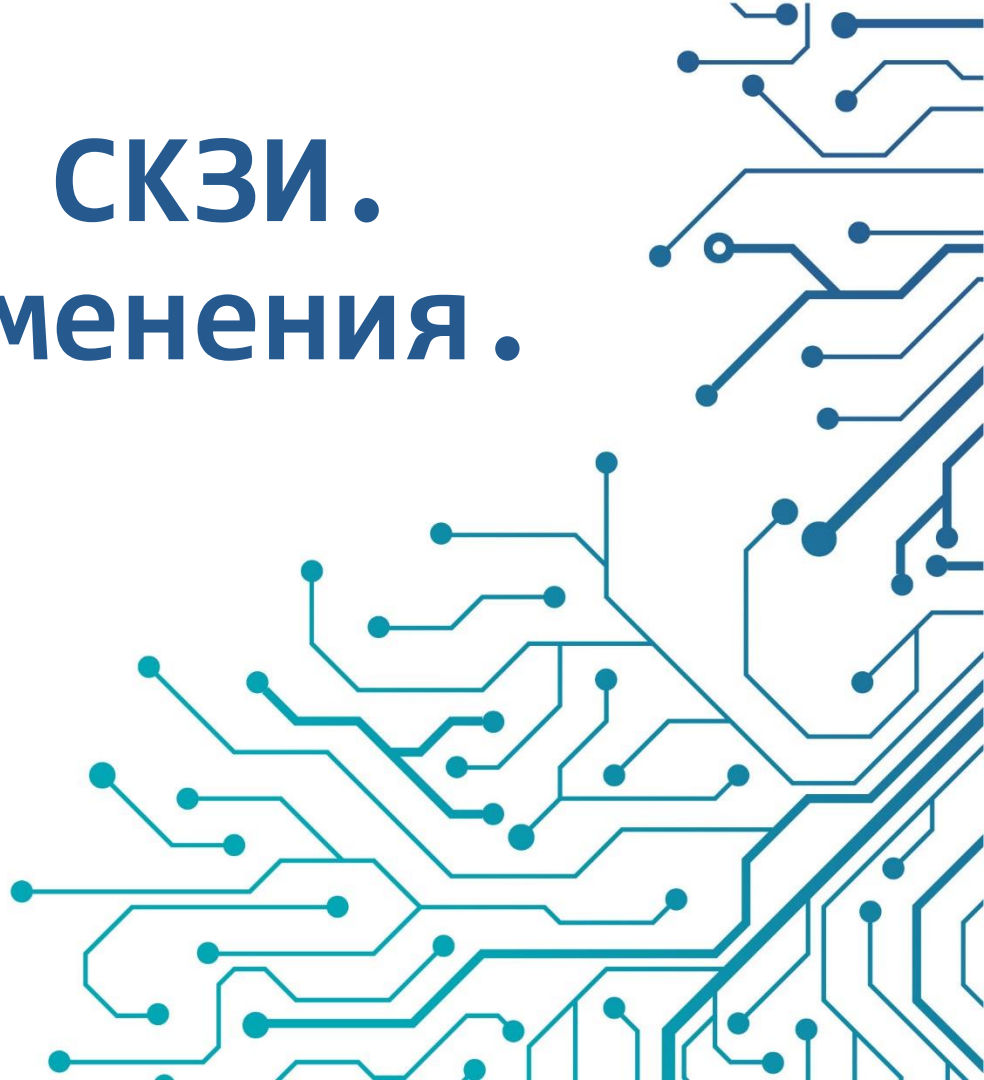
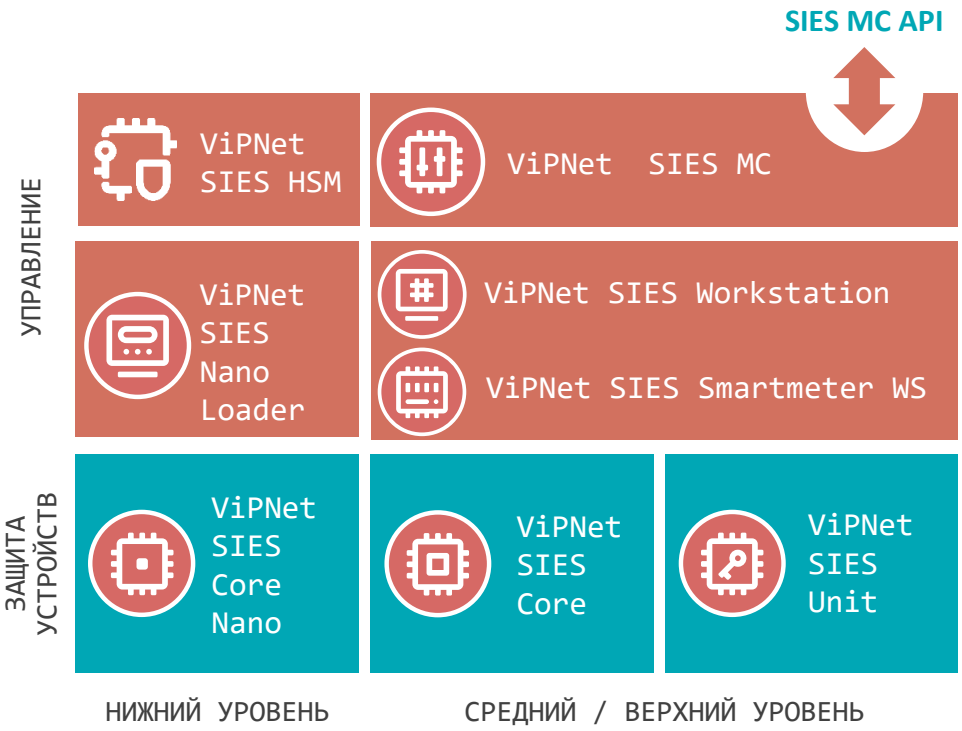
Встраиваемые СКЗИ. Сценарии применения.

