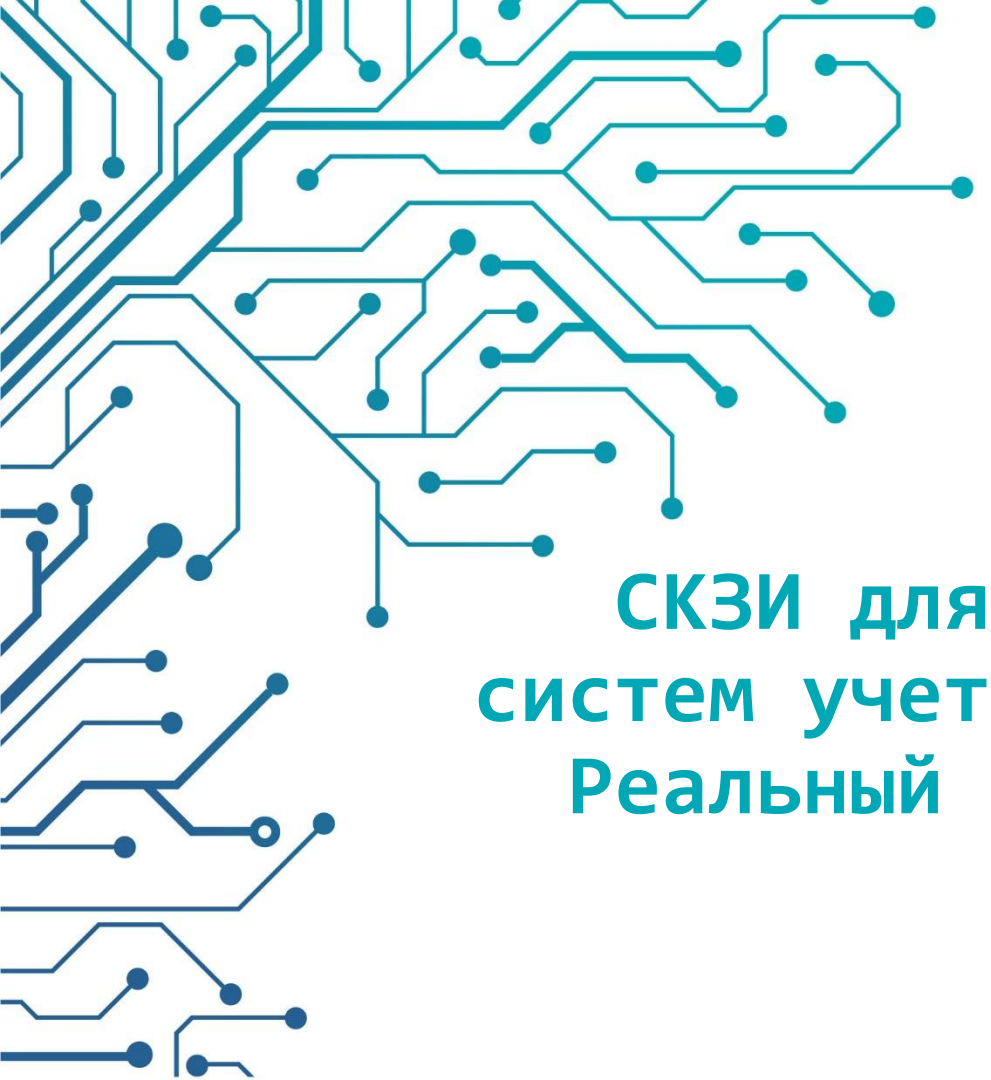


СКЗИ для Интеллектуальных систем учета электроэнергии. Реальный практический опыт ИнфоТеКС

Марина Сорокина
Руководитель направления

ОБЩИЕ ПОЛОЖЕНИЯ

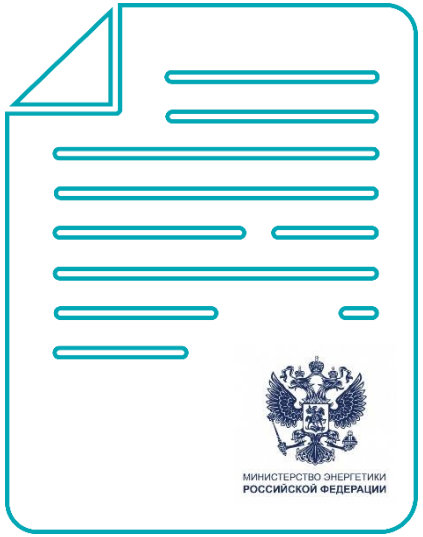
Интеллектуальная система учета электрической энергии (мощности) – ИСУЭ

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

ИСУЭ и ФЗ №187-ФЗ

- ИСУЭ – есть КИИ
- Категория значимости объекта КИИ определяется субъектом КИИ при категорировании определятся
- Требуется создание подсистемы безопасности
- В большинстве случаев подсистема безопасности ИСУЭ должна учитывать требования по подключению объектов к сетям связи общего пользования

