

kaspersky



Kaspersky Industrial
Cybersecurity
Conference 2021

Марина Сорокина


Руководитель продуктового
направления, ИнфоТеКС, Россия

#KasperskyICS

Чат конференции: <https://kas.pr/kicscon>

Криптография для промышленных систем

Марина Сорокина
Руководитель направления отдела развития продуктов



**ЗАЧЕМ НУЖНА
КРИПТОГРАФИЯ
В ПРОМЫШЛЕННЫХ
СИСТЕМАХ?**

Криптографические
методы защиты
информации —
самые популярные
среди
разработчиков
устройств
автоматизации



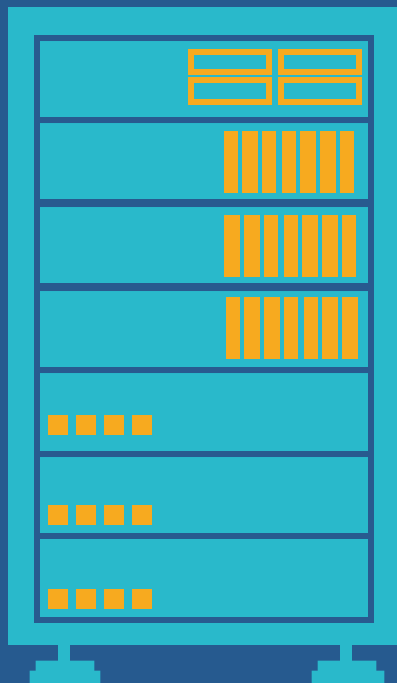
Некоторые сценарии применения криптографии в АСУ



- Защита каналов/ защита коммуникаций
- Безопасное хранение паролей
- Аутентификация и авторизация пользователя
- Аутентификация устройств и приложений
- Доверенное обновление ПО
- Обеспечение и проверка целостности запускаемых приложений
- Защищенное хранение чувствительной информации

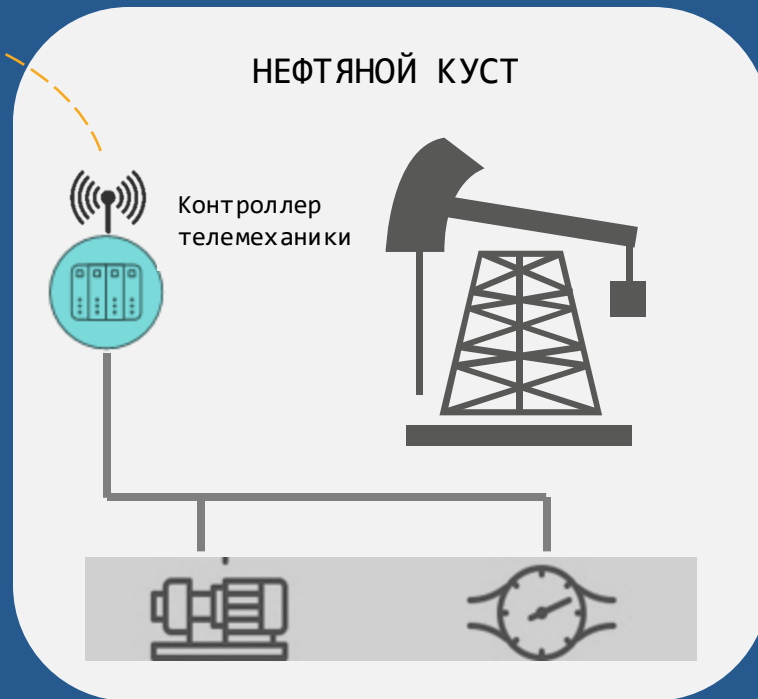
Защита каналов АСУ ТП

SCADA
(ДИСПЕТЧЕРСКИЙ ЦЕНТР)



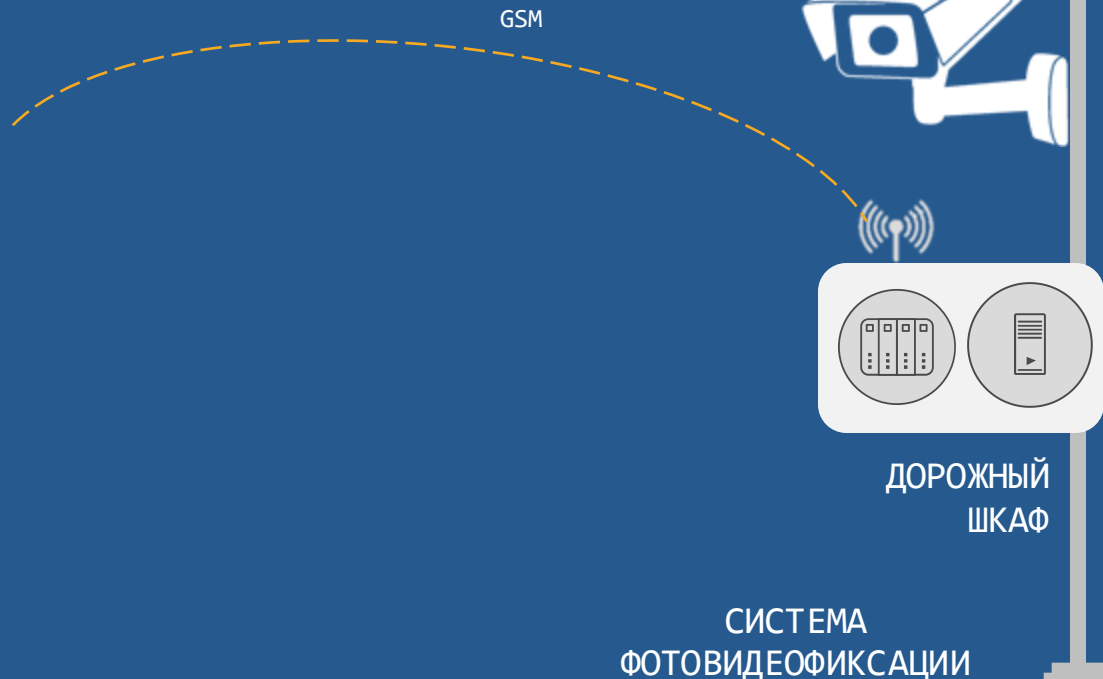
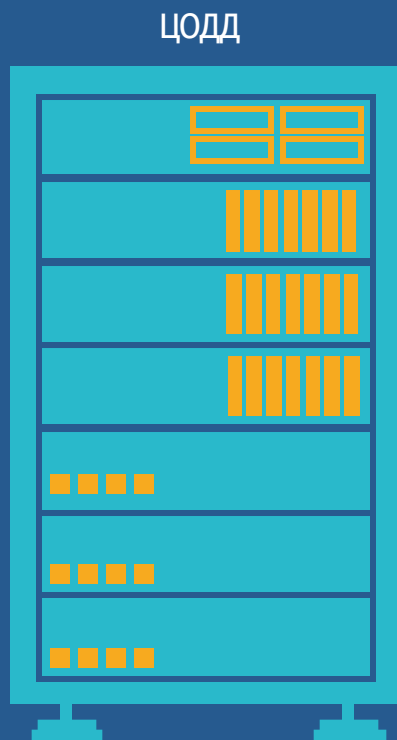
GSM