Марина Сорокина,
Руководитель продуктового направления



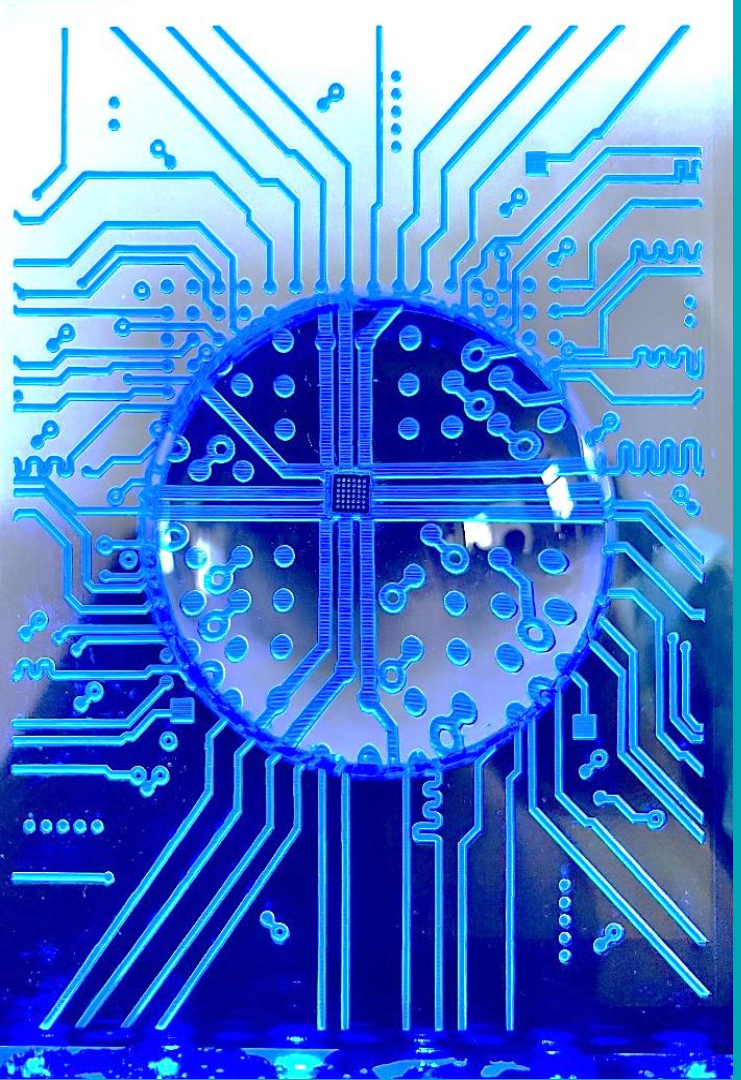
infotecs

Продукты ViPNet SIES



ViPNet SIES – комплекс продуктов для криптографической защиты информации компонентов АСУ ТП и IIoT-устройств:

- ПАК ViPNet SIES Core Nano - для встраивания в датчики и другие IIoT-устройства
- ПАК ViPNet SIES Core - для встраивания в концентраторы данных, IIoT-шлюзы
- ПК ViPNet SIES Unit - для интеграции с серверами и рабочими станциями
- ПАК ViPNet SIES MC - для управления ключевой информацией компонентов АСУ ТП и IIoT-устройств
- ПК ViPNet SIES Workstation – для инициализации ViPNet SIES Core и SIES Unit
- SIES MC API – API для интеграции сторонних СКЗИ в решение ViPNet SIES

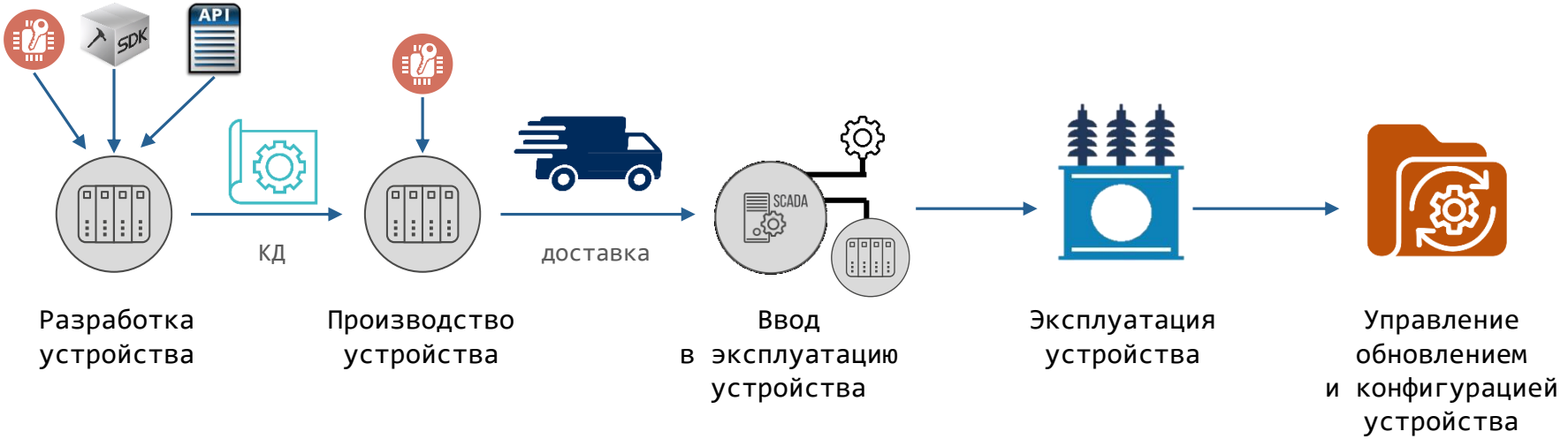


ViPNet SIES Core Nano – СКЗИ для интеграции в IIoT-устройства и приборы учета и

ФОРМ-ФАКТОР:

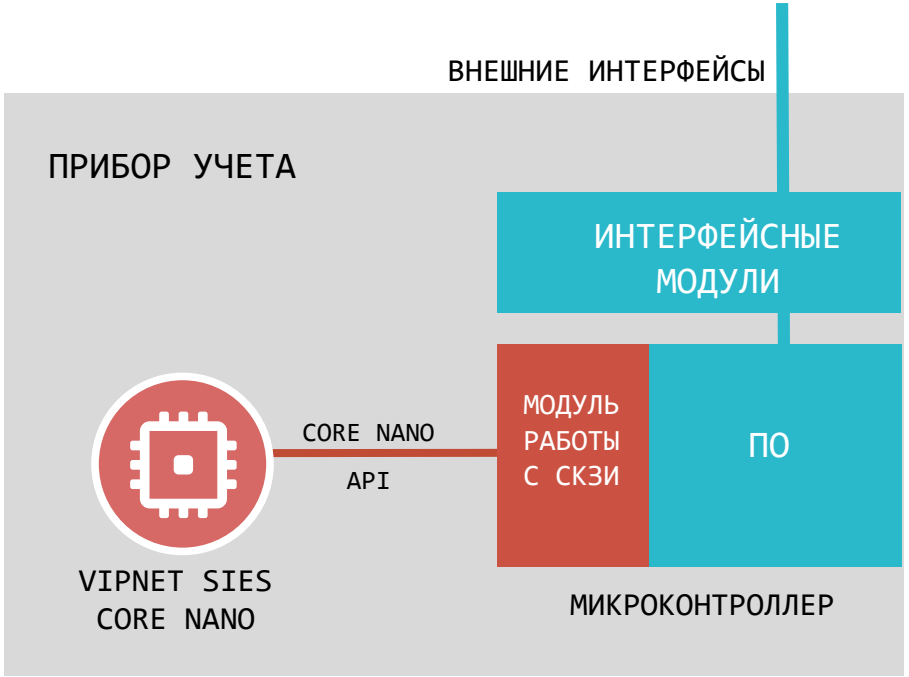
- Форм-фактор – микросхема 3x3x0,4 мм
- Рабочий диапазон температур -40…+85 ⁰C
- Напряжение питания – 3,3В
- Ток потребления – 8мА
- Инженерные меры защиты по требованиям к СКЗИ-НР

Встраивание СКЗИ в концепции Security by Design



Встраивание ViPNet SIES Core Nano в IIoT-устройства или прибор учета

- Интеграция на аппаратном уровне – SPI
- Интеграция на программном уровне – Core Nano API
- Место установки – завод, производящий устройства