Базовая модель угроз и нарушителя



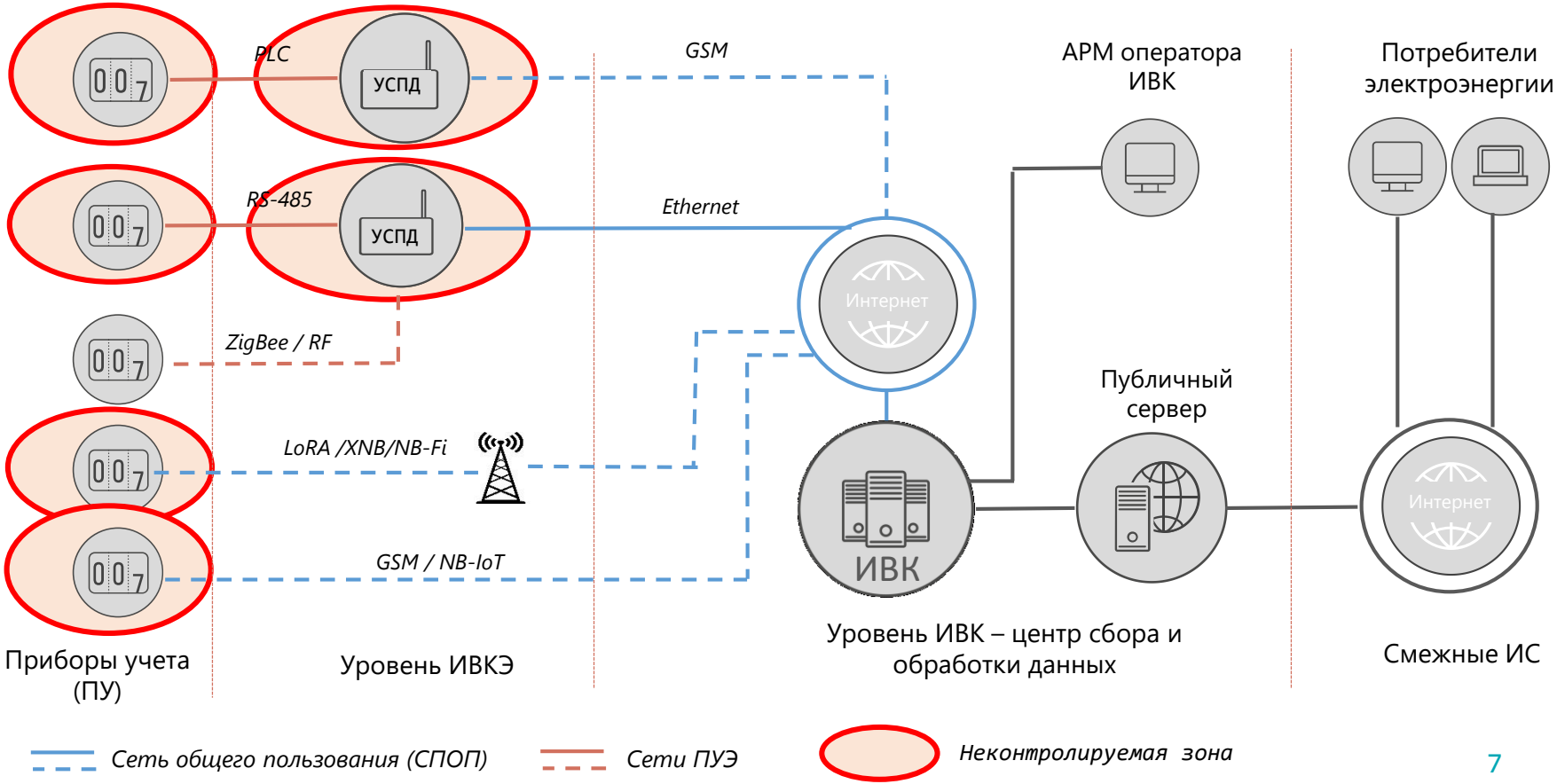
Базовая модель угроз безопасности информации интеллектуальной системы учета электрической энергии (мощности)

