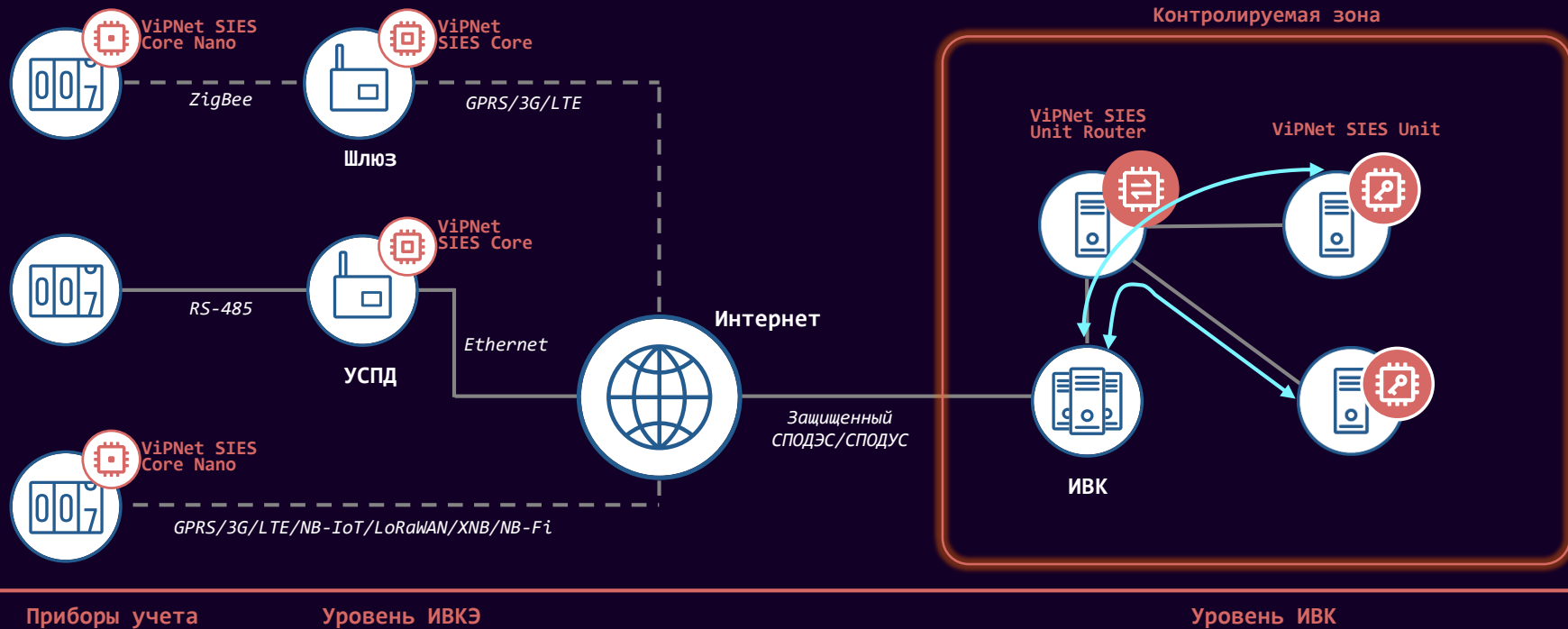
Функциональные особенности:

- 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 сертификации

Масштабирование ViPNet SIES Unit



VipNet SIES AMI Proxy: криптосервер СПОДЭС/СПОДУС

Функции:

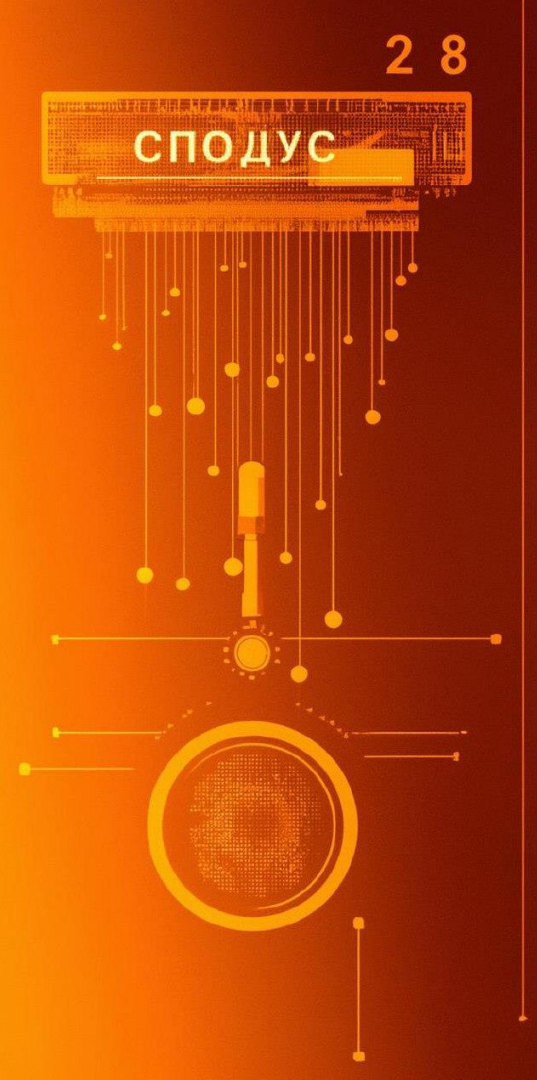
- Криптографическая защита данных для протоколов СПОДЭС/СПОДУС посредством VipNet SIES Unit
- Организация единой точки подключения к ИВК ИСУЭ по протоколам СПОДЭС/СПОДУС
- Обеспечение совместимости продуктов VipNet SIES с ИВК различных производителей, поддерживающих СПОДЭС/СПОДУС