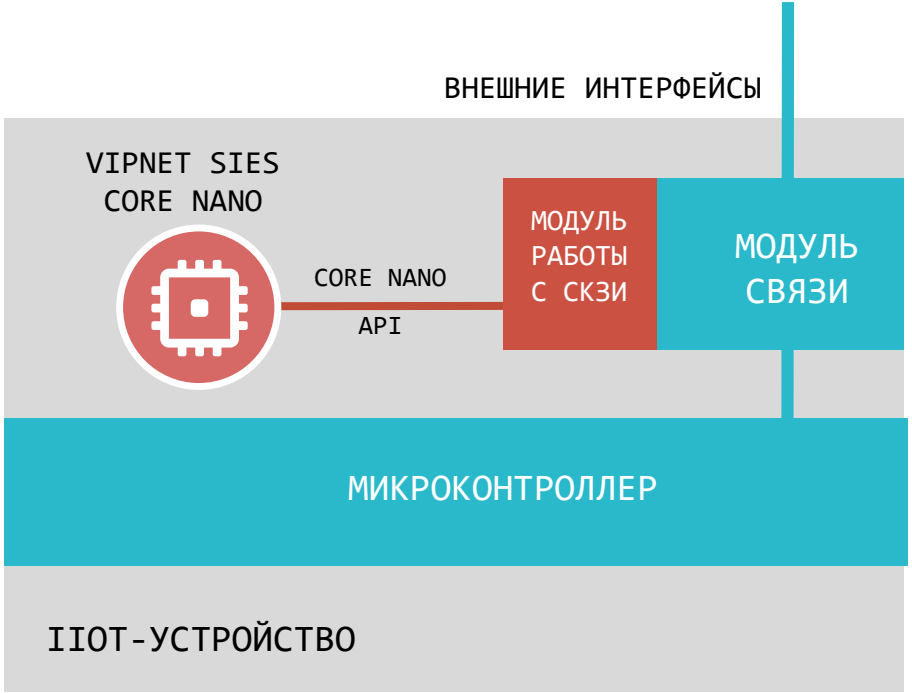


Встраивание ViPNet SIES Core Nano в модули связи

Интеграция на аппаратном уровне – SPI

Интеграция на программном уровне – Core Nano API

Место установки – завод, производящий модули связи



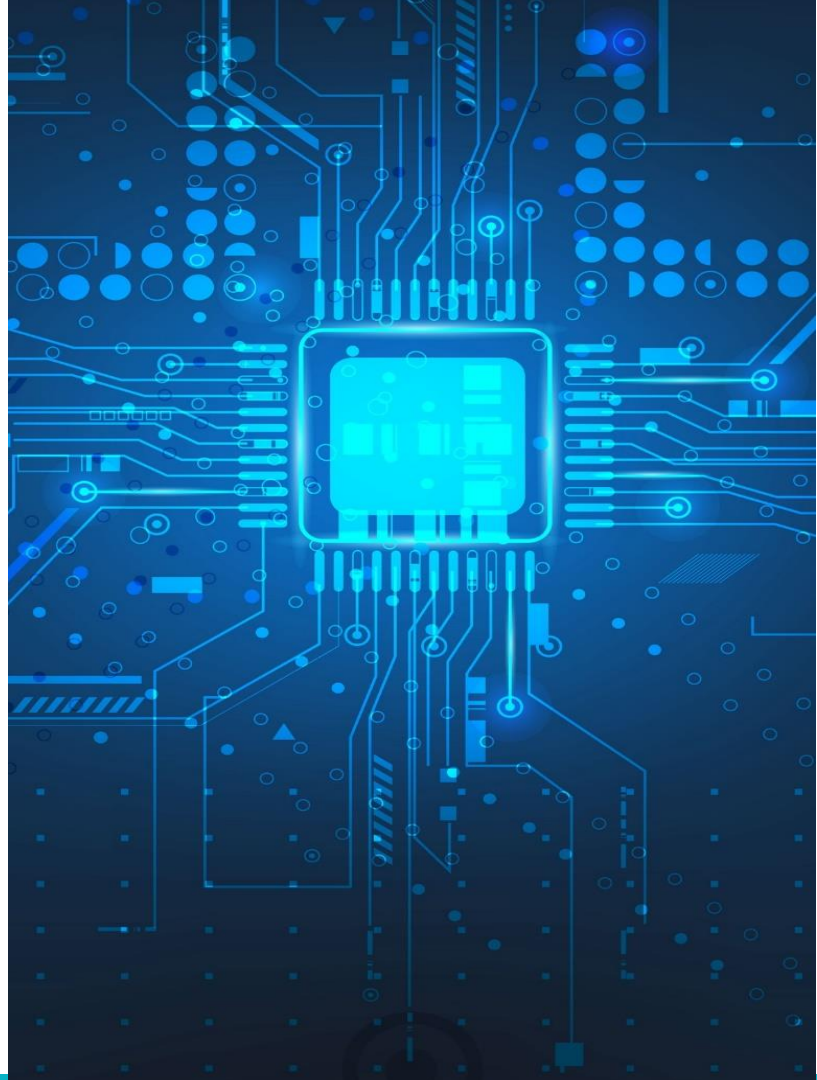
СКЗИ ViPNet SIES Core Nano

Срок службы: 16 лет

Срок хранения ключей: 16 лет

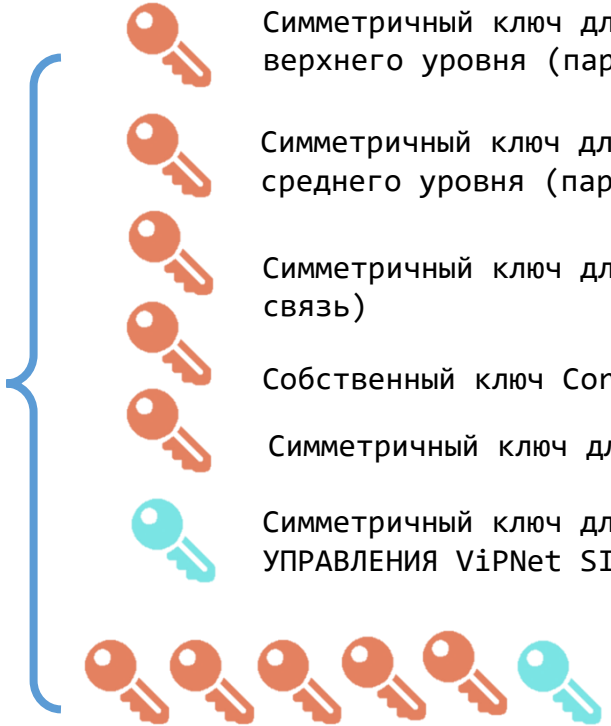
Срок действия ключей: 16 лет

Работа в необслуживаемом режиме 24/7/365



Характеристики ViPNet SIES Core Nano

СРОК СЛУЖБЫ 16 ЛЕТ



Симметричный ключ для обмена данными с устройством верхнего уровня (парная связь)

Симметричный ключ для обмена данными с устройством среднего уровня (парная связь)

Симметричный ключ для обмена данными с устройством (парная связь)

Собственный ключ Core Nano

Симметричный ключ для резервированной связи

Симметричный ключ для обмена данными с ЦЕНТРОМ УПРАВЛЕНИЯ ViPNet SIES MC

Резервный набор ключей

СКЗИ ViPNet SIES Core Nano

Криптографический протокол - Р 1323565.1.029–2019 (CRISP) (наборы 3 и 4)

Криптографические алгоритмы - ГОСТ Р 34.12-2018, ГОСТ Р 34.13-2018, ГОСТ Р 34.11-2018

Соответствие требованиям:

- СКЗИ класса КС3*
- СКЗИ-НР* в части защиты атак инженерного проникновения

В процессе тематических исследований, ожидание сертификата – Q3– Q4 2024 г.