https://docs.cntd.ru/document/607167779

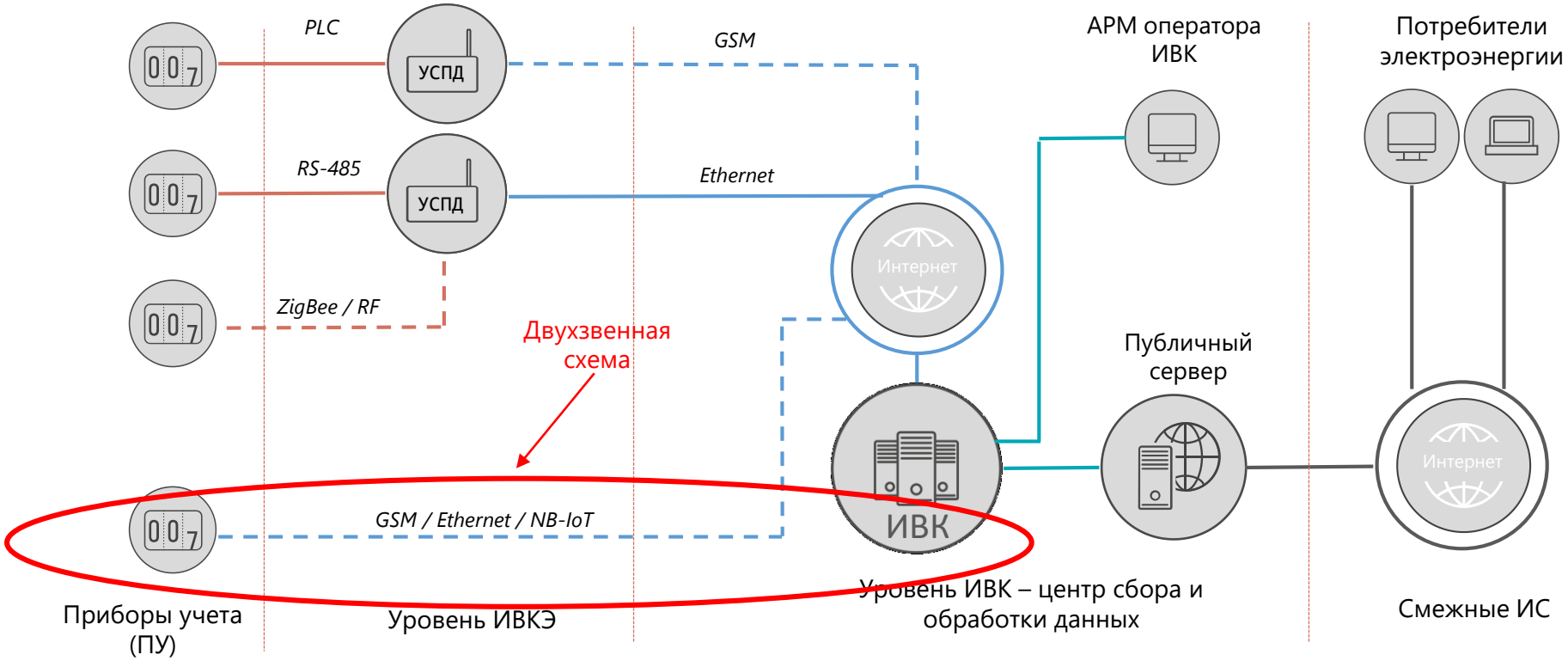
Базовая модель угроз и нарушителя

- Требуется **частная модель угроз**
- Требуется защиты информации с помощью **СКЗИ от уровня ИВК до ИВКЭ**
- **До 01.01.2024 Базовая модель угроз** должна быть **пересмотрена** с целью обеспечения защиты информации **на всех уровнях ИСУЭ (включая ПУ)**