НЕФТЯНОЙ КУСТ

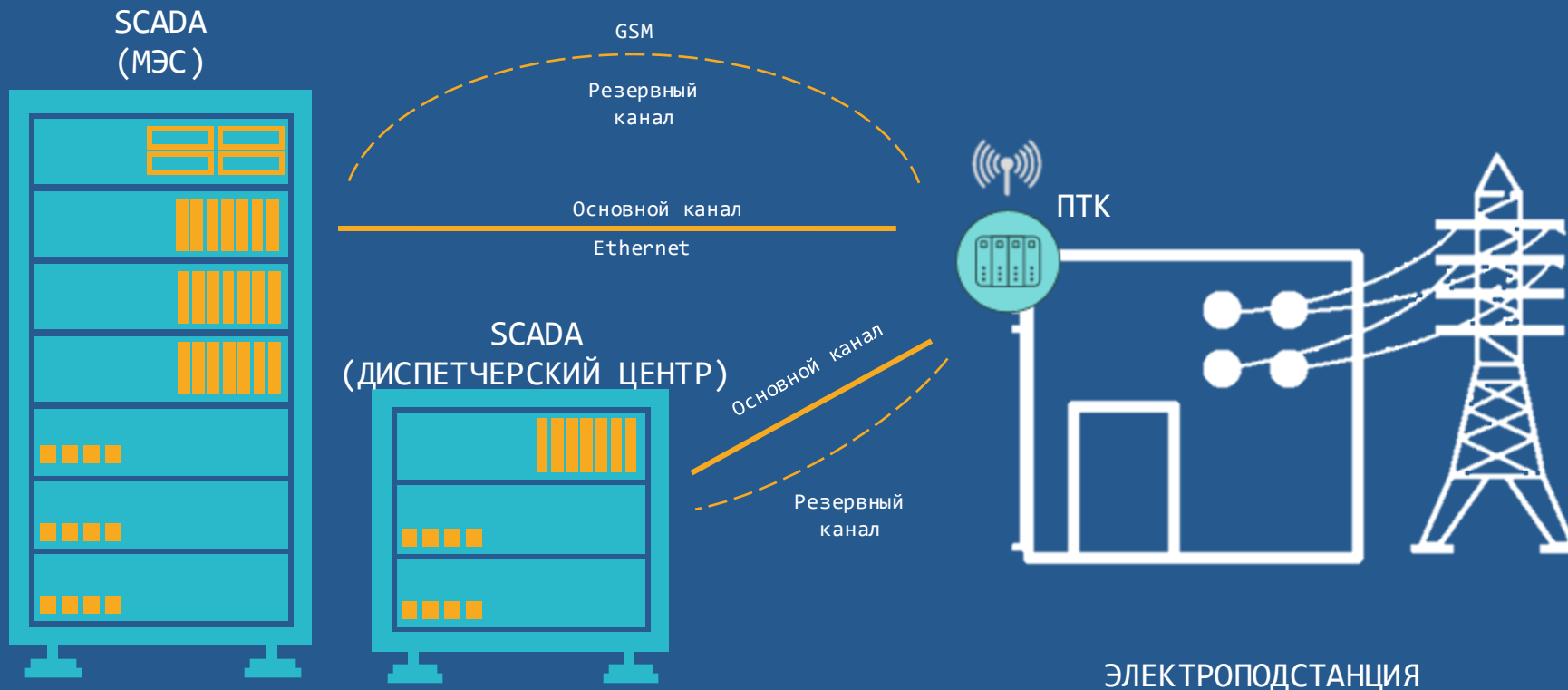


Контроллер
телемеханики

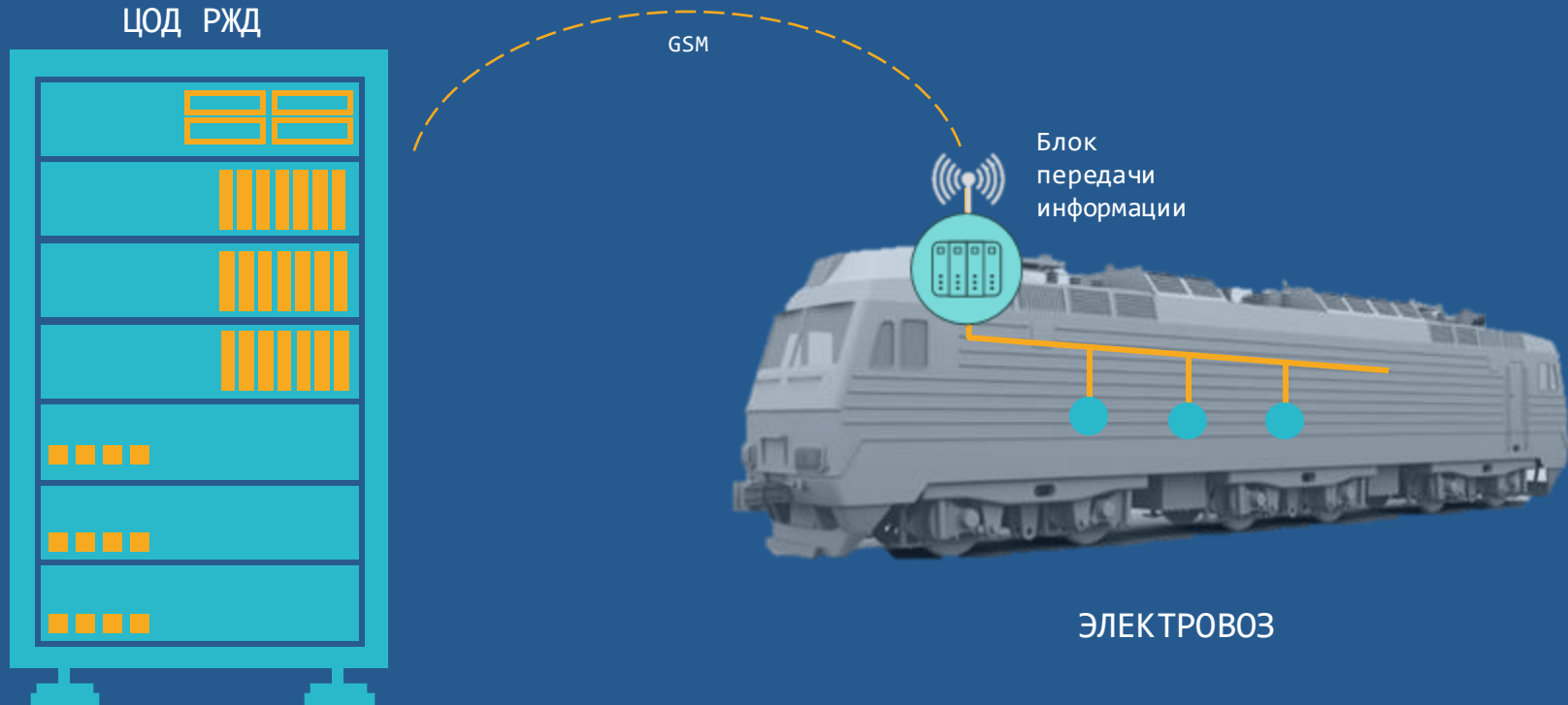
Защита каналов АСУ



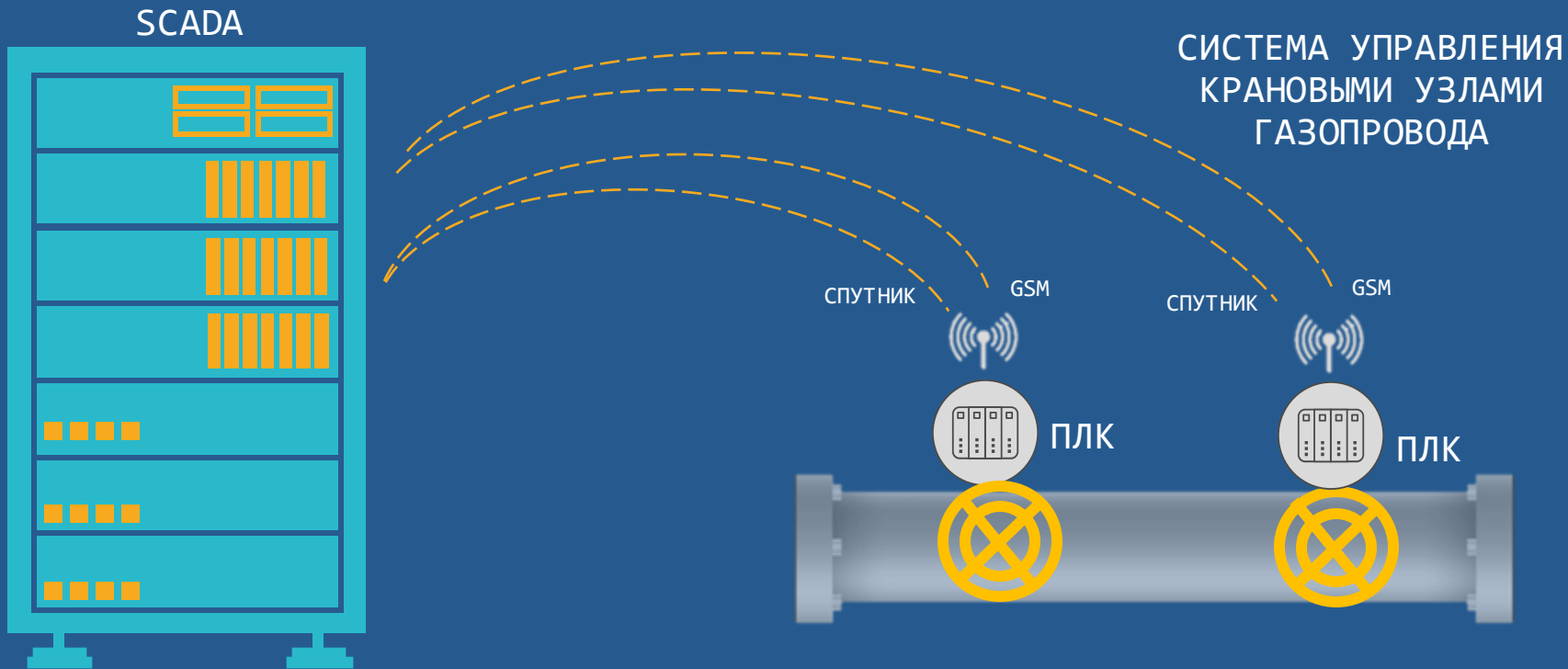
Защита резервируемых каналов АСУ



Обеспечение целостности и неизменяемости при передаче данных

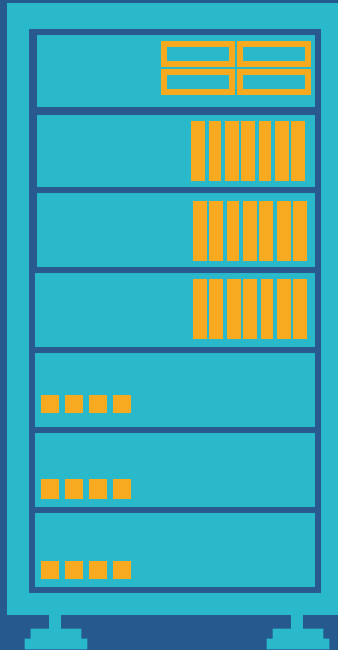


Защита спутниковых каналов в АСУ ТП



Защита каналов связи до смежных систем

SCADA
(ДИСПЕТЧЕРСКИЙ ЦЕНТР)