Криптографические операции:

Защита данных с помощью протокола CRISP

- 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

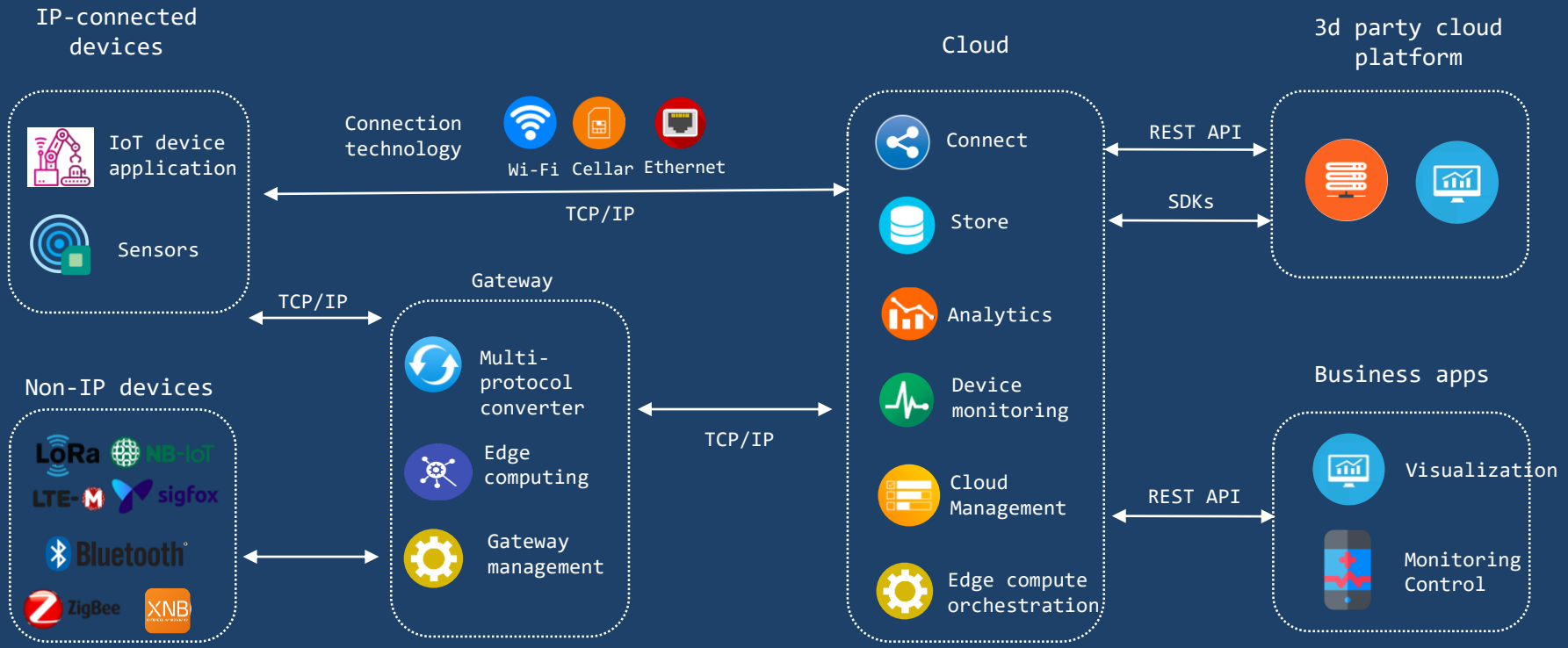
Минимальный оверхед и минимальная нагрузка на сеть

Универсальный стандартизированный протокол защиты любых протоколов ИСУЭ

Сценарии применения

Защита данных, передаваемых по каналам связи IIoT-систем

Типовая архитектура IIoT-системы



Беспроводные каналы связи IoT в РФ

	Технология	Радиус действия	Скорость передачи	LPWAN	Non-IP	Сотовый стандарт	Гармониза-ция в РФ	Провайдеры
1	ZigBee	500-1000 м	20-250 Кбит/с	-	+	-		-
2	Wi Fi	50-500 м	До 600 Мбит/с	-	-	-		-
3	GSM	1 км	1 Мбит/с	-	-	+		МТС, Билайн, Мегафон и т.д
4	LoRaWAN	10 км	0,3-50 Кбит/с	+	+	-	+	ЭР-Телеком, Лартех
5	NB-IoT	До 5 км	250 Кбит/с	+	+	+	-	МТС, Мегафон
6	Стриж XNB EXTENDED NARROWBAND	10-50 км	100 бит/с	+	+	-	Разработан в РФ	СРТ, ГЛОНАСС-ТМ
7	NB-Fi waviot	16,6 км	10-100 бит/с	+	+	-	Разработан в РФ	Вавиот