Архитектура ИСУЭ

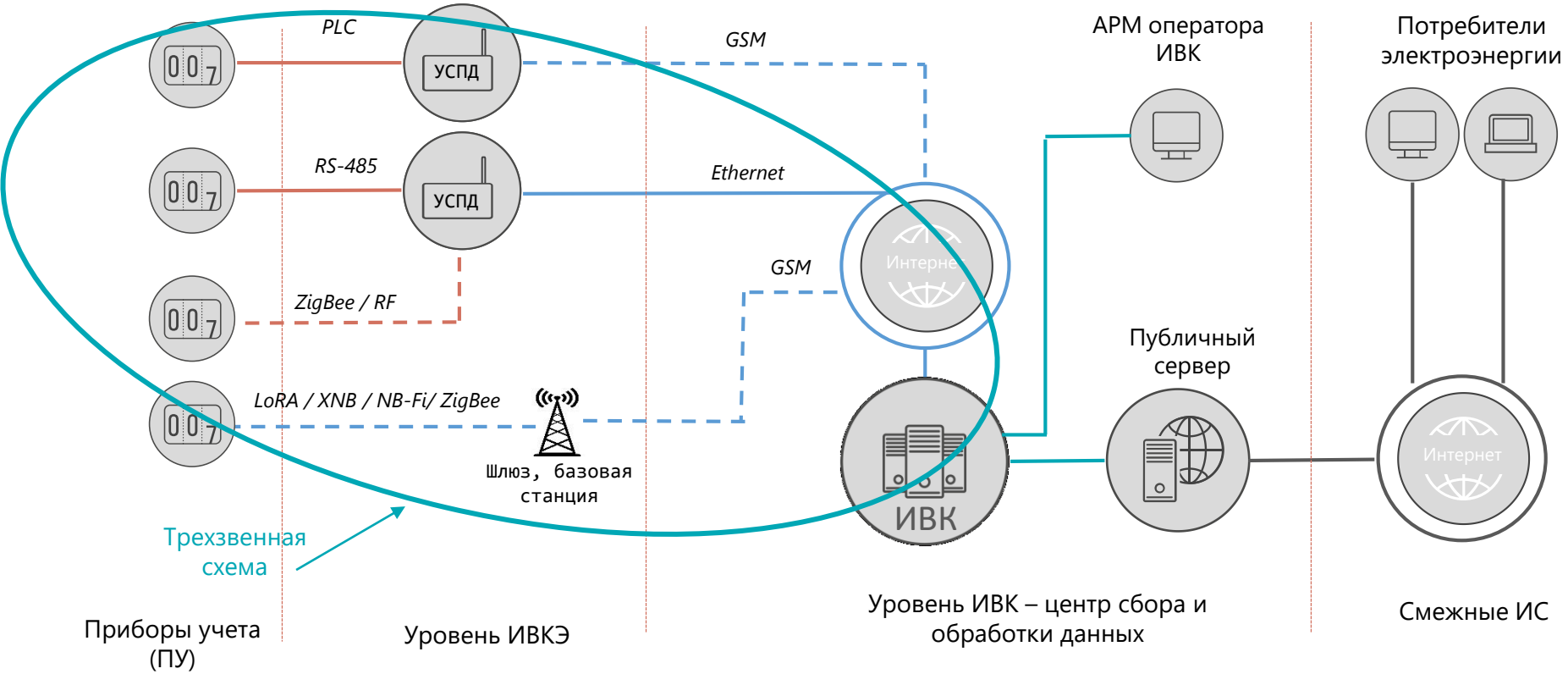


Архитектура ИСУЭ

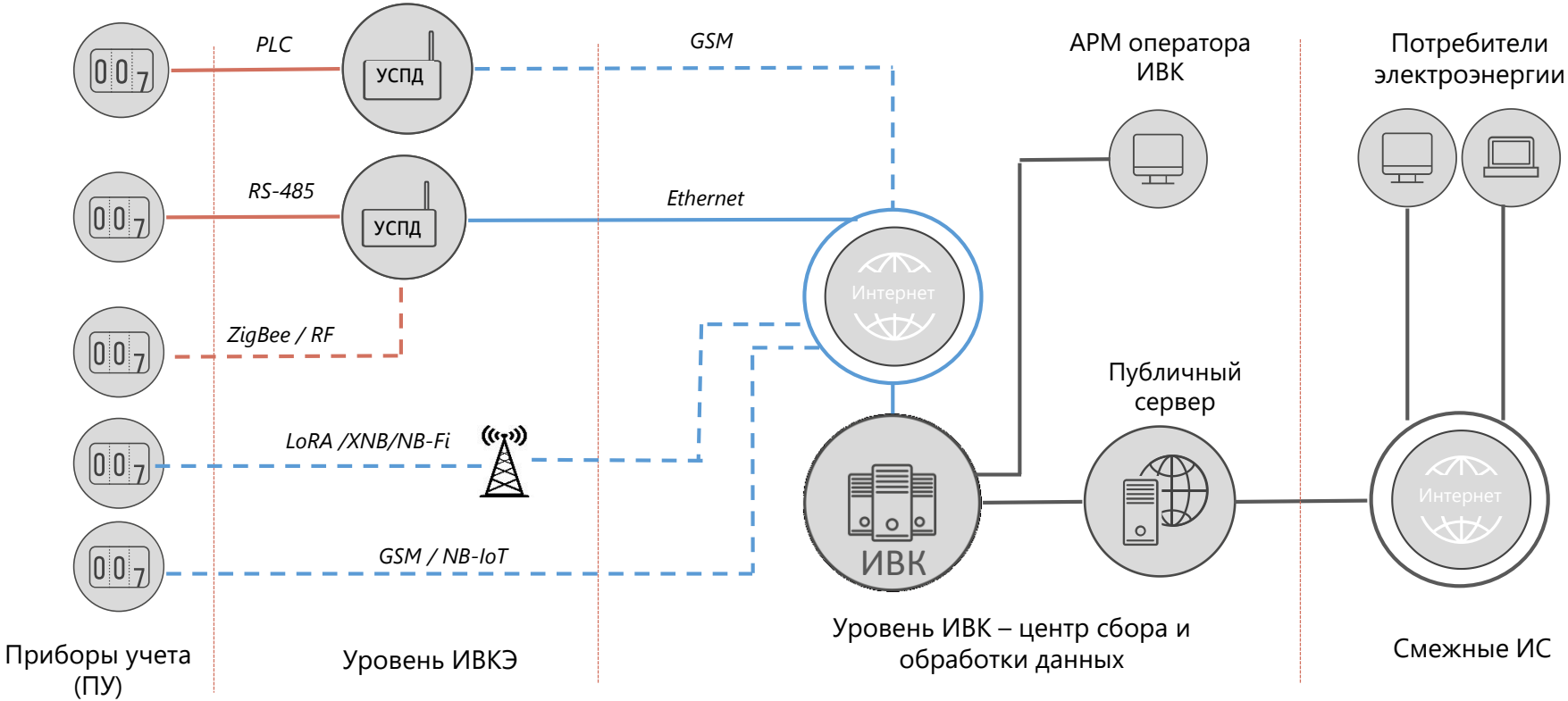


Корпоративная сеть (КСПД) *Сеть общего пользования (СПОП)* *Сети ПУЭ*

Архитектура ИСУЭ



Архитектура ИСУЭ



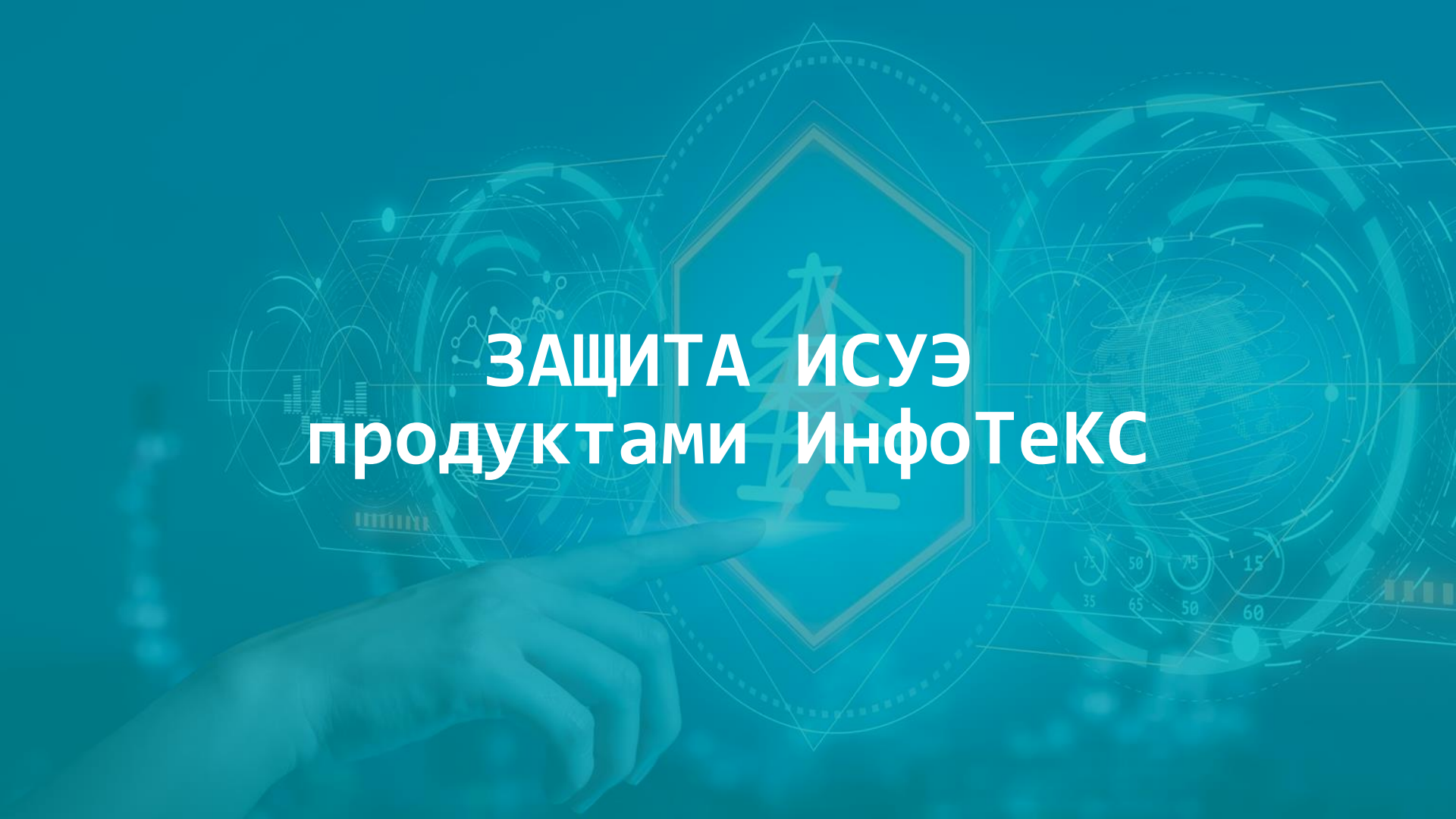
Сеть общего пользования (СПОП) *Сети ПУЭ*