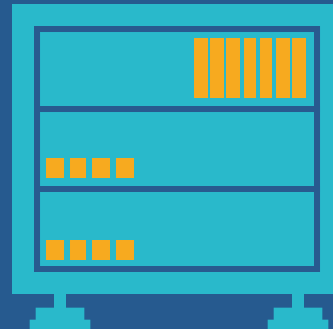


GSM

Резервный канал

Основной канал

МЭС



Основной канал

GSM

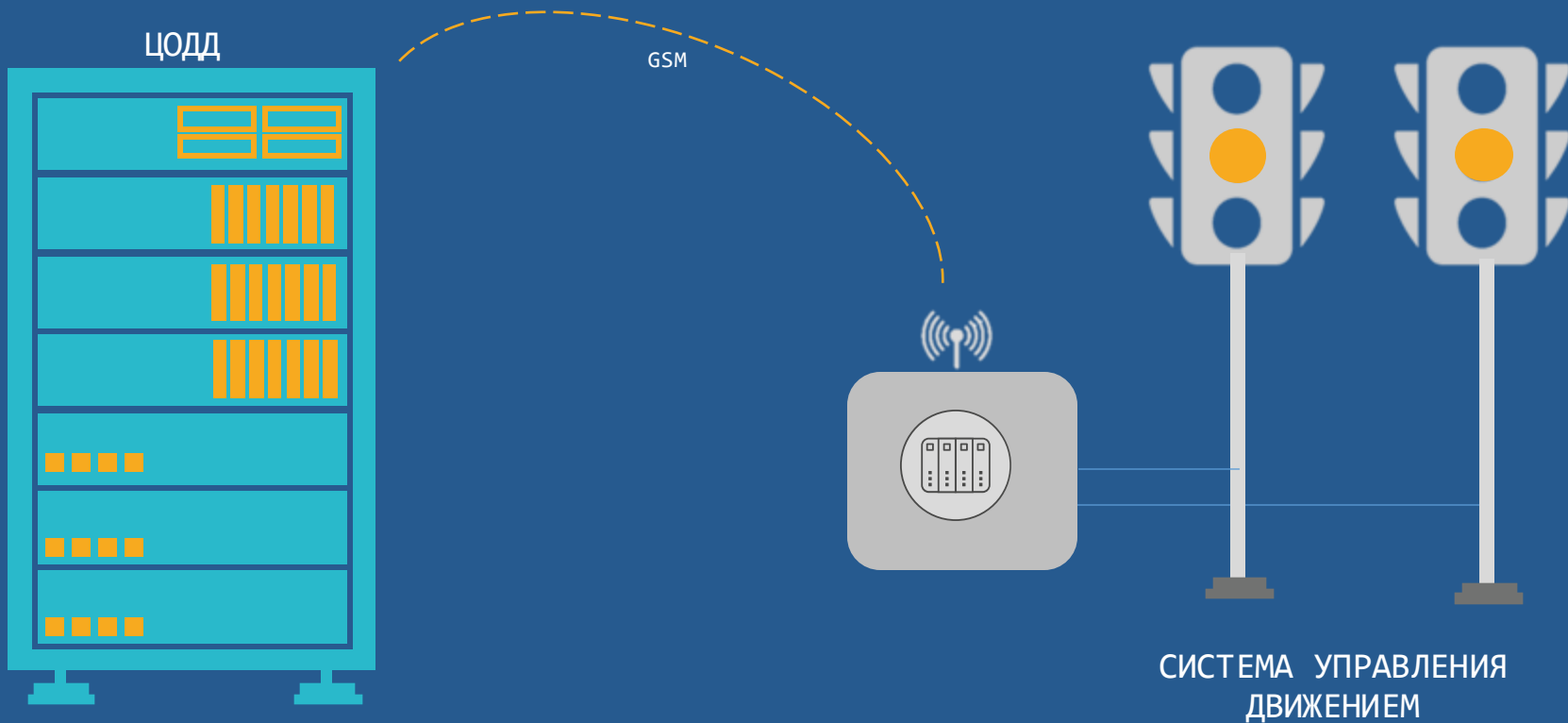
Резервный канал

ПЛК

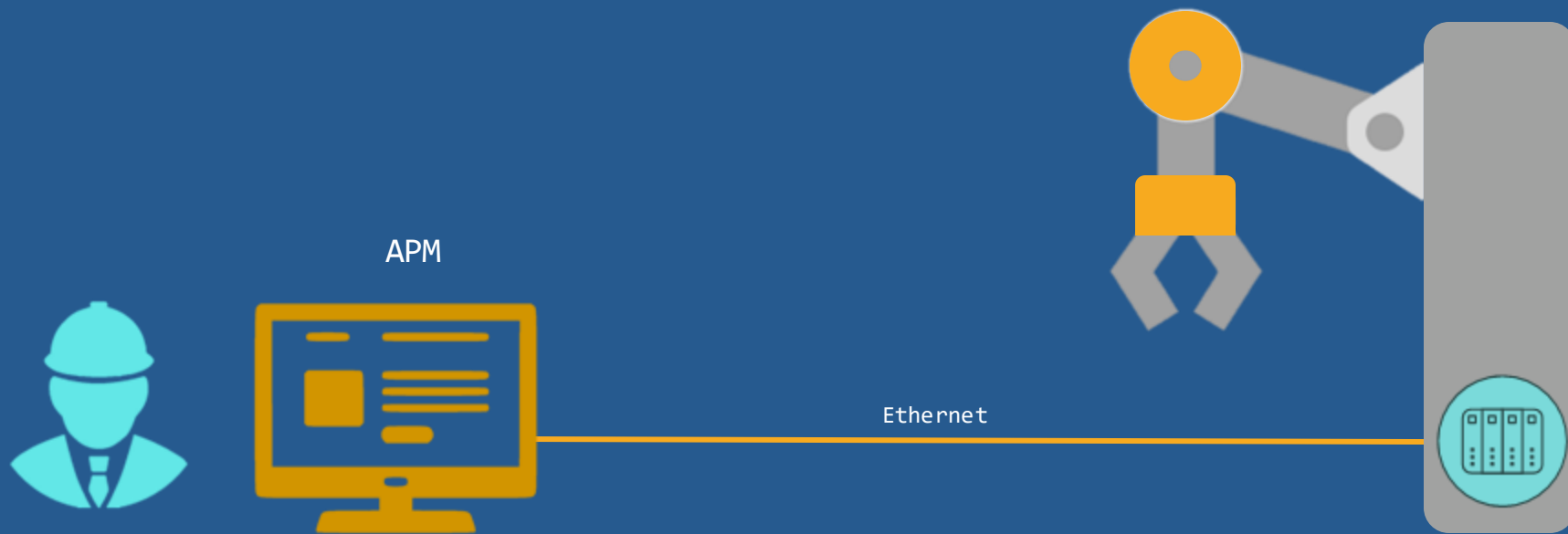


РЕКЛОУЗЕР

Идентификация объектов при управлении



Доверенное конфигурирование



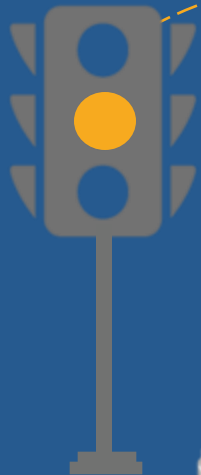
ПРОИЗВОДСТВЕННЫЕ
РОБОТЫ, СТАНКИ С ЧПУ

Удаленное сервисное обслуживание

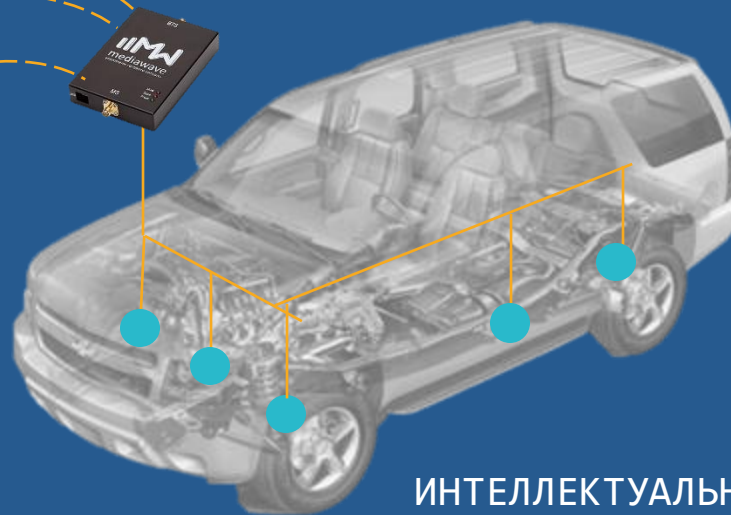


Доверенные коммуникации

ДОРОЖНАЯ
ИНФРАСТРУКТУРА



ТРАНСПОРТНЫЕ СРЕДСТВА НА ДОРОГЕ



ИНТЕЛЛЕКТУАЛЬНЫЙ
ТРАНСПОРТ

Техническое обслуживание и ремонт