IIoT-системы требуют новых подходов к информационной безопасности

Отсутствие периметра

Территориально-распределенное размещение

Большая вариативность технологий

Малые вычислительные ресурсы устройств

Множество не стандартизированных протоколов

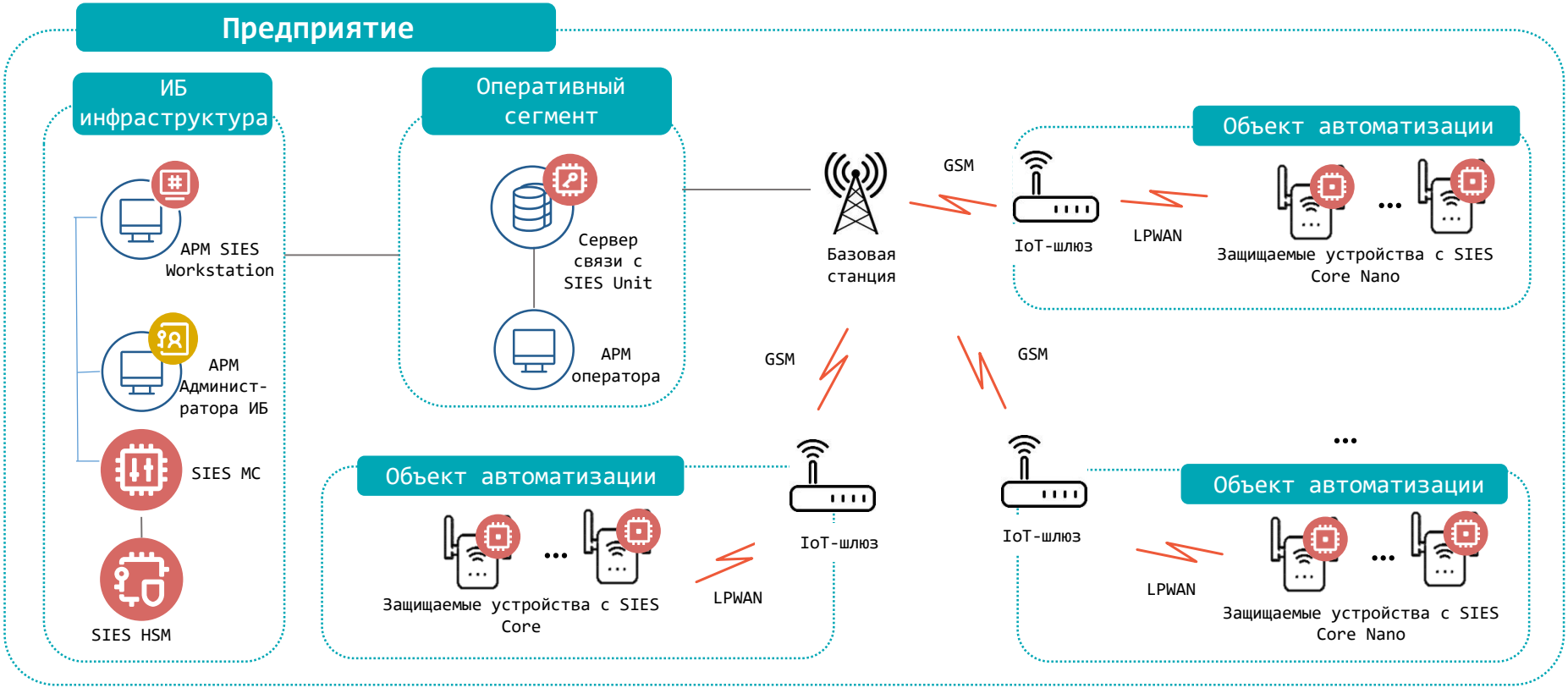
Возможность физического доступа

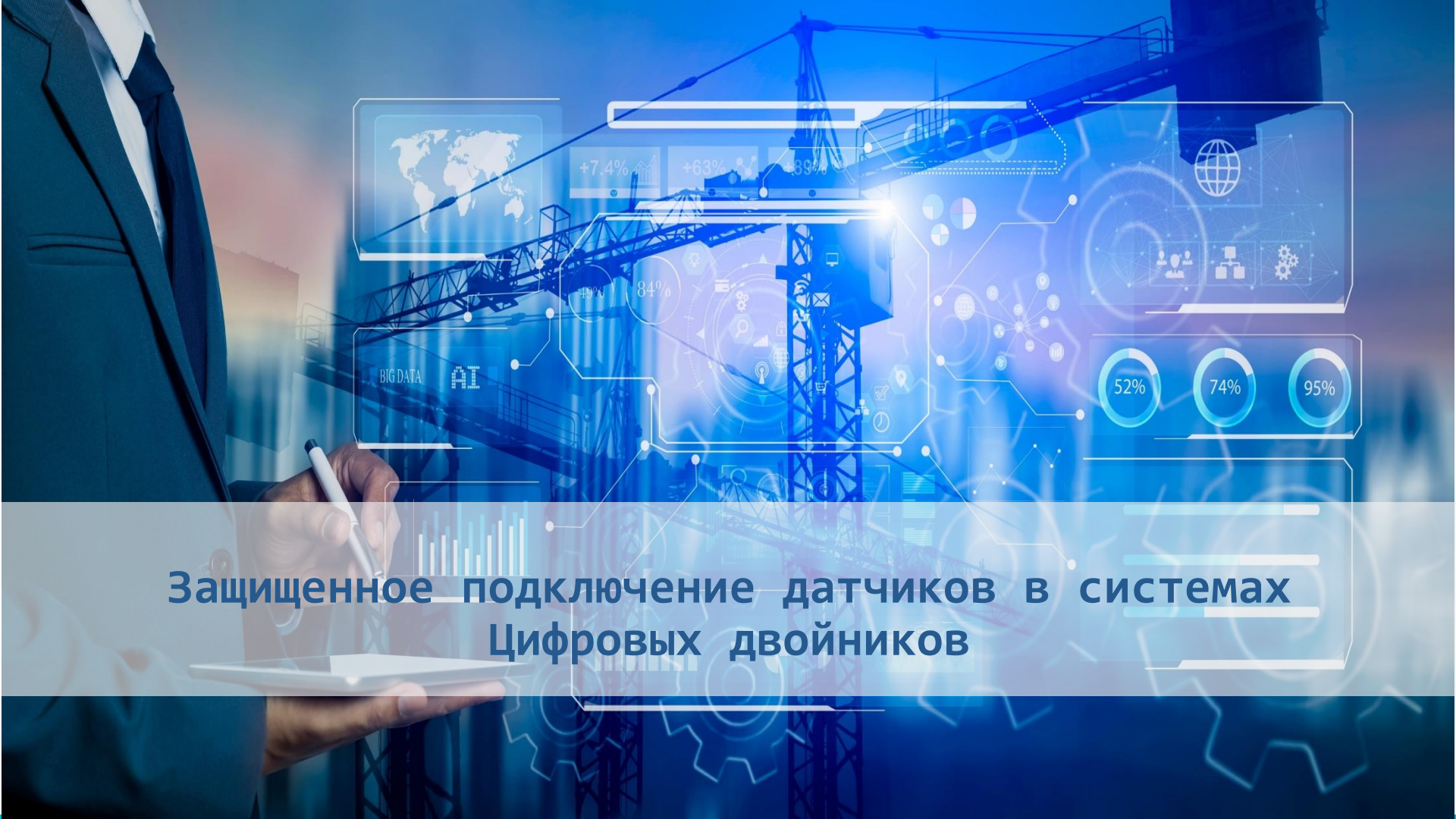
Высокая латентность полевых протоколов

Низкая пропускная способность полевых протоколов

Групповые операции

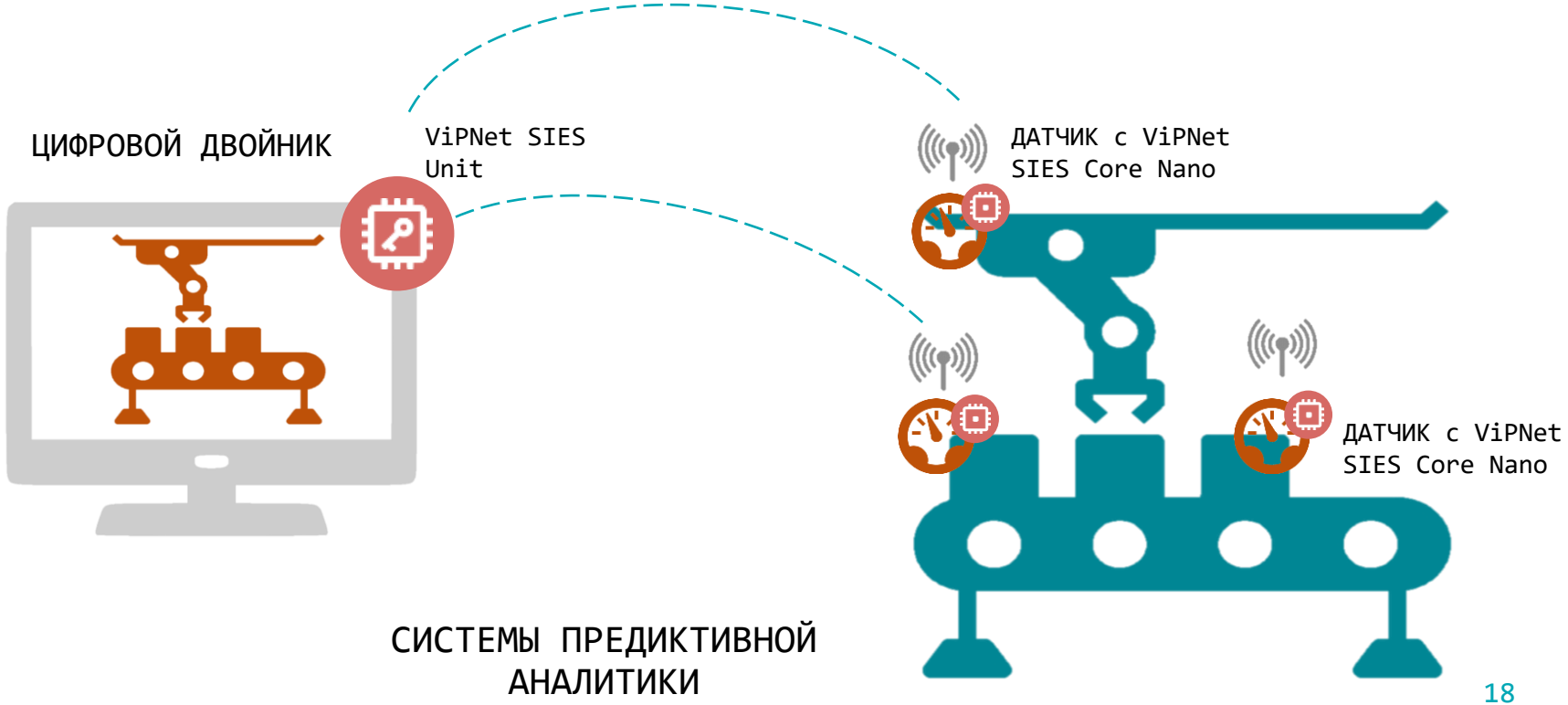
Типовые схемы защиты информации в IIoT





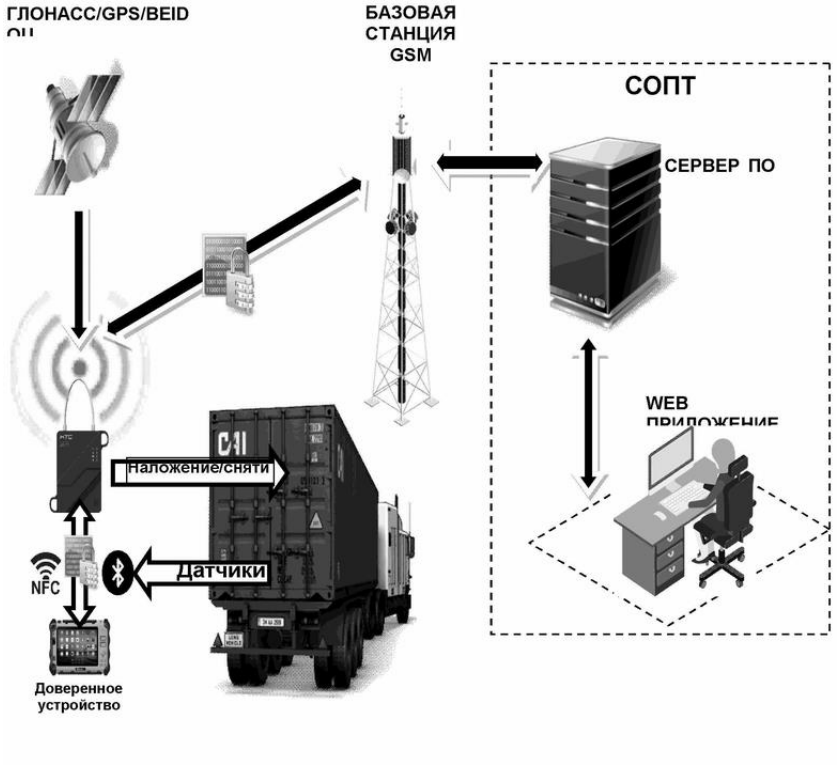
Защищенное подключение датчиков в системах Цифровых двойников

Защита систем сбора информации для предиктивной аналитики



Защищенные электронные навигационные пломбы

Электронная навигационная пломба