Сложности обеспечения ИБ ИСУЭ

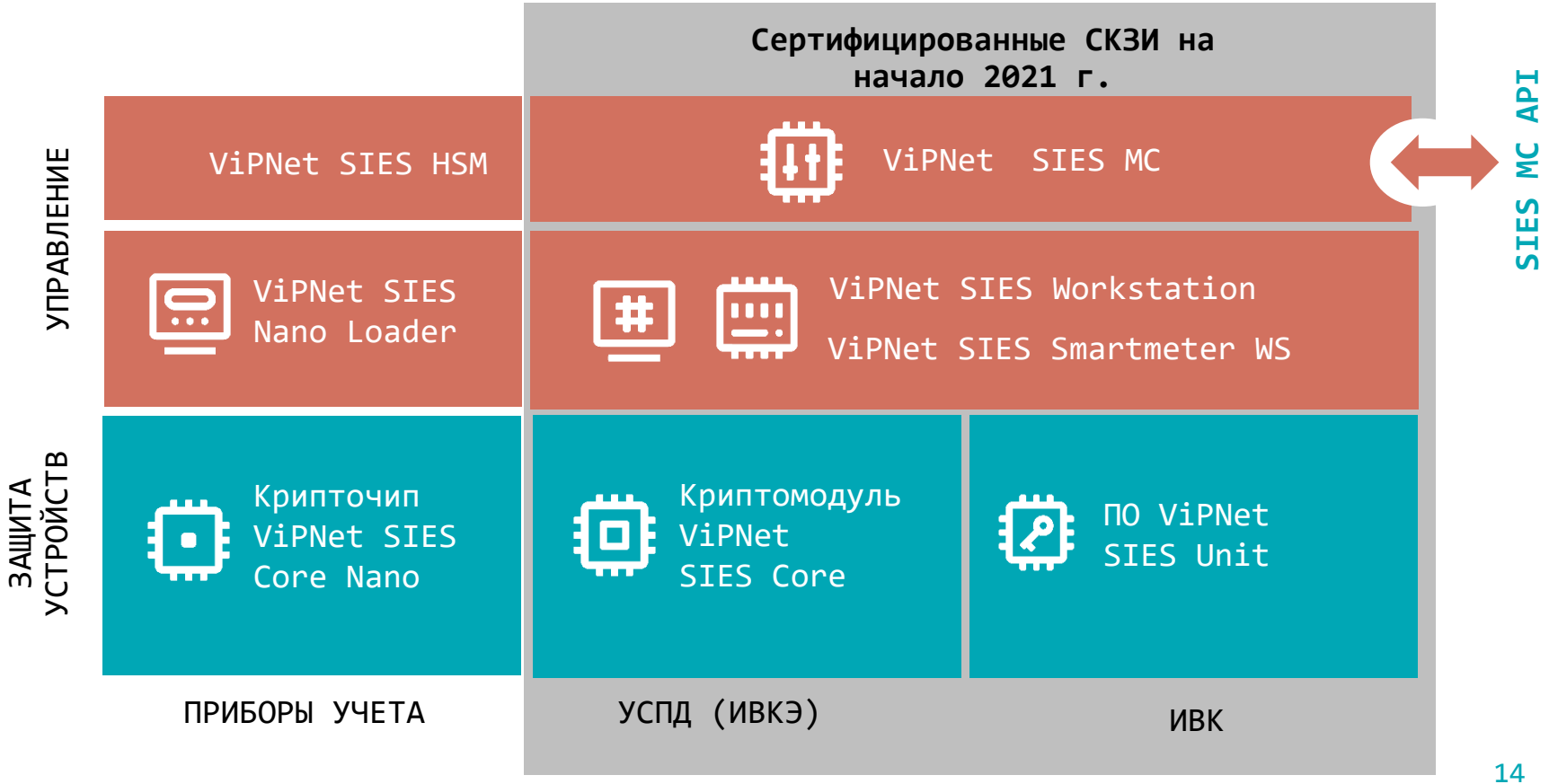
- Большая распределенная система
- Элементы ИСУЭ, за исключение ИВК, расположены вне контролируемой зоне
- ИСУЭ по своей архитектуре является IIoT-системой и защищать ИСУЭ, нужно как IIoT
- СЗИ и СКЗИ должны быть встроенными в компоненты ИСУЭ
- Большое количество протоколов и интерфейсов
- Большое количество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