ТОИР



ИНЖЕНЕР ОБХОДЧИК,
ЦИФРОВОЙ МОНТЕР

Wi-Fi



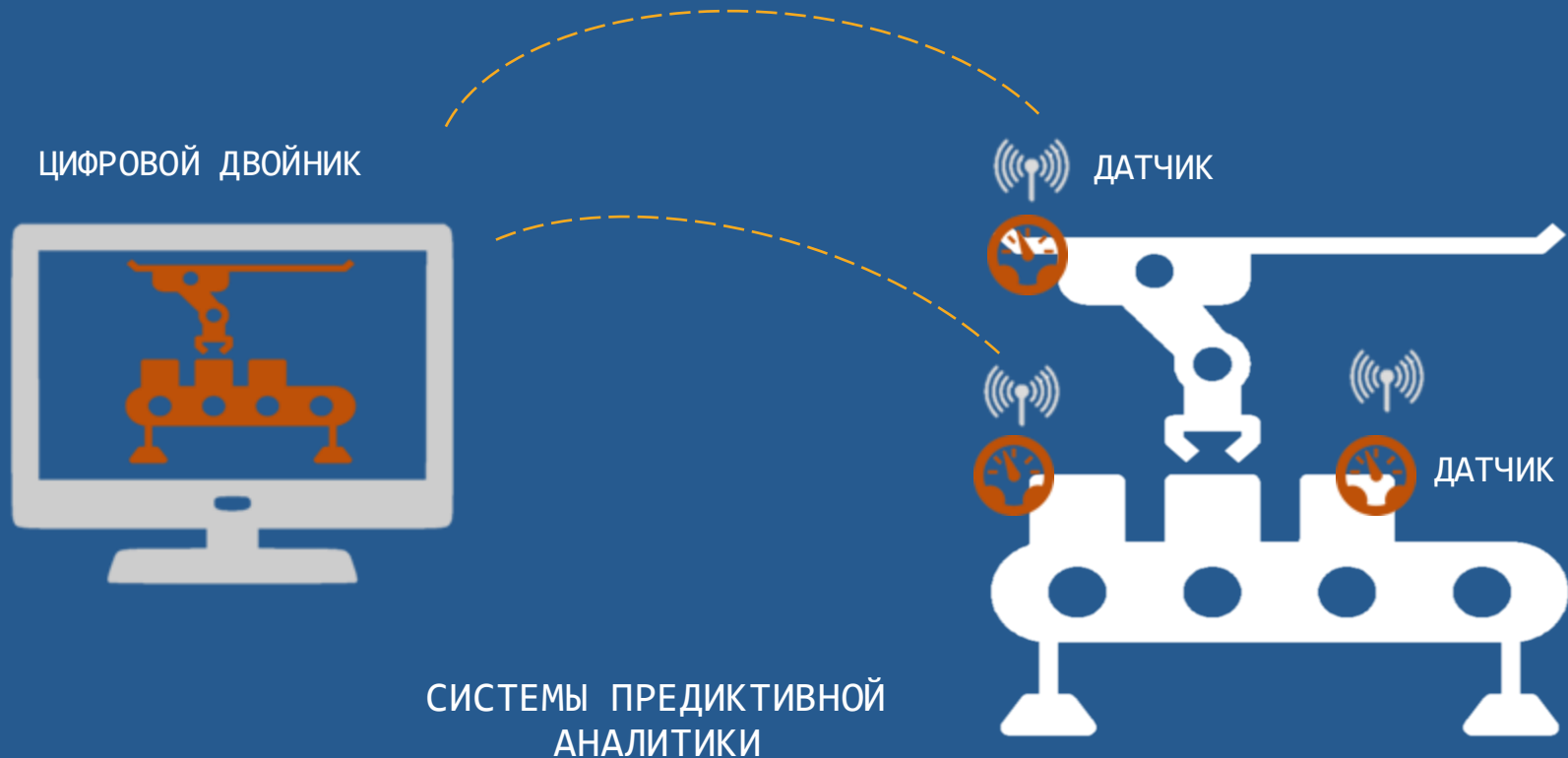
ПЛК



Дистанционное управление

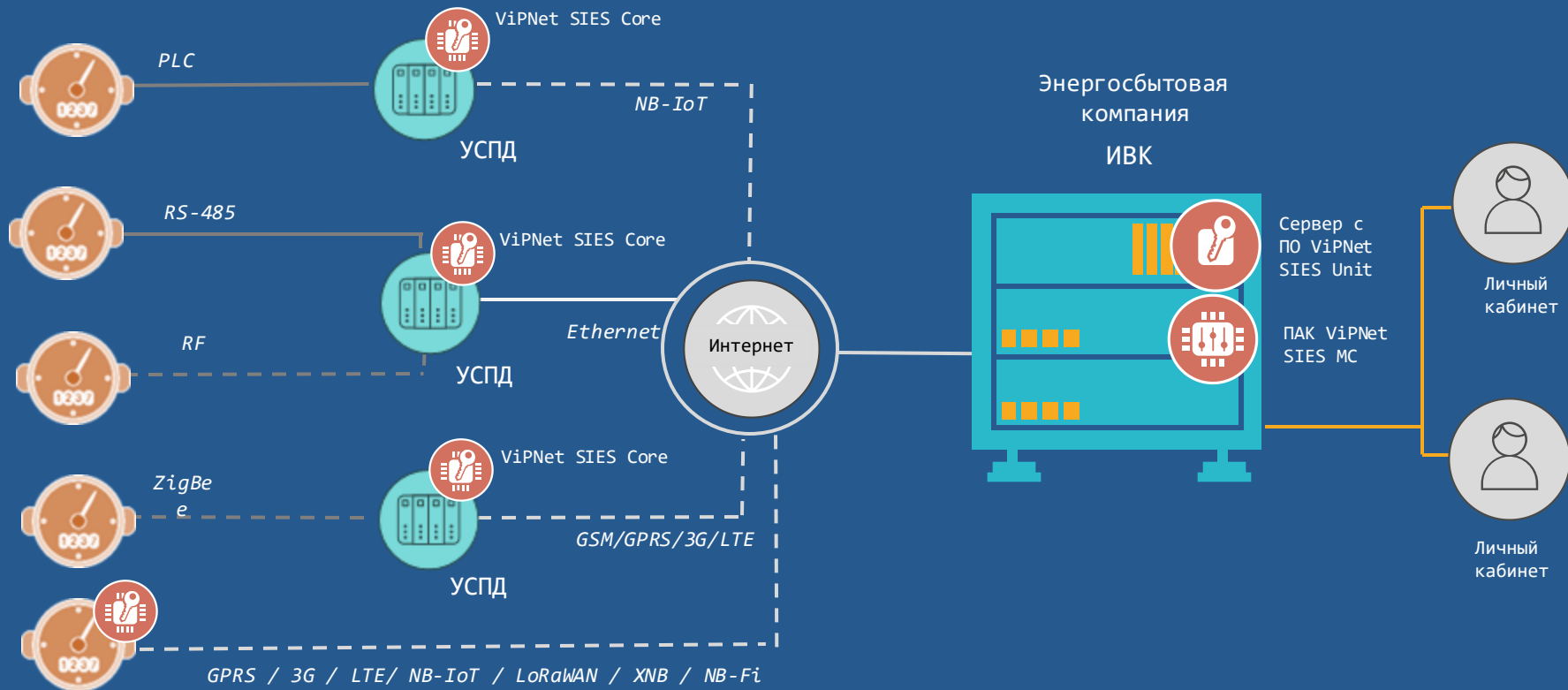


Защита систем сбора информации для предиктивной аналитики



Защита интеллектуальных систем учета электроэнергии

ПРИБОРЫ УЧЕТА (ПУ)





VIPNet VPN



Симметричная
криптография:
Честный P2P
VPN

Не сессионный
VPN:
Работа на плохих
и нестабильных
каналах

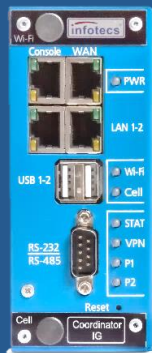
Работа через
NAT:
Соединение
устройств
за различными
NAT

Централизованное
управление:
Ключи
шифрования,
справочники,
политики
безопасности