Назначение пломбы:

- Сохранность грузов
- Прослеживаемость перевозок
  - Мониторинга состояние (наложена, вскрыта или иное состояние)
  - мониторинг местоположения и скорости движения на карте
  - анализ треков каждой перевозки позволяет выявлять отклонения на маршруте и оптимизировать маршруты доставки
- Сообщения о нештатных ситуациях:
  - нарушение целостности корпуса ЭНП
  - взлом запорного штыря или перерезание троса
  - потеря связи
  - Низкий уровень заряда

Единые требования к электронной навигационной пломбе

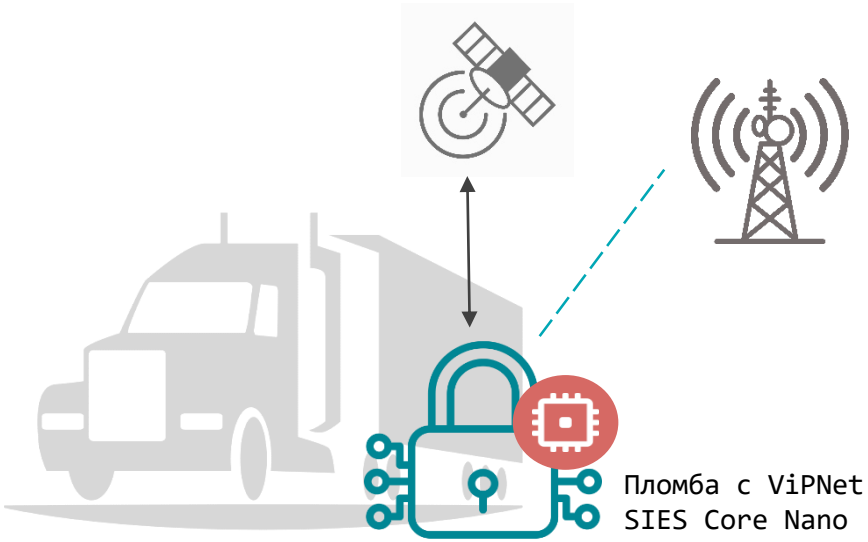
Решение Совета Евразийской экономической комиссии от 4 июля 2023 г. N 75 "О требованиях к навигационным пломбам, применяемым при перевозках товаров по территориям двух и более государств - членов Евразийского экономического союза"