ЗАЩИТА ИСУЭ
продуктами ИнфоТеКС

Состав решения ViPNet SIES



Решение ViPNet SIES - решение для криптографической защиты ИСУЭ

ЭТАП 1 (ИСУЭ 1.0) – СКЗИ в ИВК и ИВКЭ

- Криптомодуль **ViPNet SIES Core** предназначен для встраивания в УСПД и коммуникационные шлюзы
- ПО **ViPNet SIES Unit** предназначено для интеграции с ИВК
- ПАК **ViPNet SIES MC** предназначен для управления ключевой информацией решения, размещается у субъекта КИИ
- ПО **ViPNet SIES Workstation** отвечает за инициализацию ViPNet SIES Core и автоматизацию при разворачивании решения в эксплуатации

ЭТАП 2 (ИСУЭ 2.0) – СКЗИ в ИВК, ИВКЭ, ПУ

- Крипточип **ViPNet SIES Core Nano** предназначен для встраивания в приборы учета
- Ключевой центр **ViPNet SIES HSM** предназначен для выработки долговременных ключей крипточипа (до 16 лет)
- ПАК **ViPNet SIES Nano Loader** предназначен для загрузки ключей в ViPNet SIES Core Nano в условиях завода-производителя приборов учета

Защита данных ИСУЭ при передаче по каналам связи

Защита данных при передаче по каналам связи в ИСУЭ обеспечивается ViPNet SIES благодаря использованию протокола CRISP (Рекомендация по стандартизации РФ Р 1323565.1.029-2019*), который обеспечивает:

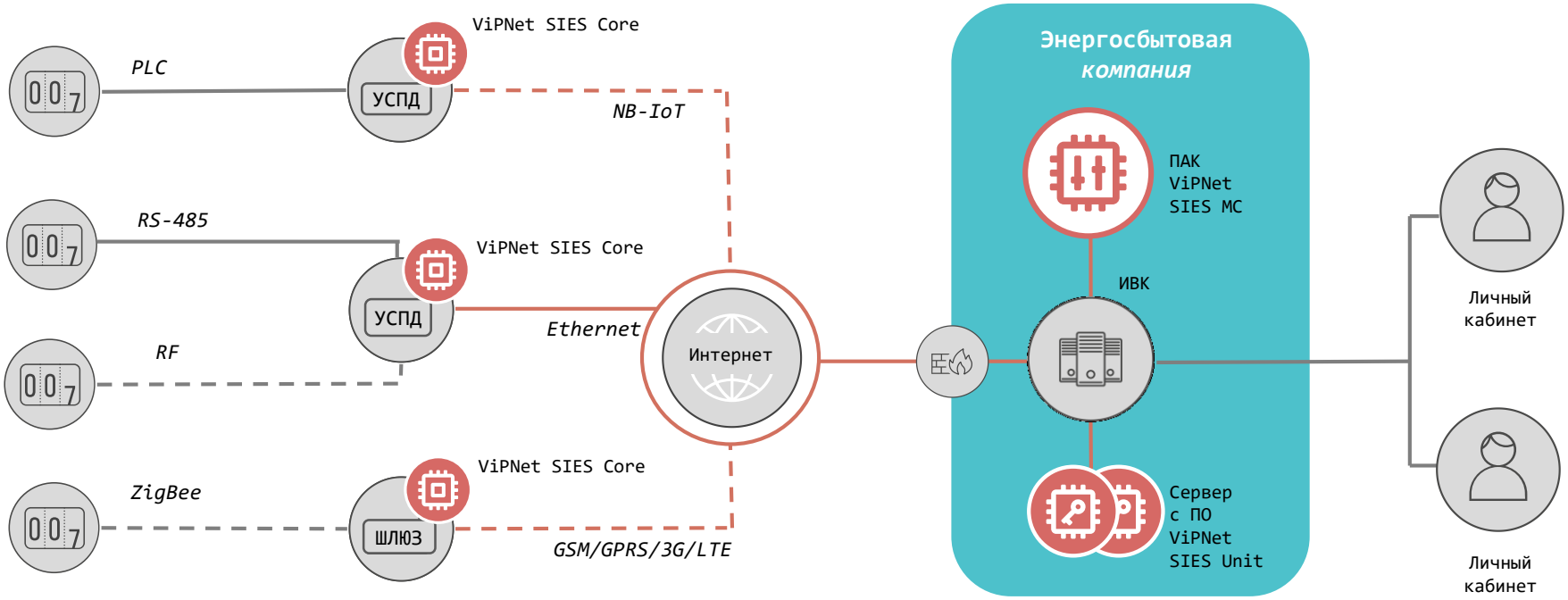
- Целостность
- Конфиденциальность (опционально)
- Защиту от навязывания повторных сообщений
- Аутентификацию источника сообщений

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

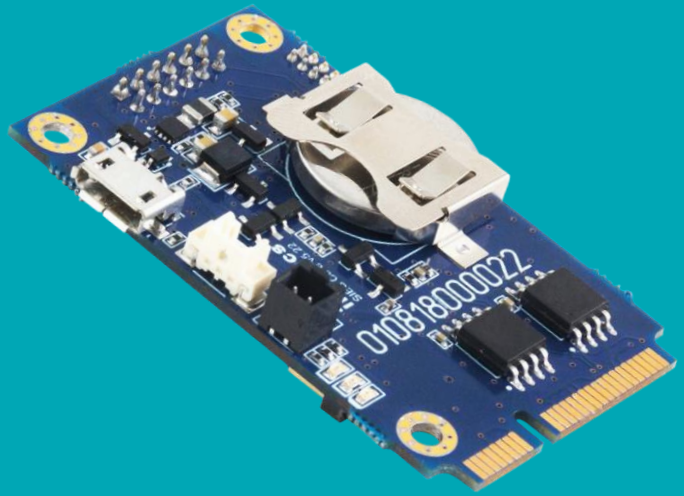
- Защита адресных и групповых сообщений
- Бессесионный криптографический протокол
- Минимальный оверхед и минимальная нагрузка на сеть
- Универсальный стандартизированный протокол защиты любых протоколов ИСУЭ