Индустриальный шлюз ViPNet Coordinator IG



ViPNet
Coordinator
IG10 I1



ViPNet
Coordinator
IG100 I1



ViPNet
Coordinator
IG10 I2



ViPNet
Coordinator
IG100 I4



ViPNet
Coordinator
IG10 I3



ViPNet
Coordinator
IG100 I5

Сертифицированные
исполнения

Новое исполнение

Ближайшие планы

Линейка шлюзов безопасности ViPNet Coordinator IG 4

VPN-шлюз уровня
L3, L2

По требованиям к
СКЗИ класса КСЗ

4 уровень доверия
по требованиям
ФСТЭК России

Импортозамещение
Произведено в России



Межсетевой экран

Типа «А» 4 класса
Типа «Д» 4 класса по
требованиям ФСТЭК России

4 класс защищенности по
требованиям ФСБ России

Промышленный
маршрутизатор,
беспроводной роутер

Проводные,
3G/LTE, Wi-fi,
RS-232/485 интерфейсы



Защита объектов

Приказ ФСТЭК №239

Защита объектов КИИ для всех категорий значимости включительно (АСУ, ИС, ИТС)

Приказ ФСТЭК №31

Защита объектов АСУ ТП до класса защищенности К1 включительно

Приказ ФСТЭК №17

Защита ГИС до класса К1 включительно

Приказ ФСТЭК №21

Защита ИСПДн до 1 уровня защищенности

Приказ ФСТЭК №489

Защита ИС общего пользования II класса

Сценарии эксплуатации

- защита периметра сети
- сегментирование сети и разграничение доступа к ее сегментам
- защита проводных и беспроводных каналов связи сети
- организация ДМЗ
- управление сетевыми потоками
- сокрытие реальных адресов и архитектуры сети
- организация удаленного доступа для стационарных и мобильных пользователей, в том числе с мобильных устройств



Защита систем с подключением к сетям общего пользования



Управление в АСУ/
Контроль выполнения
тех. процесса/
взаимодействие между
сегментами ОКИИ



Контроль за
производственным
оборудованием

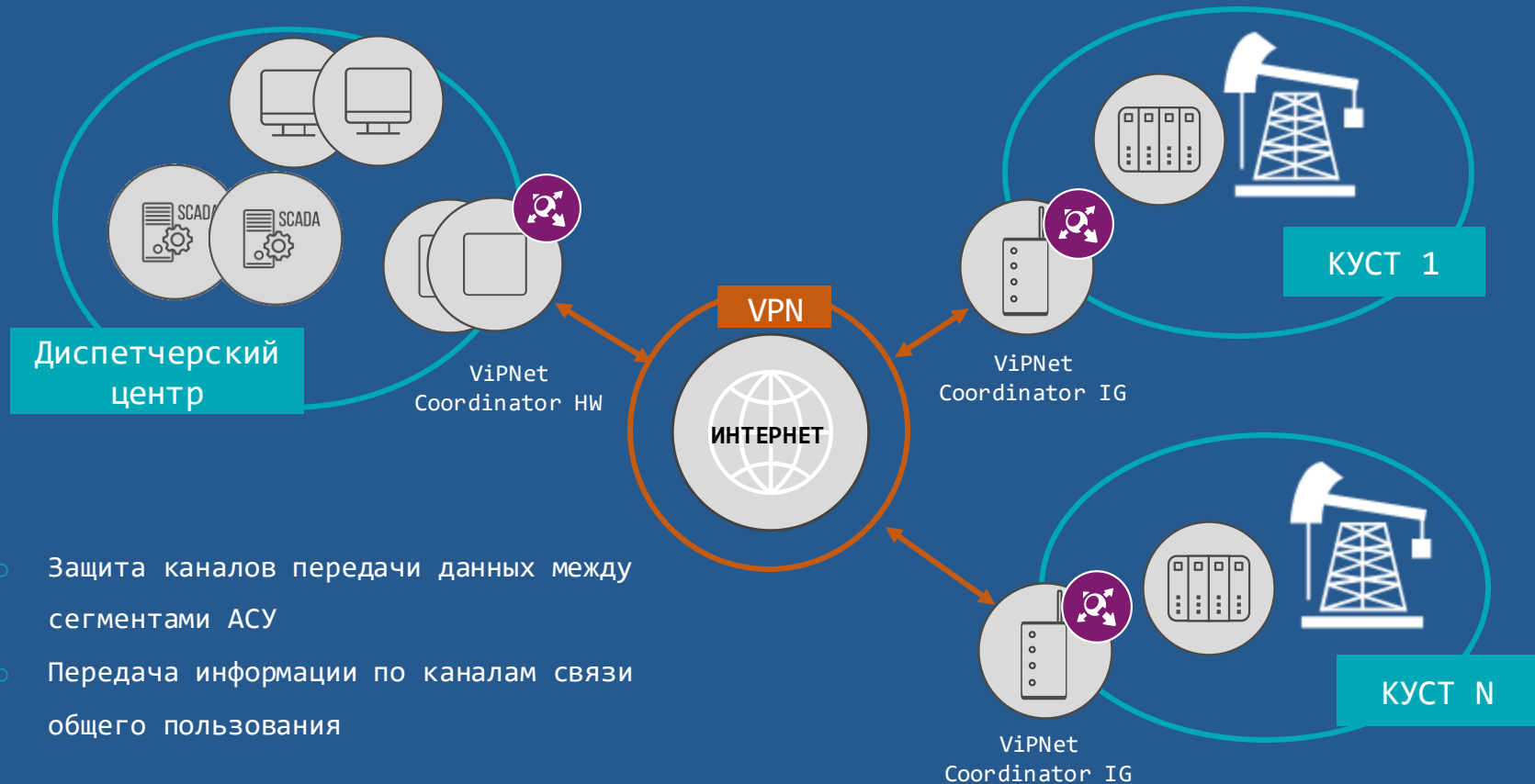


Взаимодействие с
иными
системами/межсетевое
взаимодействие



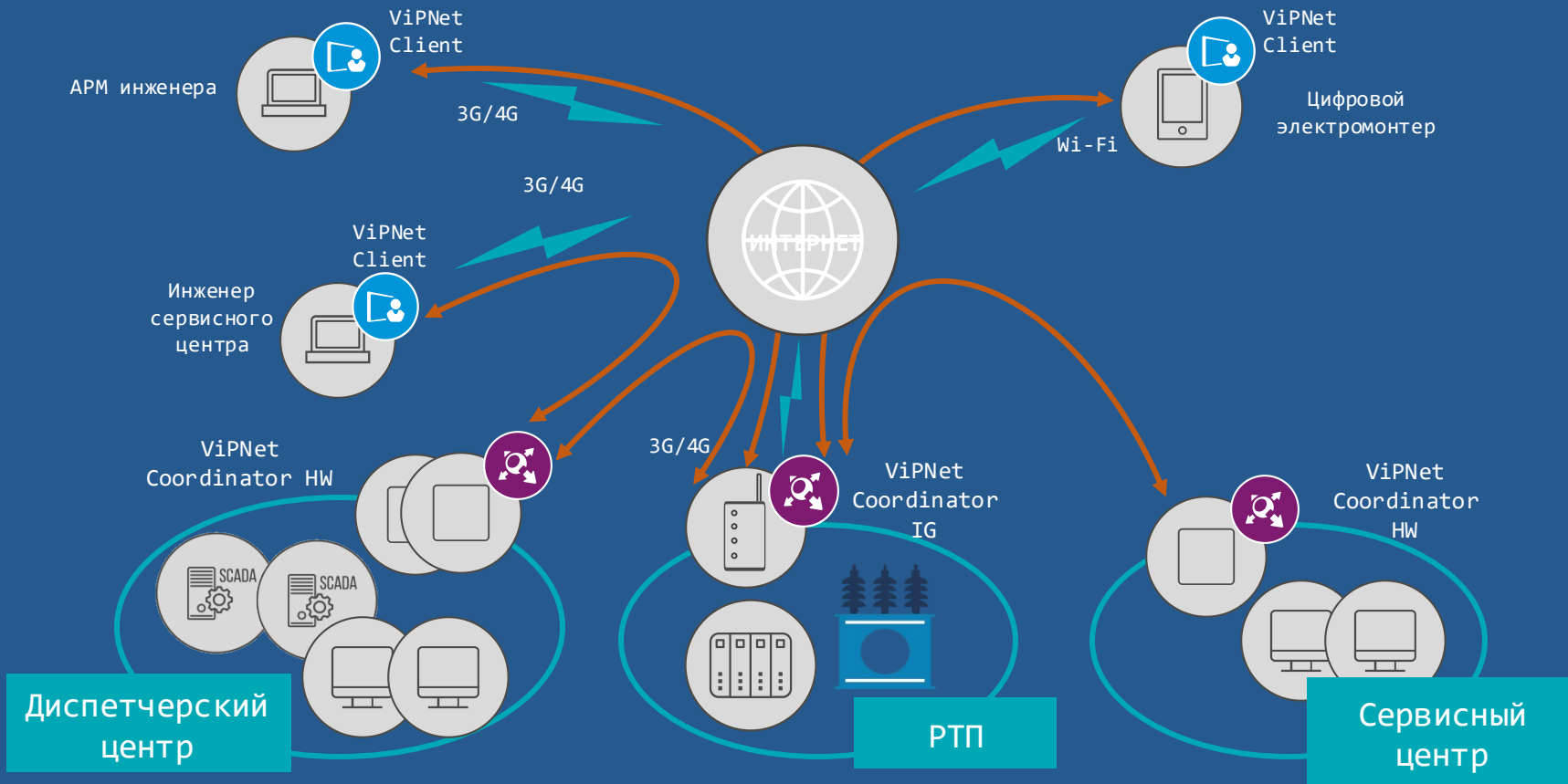
Оказание услуг

Защита каналов связи



- Защита каналов передачи данных между сегментами АСУ
- Передача информации по каналам связи общего пользования

Защищенный удаленный доступ



Сертификаты соответствия



По линии ФСБ России:

- Сертификат по требованиям к СКЗИ класса КСЗ;
- Сертификат по требованиям к МЭ 4 класса защищенности;



По линии ФСТЭК России:

- по требованиям к МЭ;
- профилю защиты МЭ типа Д 4 класса (ИТ.МЭ.Д4.ПЗ);
- профилю защиты МЭ типа А 4 класса (ИТ.МЭ.А4.ПЗ);
- 4 уровню доверия по требованиям безопасности информации (2020 г.).