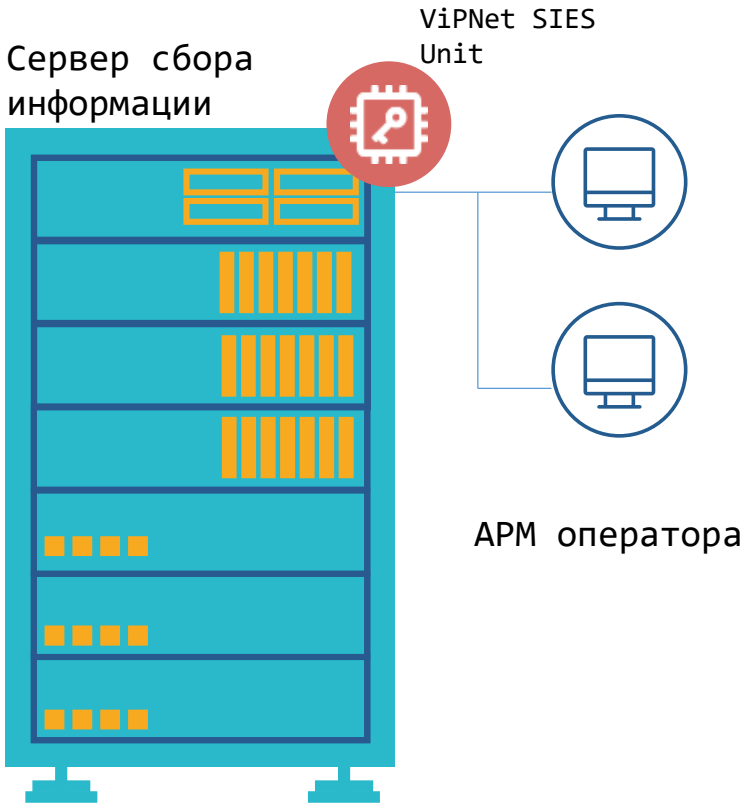
Совета Евразийской экономической комиссии от 29 августа 2023 г. N 82 « О ЕДИНЫХ МЕРАХ ЗАЩИТЫ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В НАВИГАЦИОННОЙ ПЛОМБЕ»

Единые меры защиты информации, содержащейся в навигационной пломбе:

- обеспечение конфиденциальности информации с применением одного или нескольких стандартов - ГОСТ 34.12-2018, ГОСТ 34.13-2018, СТБ 34.101.31-2020, ГОСТ 34.311-95, СТ РК ГОСТ Р 34.11-2015, ГОСТ 28147-89, ГОСТ 34.310-2004;
- обеспечение целостности, подлинности, невозможности отказа от авторства информации с применением одного или нескольких стандартов -ГОСТ 34.10-2018, ГОСТ 34.11-2018, ГОСТ 34.310-2004, СТБ 34.101.45-2013, СТ РК ГОСТ Р 34.10-2015.

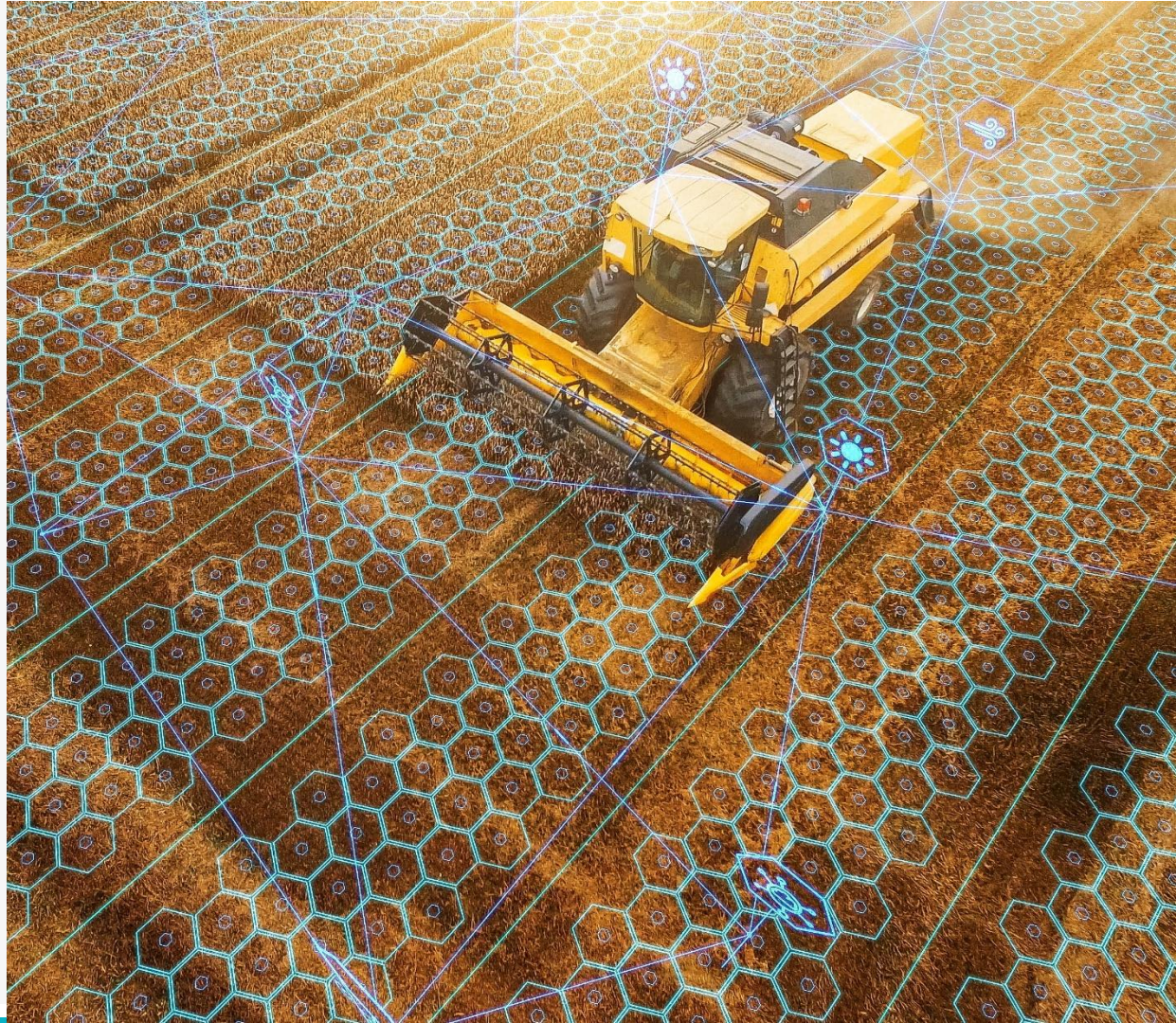
Защищенная электронная навигационной пломбе