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

ИСУЭ 1.0 - защита ИСУЭ продуктами ViPNet SIES



ПРИБОРЫ УЧЕТА (ПУ) УРОВЕНЬ ИВКЭ УРОВЕНЬ ИВК



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 ⁰C
- Возможность использования вне контролируемой зоны при подключении ДНСД
- Наличие SDK под Linux (ARM, x86), Windows, RTOS
- Сертификат СКЗИ класса КС3 по требованиям ФСБ России

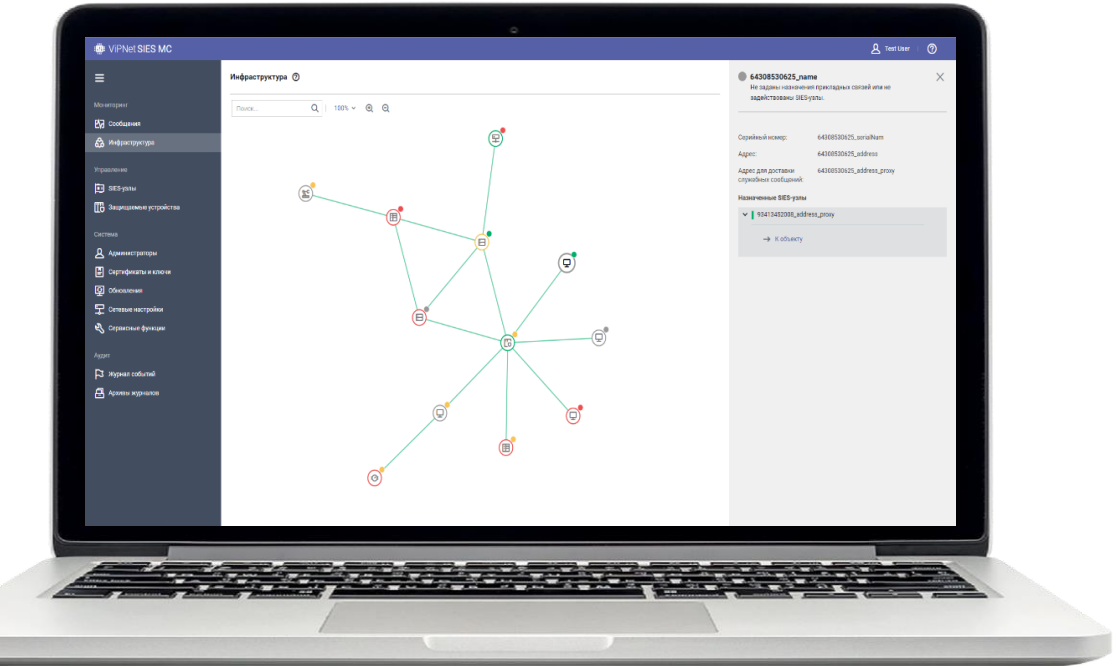
ПАК ViPNet SIES Core

ПО ViPNet SIES Unit

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
- 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 связей
- Сертификат СКЗИ класса КС1 и КС3 по требованиям ФСБ России

ПАК ViPNet SIES MC



- Ключевой и Удостоверяющий центры
- Управление связями в системе
- Управление ключевой информацией
- Управление активами
- Разграничение прав доступа к решению SIES
- UI — Доступ к интерфейсу по WedUI