Сертификация по требованиям Минкомсвязи России



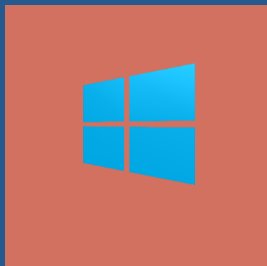
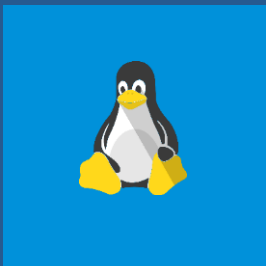
- Исполнения ПАК ViPNet Coordinator IG имеют сертификаты соответствия для применения на сетях связи общего пользования и технологических сетях связи как оборудование маршрутизации и коммутации пакетов, и как базовая станция для беспроводной передачи данных стандарта 802.11 b/g частотой 2,4 ГГц;
- Исполнения ПАК ViPNet Coordinator IG имеют декларации соответствия по требованиям:
 - к абонентским станциям стандарта GSM-900/1800, UMTS, LTE, LTE-Advanced;
 - к оборудованию проводных и оптических систем передачи абонентского доступа.



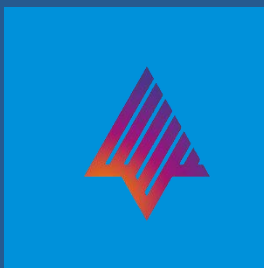
Программный клиент
ViPNet Client

ViPNet Client: среда функционирования

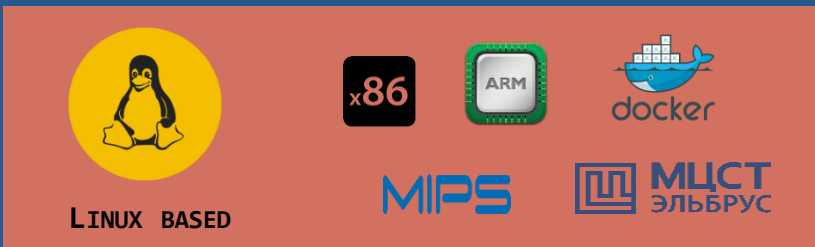
КОМПЬЮТЕРЫ
НОУТБУКИ
СЕРВЕРА



ТЕЛЕФОНЫ
ПЛАНШЕТЫ



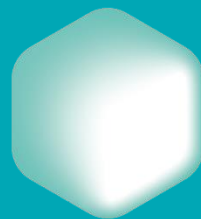
ТЕРМИНАЛЫ, ПЛК,
ИОТ-УСТРОЙСТВА



- Прозрачен для приложений пользователя и сервисов ОС
- Независим от физических каналов связи
- Подключается к неограниченному количеству сегментов сети
- Поддерживает ОС Windows, Linux, MacOS, Android, iOS, Aurora
- Работает на x86, ARMv5, ARMv7, ARMv8, MIPS, Эльбрус и в Docker
- Имеет сертификаты ФСБ России на СКЗИ по классам от КС1 до КС3

VIPNet Client for KasperskyOS

- Защита каналов внутри сетей VIPNet VPN
- Работа в фоновом режиме
- Стабильная работа на каналах связи любого качества
- Автоматическое восстановление защищенного соединения при временных разрывах
- Прозрачная защита канала для сторонних приложений на устройстве