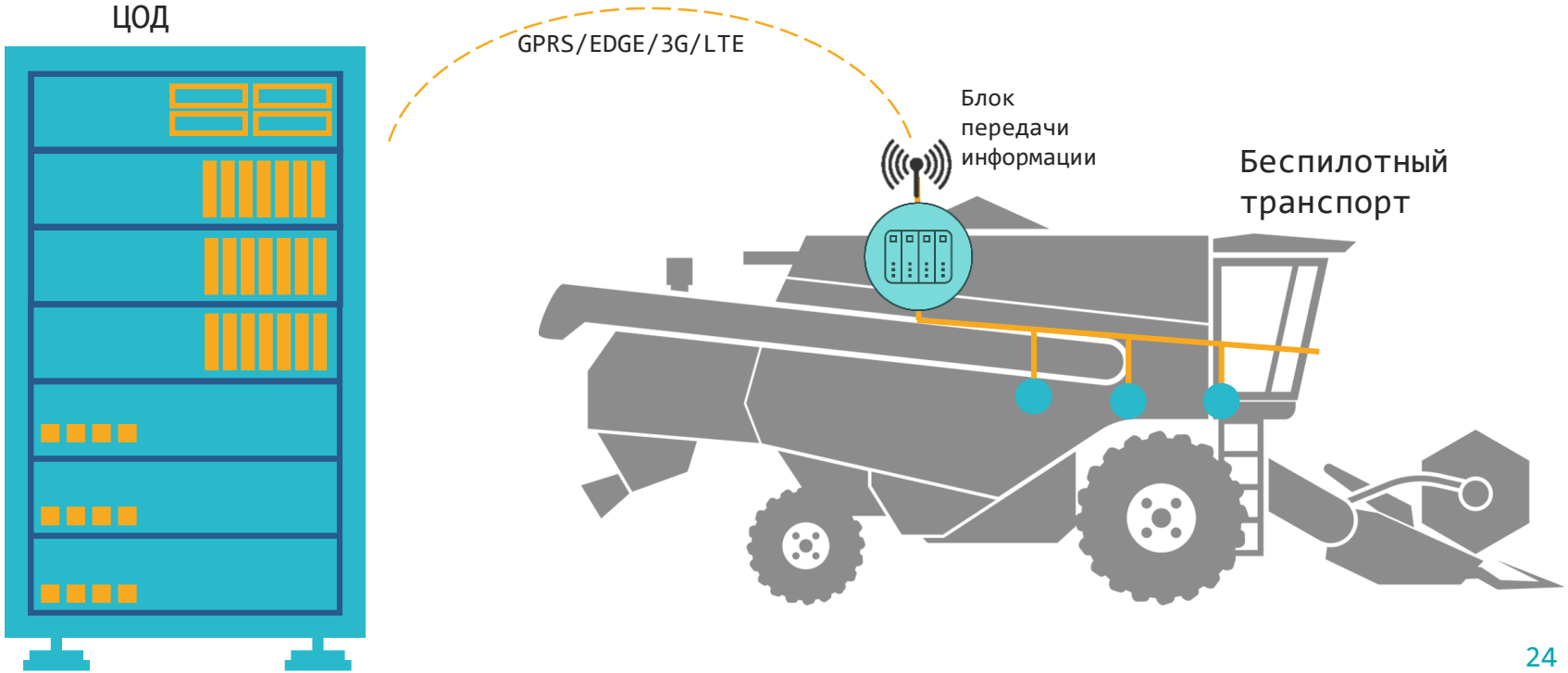


- Обеспечение конфиденциальности при передаче данных с помощью шифрования по протоколу CRISP с (алгоритм «Магма» ГОСТ 34.12-2018);
- Обеспечение целостности, подлинности с помощью функции хэширования (ГОСТ 34.11-2018)

Защита канала управления беспилотного транспорта



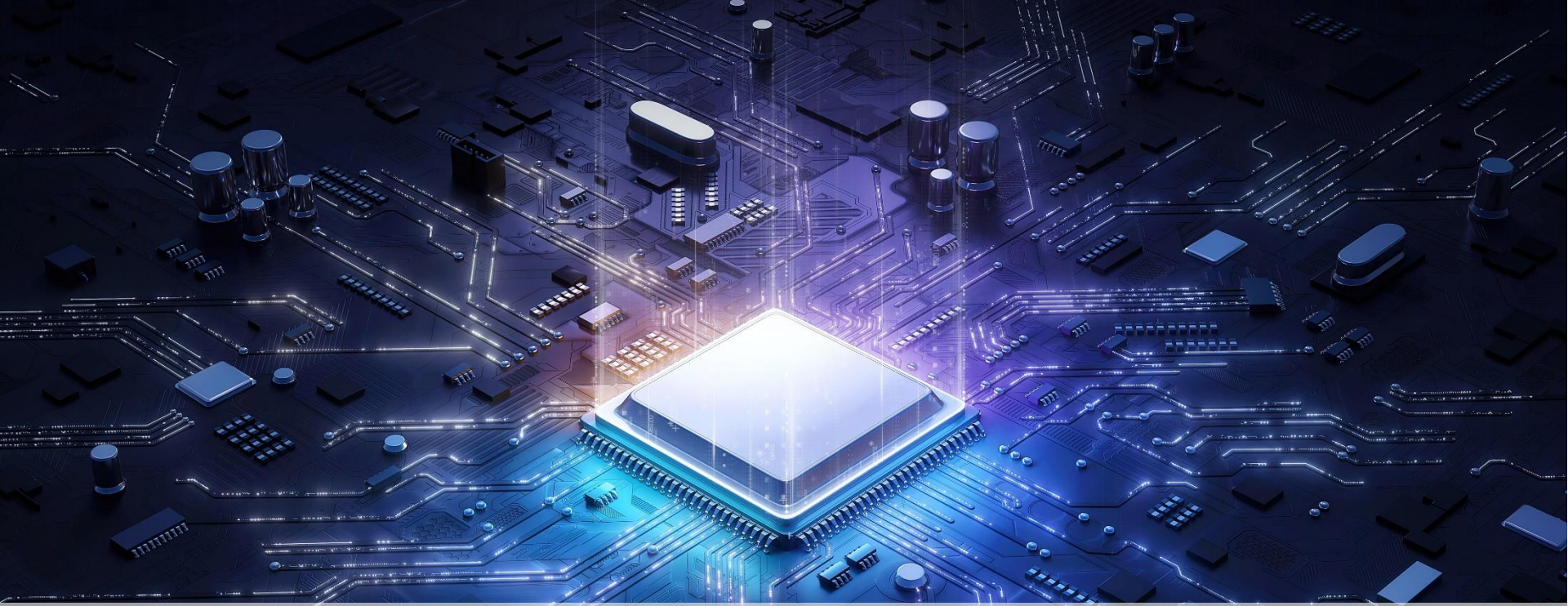
Обеспечение целостности и неизменяемости при передаче данных



Сбор телеметрии и управление сельскохозяйственным оборудованием

Обеспечение конфиденциальности и целости при сборе параметров измерения с медицинского оборудования

Защищенная передача данных с трекеров



Обеспечение доверия к устройству

infotecs

Спасибо за внимание

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363