Центр управления ViPNet SIES MC

ViPNet SIES MC VA

- Max: 5000-узлов
- Max: 500 администраторов безопасности
- Сертификат СКЗИ КС1

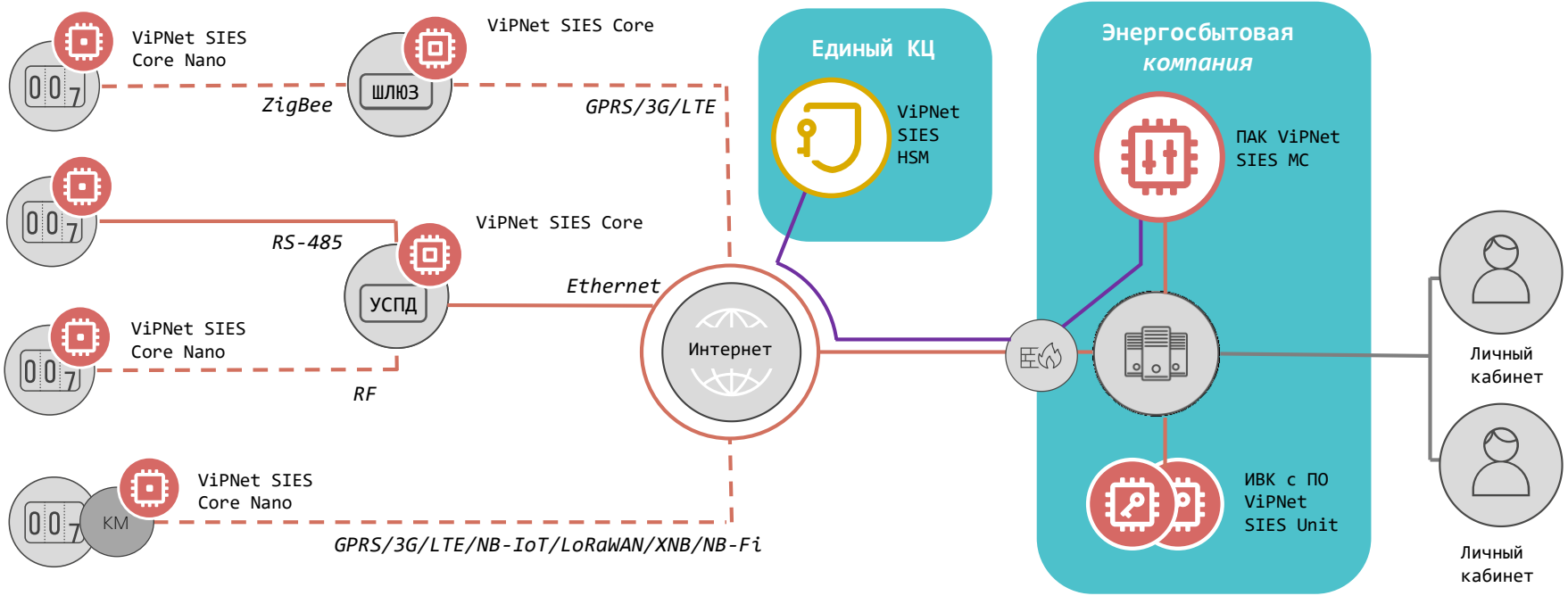
ViPNet SIES MC 3000

- Max: 3000-узлов
- Max: 300 администраторов безопасности
- Сертификат СКЗИ КС3

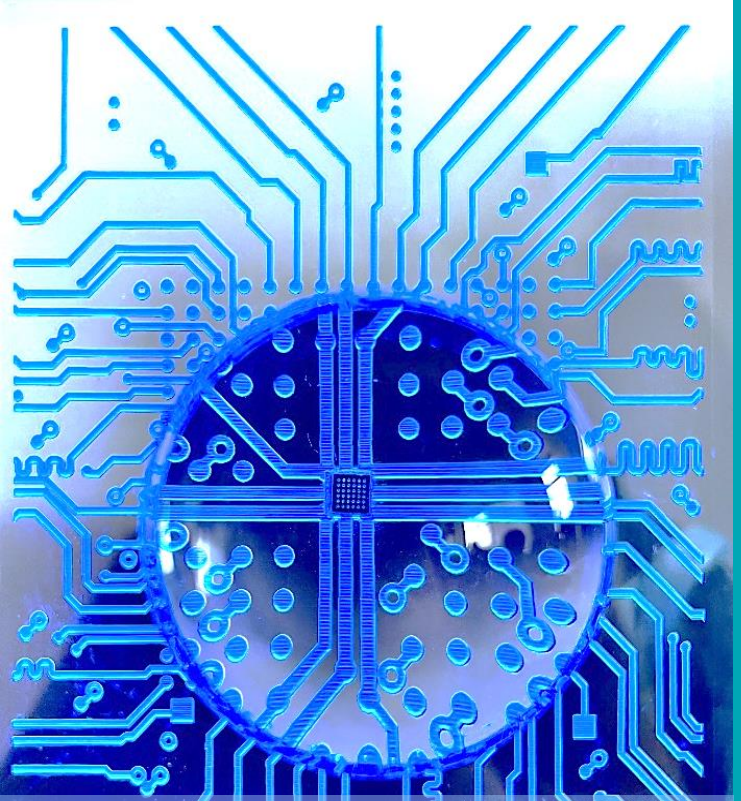
ViPNet SIES MC 10000

- Max: 1 млн узлов
- Max: 1000 администраторов безопасности
- Сертификат СКЗИ КС3

ИСУЭ 2.0 - защита ИСУЭ продуктами ViPNet SIES



ПРИБОРЫ УЧЕТА (ПУ) УРОВЕНЬ ИВКЭ УРОВЕНЬ ИВК



3x3x0,45 мм

ДЛЯ ИНТЕГРАЦИИ
В ПРИБОРЫ УЧЕТА
И КОММУНИКАЦИОННЫЕ
МОДУЛИ

ПАК ViPNet SIES Core Nano

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
- Рабочий диапазон температур -40…+85 ^{0}C
- Форм-фактор – микросхема 3x3x0,45 мм

Планируемая сертификация:

- СКЗИ-НР и СКЗИ класса КС3 (конец 2023 г.)

ПРАКТИЧЕСКИЙ ОПЫТ

ПРАКТИЧЕСКИЕ СЛОЖНОСТИ ВСТРАИВАНИЯ СКЗИ

Отсутствие единых требований к защите ИСУЭ со стороны профильных структур

Отсутствие опыта у разработчиков УСПД и ПУ по работе с СКЗИ

Отсутствие лицензий на работу с СКЗИ

Необходимость обеспечивать защиту цифровой системы XXI века по нормативным документам, разработанным в прошлом веке

Результаты:

1. 4 из 10 вендоров встроили СКЗИ ViPNet SIES Core в УСПД/шлюзы/базовые станции, в том числе работающие по протоколам каналов GSM, LoRaWan
2. Один вендор (НТЦ «Нартис») завершил работы по оценке влияния шлюза на СКЗИ ViPNet SIES Core, ведется опытная эксплуатация
3. Согласовано ТЗ на крипточип SIES Core Nano с хранением ключей до 16 лет
4. Более 15 вендоров запросили комплект разработчика SIES Core Nano для встраивания в ПУ и модули связи

Открытые вопросы

1

Изменения в ПП313

- Распространение, настройка и монтаж устройств с СКЗИ – это лицензированные виды деятельности и требуют

2

Замена инструкции №152 ФАПСИ

- Невозможен поэкземплярный учет миллиона устройств

3

Изменения ПКЗ-2005

- Порядок проведения оценки влияния
- Невозможен поэкземплярный учет миллиона устройств

4

Разработка требований к встраиваемым СКЗИ

- Встраивание в устройства без привязки к конкретной системе
- Сроки действия заключения и сертификатов

Спасибо за внимание!

Марина Сорокина

e-mail: marina.sorokina@infotecs.ru

Подписывайтесь на наши соцсети

https://vk.com/infotecs_news

https://t.me/infotecs_news