KasperskyOS
Be Immune

15:13

100%

15 : 13

Четверг, 5 августа



Контакты



Сообщения



Калькулятор



Настройки



Телефон



Почта



Интернет



Календарь



VIPNet Client



Документы



VipNet Client — защита каналов связи рабочих станций и конечных устройств

SCADA LEVEL



APM Оператора
VipNet Client for Windows
VipNet Client for Linux



HMI
VipNet Client for Windows
VipNet Client for Linux



Мобильный APM
VipNet Client for Android
VipNet Client for iOS

AUTOMATION LEVEL

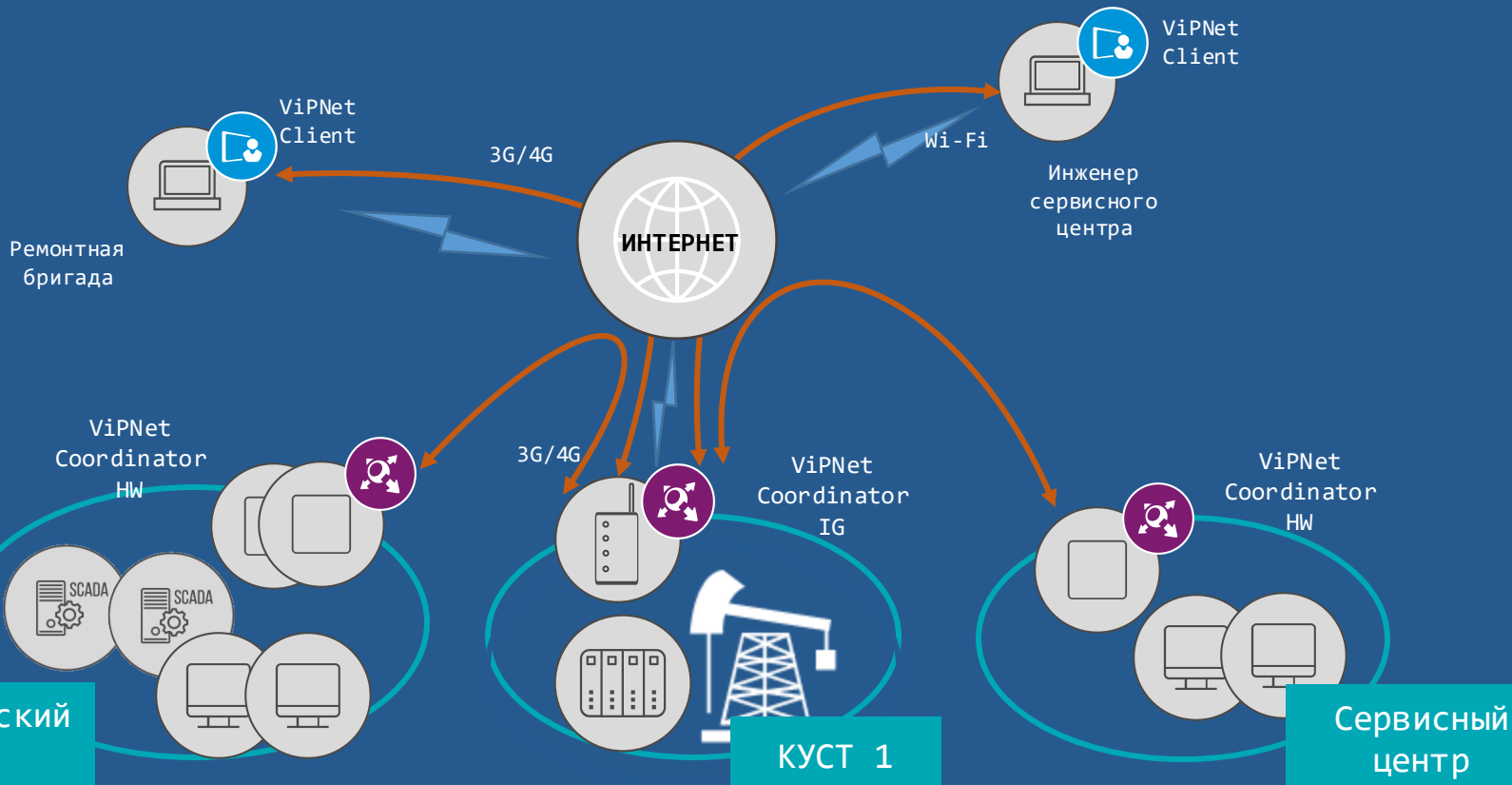


APM инженера
VipNet Client for Windows
VipNet Client for Linux



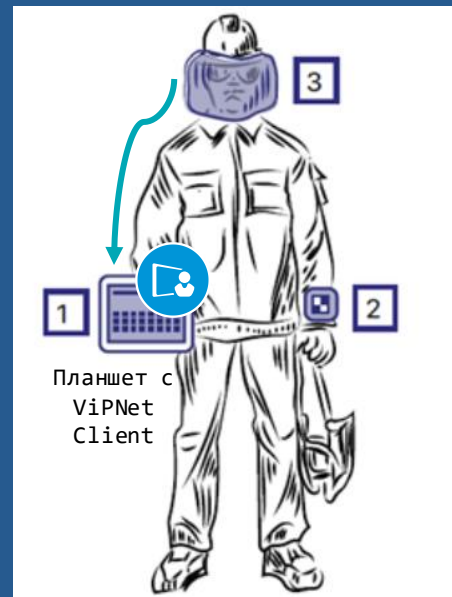
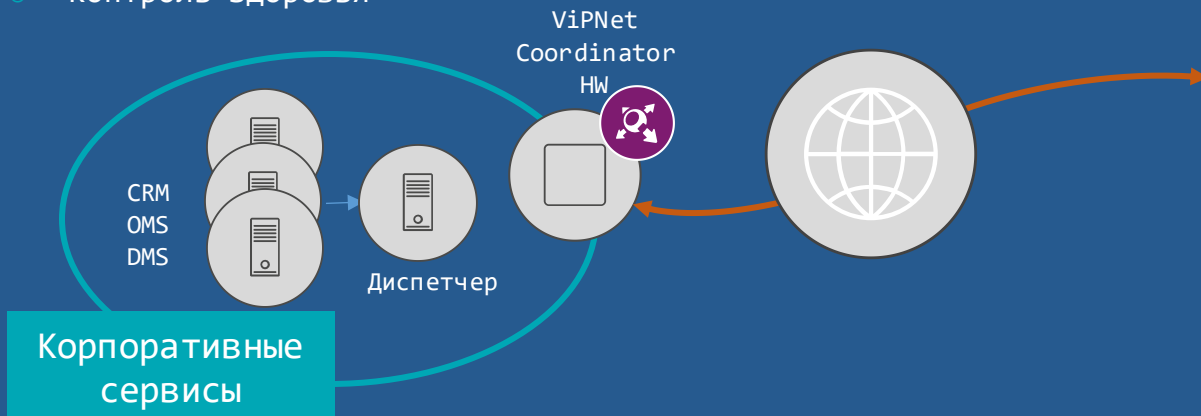
Контроллер
Встраиваемый
VipNet Client 4U

Защищенный удаленный доступ для АРМ



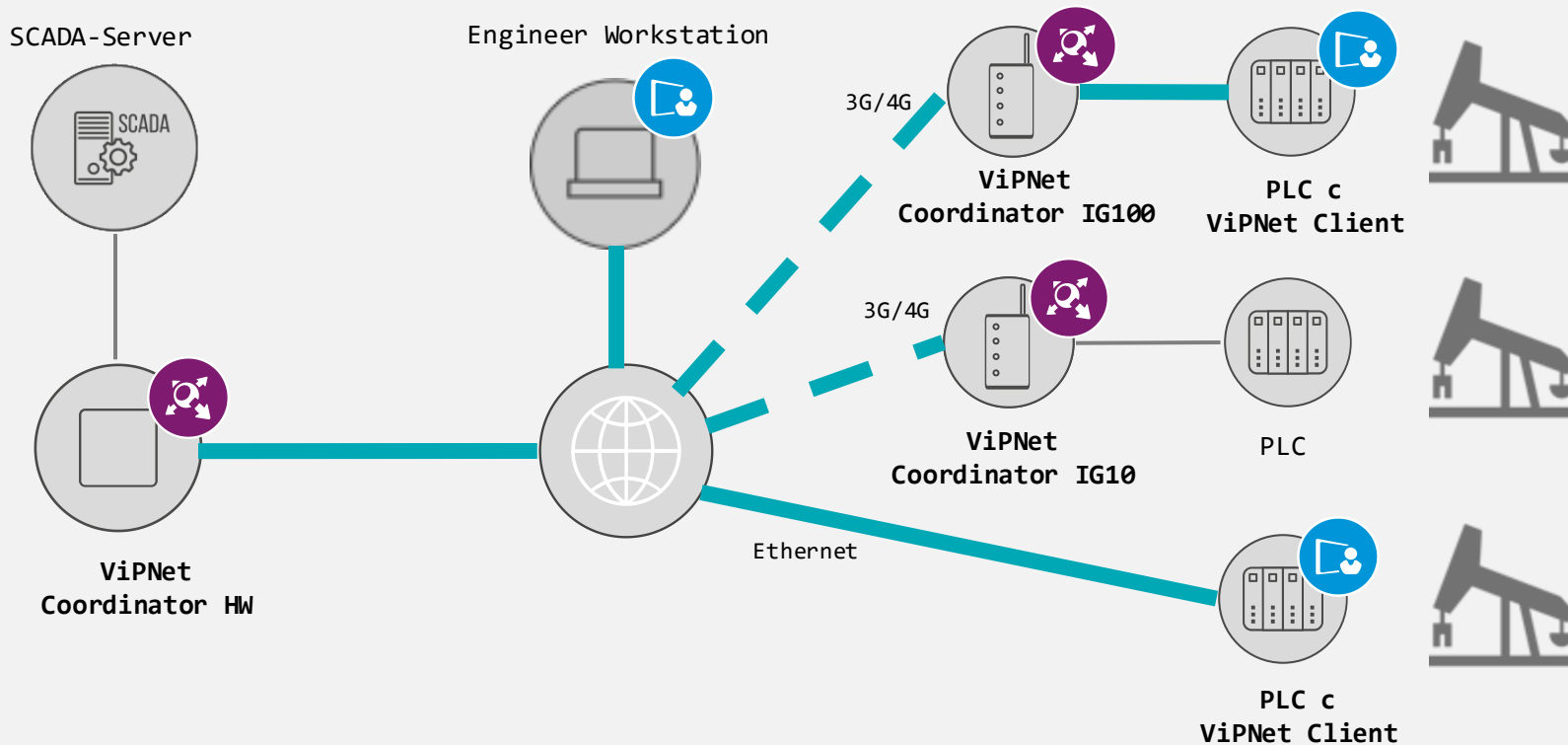
Защита мобильных устройств в АСУ

- ТОиР
- Доступ к ресурсам с документацией
- Контроль выполнения работ
- Учет обхода маршрута
- Контроль здоровья