Функциональные особенности:

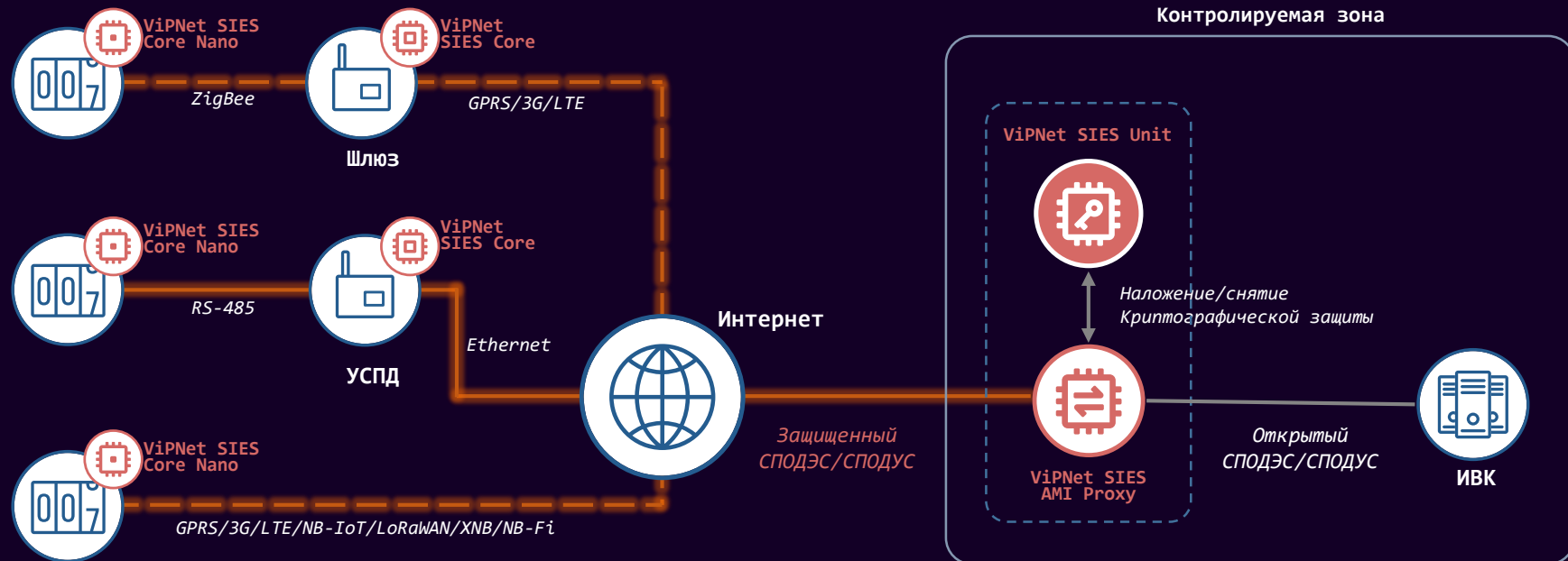
- Программный комплекс работает как служба ОС
- Стоит в разрыв связи перед ИВК ИСУЭ, перехватывая данные
- Прозрачный режим при взаимодействии ИВК с ИВКЭ и ПУ
- Поддерживаемые архитектуры: x86-64
- Поддерживаемые ОС: Astra Linux, Альт СП, Debian

Соответствие требованиям:

- Не является СКЗИ и не подлежит сертификации



Защита протоколов СПОДЭС/СПОДУС



Приборы учета

Уровень ИВКЭ

Уровень ИВК

На практике

Криптография в каждый дом: на практике



Шлюз коммуникационный CG-ZB-02C
с ViPNet SIES Core
Завод Нартис
ОВ: март 2023 г.
Выпущено: ~ 35тыс.
Установлено: ~ 30 тыс.
Планы: ~20 тыс. в 2025 г.

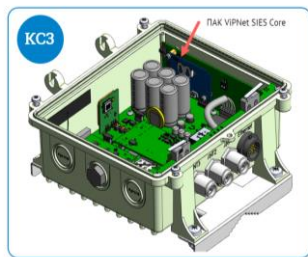


СИГМА.ИБК и СУП СПД ПИОНЕР
с ViPNet SIES Unit
ООО «Сигма»
ОВ: декабрь 2023 г.
Установлено: в 13 ЭСК
ПАО «ИнтерРАО»

Криптография в каждый дом на практике



lar.tech



Базовые станции LoRaWAN с
КСЗИ (ViPNet SIES Core)



УСПД МИРТ-881 с
КСЗИ ViPNet SIES
Core



Модем-коммуникатор МИР
МК-01.A с ViPNet SIES
Core Nano



УСПД АТБ-Нексус с
КСЗИ ViPNet SIES
Core

Криптография в каждый дом

СКЗИ для ИСУЭ – это не только конечное СКЗИ для ПУ и УСПД, но и удобство производства и массового ввода в эксплуатацию тысяч и миллионов устройств.

Это инфраструктура, рассчитанная на надежную работу с этого объема оборудования!

ДА БУДЕТ СВЕТ!

ТЕХНОinfotecs Фест

Марина Сорокина
Marina.Sorokina@infotecs.ru



NBJ НАЦИОНАЛЬНЫЙ
БАНКОВСКИЙ ЖУРНАЛ

GLOBAL
DIGITAL
SPACE



РУТОКЕН
КОМПАНИЯ ПРАКТИВ



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

АВАНГАРД

ARinteg

АТБ
ЭЛЕКТРОНИКА

infotecs
{/cademy}

m≈rlion

УЧЕБНЫЙ
ЦЕНТР
ИНФОТЕКС

Подписывайтесь
на наши соцсети,
там много интересного