Мобильный обходчик,
Цифровой монтер

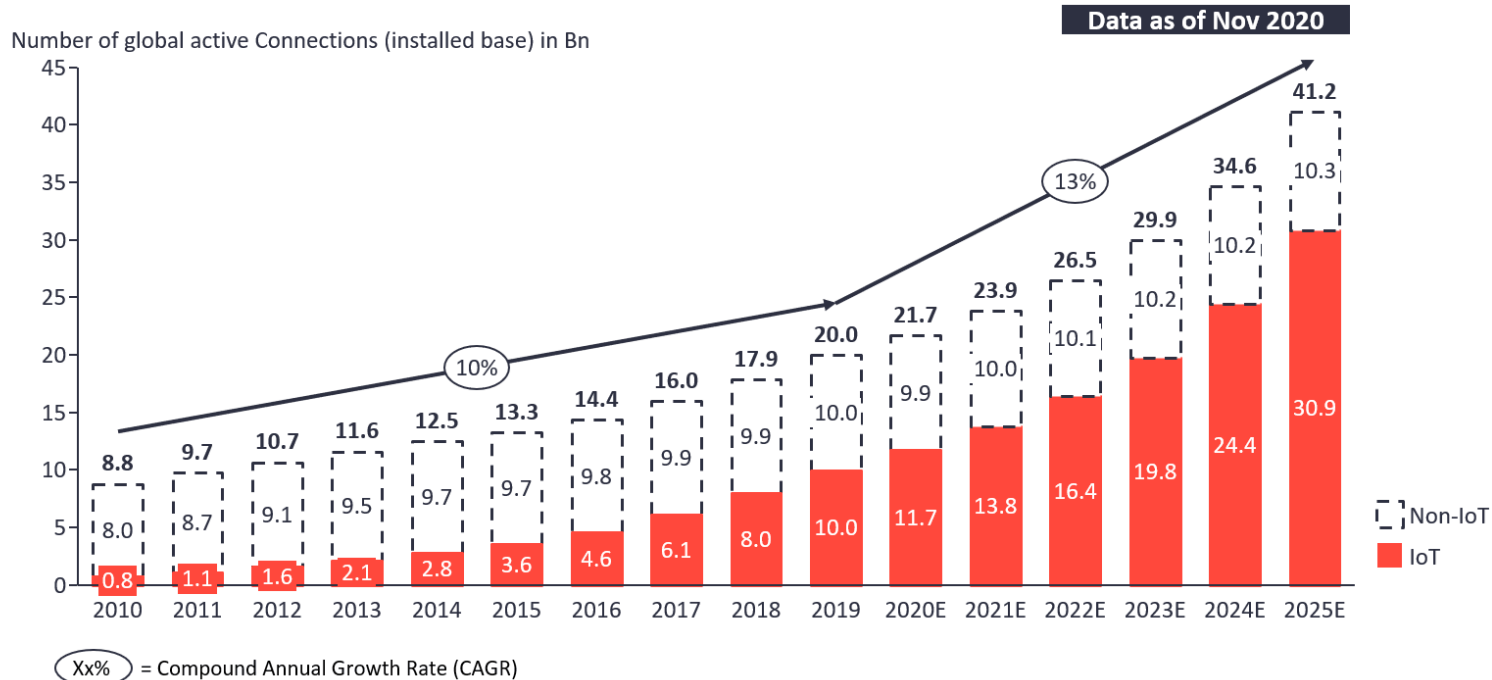
Защита каналов связи контроллеров



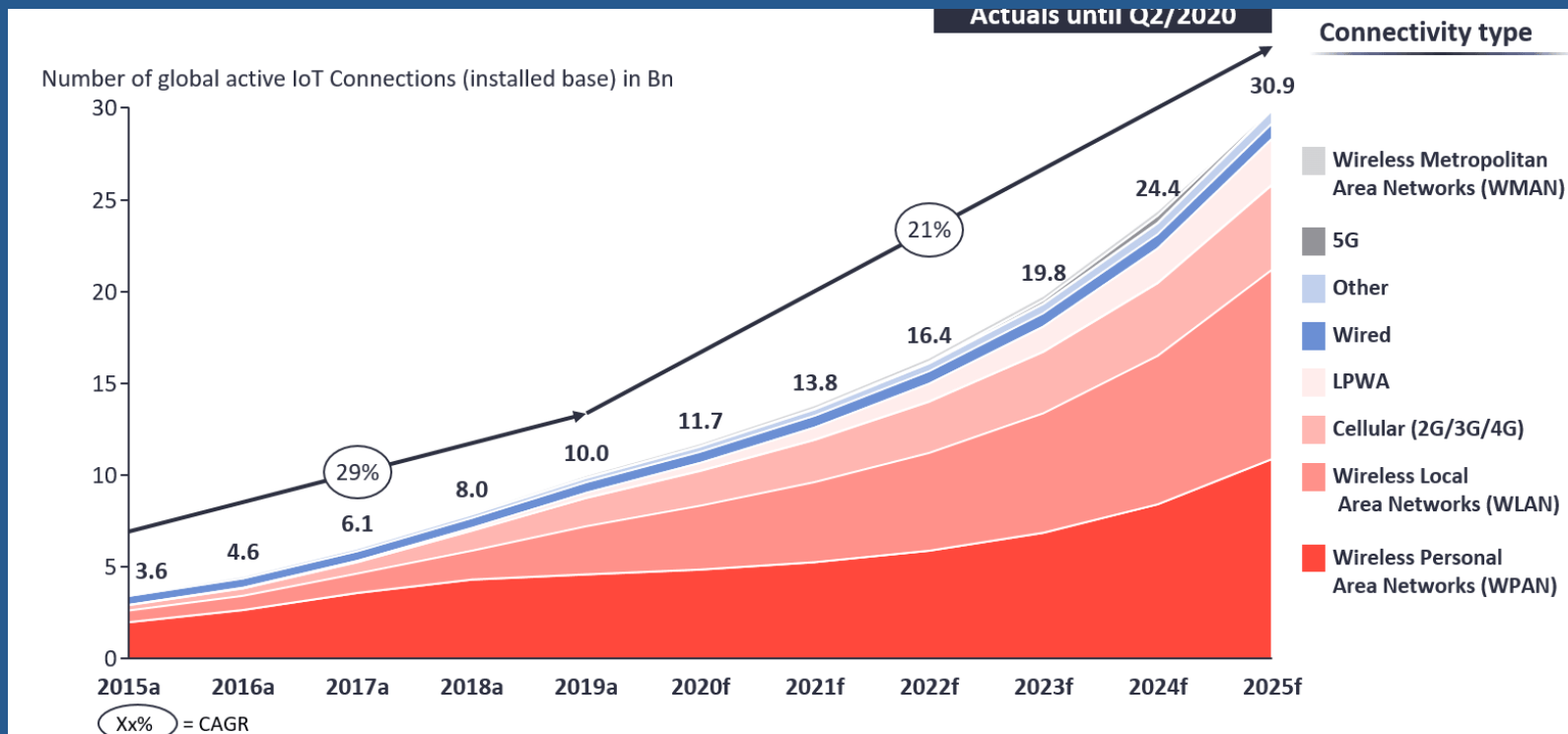


Встраиваемые средства защиты информации ViPNet SIES

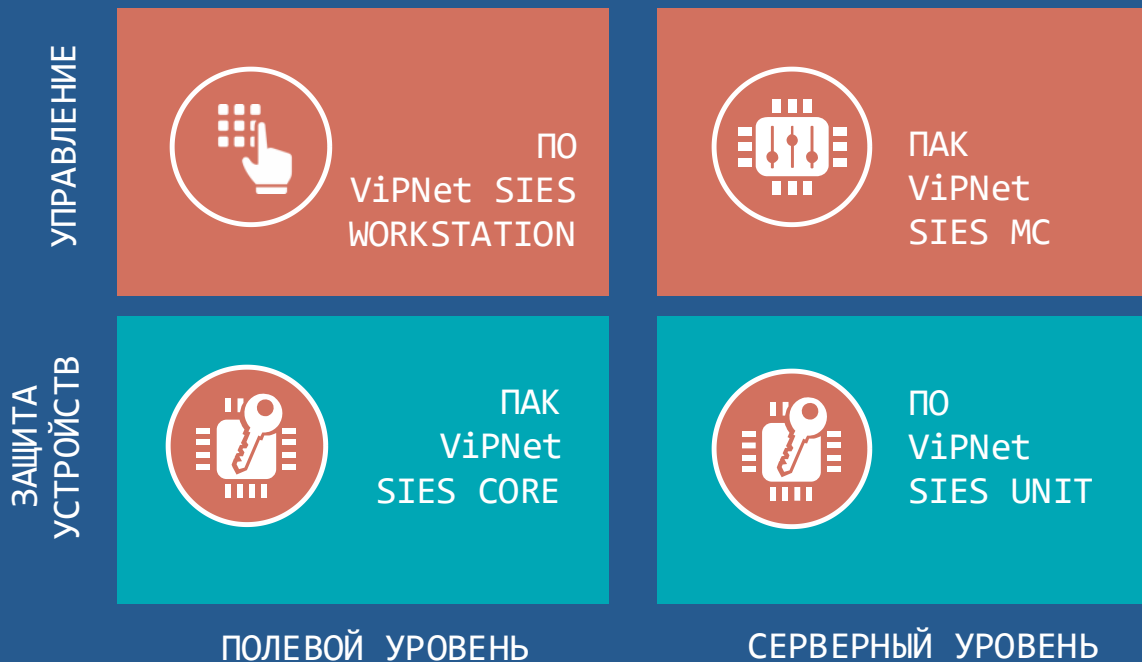
Количество подключенных устройств (включая non-IP)



Количество подключенных устройств (включая non-IP)



Состав решения ViPNet SIES



- СКЗИ класса КС1 и КС3 по требованиям ФСБ России
- Возможность использования криптографии на разных по вычислительной мощности устройствах
- Нет зависимости от ОС и архитектуры устройств
- Поддержка разных моделей взаимодействия: точка-точка, мультивещательные связи, подписочная модель
- Поддержка сценариев резервирования

Концепция **Security by Design**

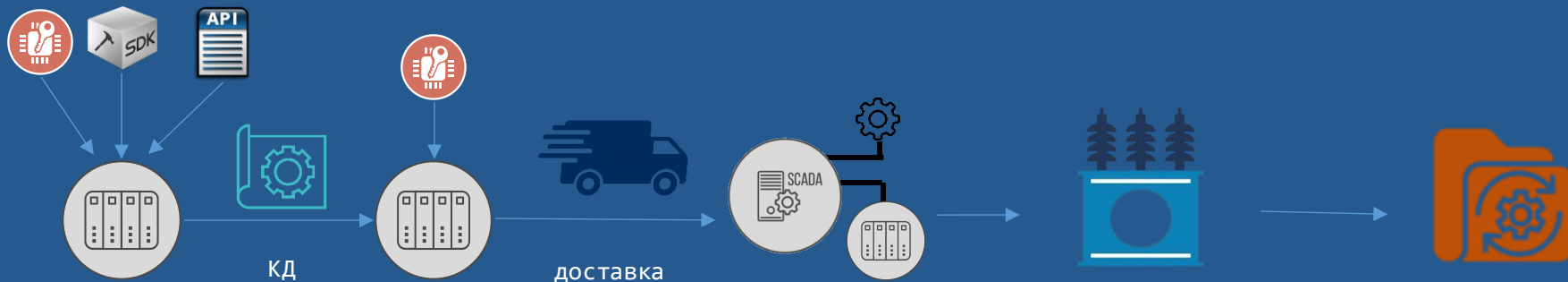
РАЗРАБОТКА
УСТРОЙСТВА

ПРОИЗВОДСТВО
УСТРОЙСТВА

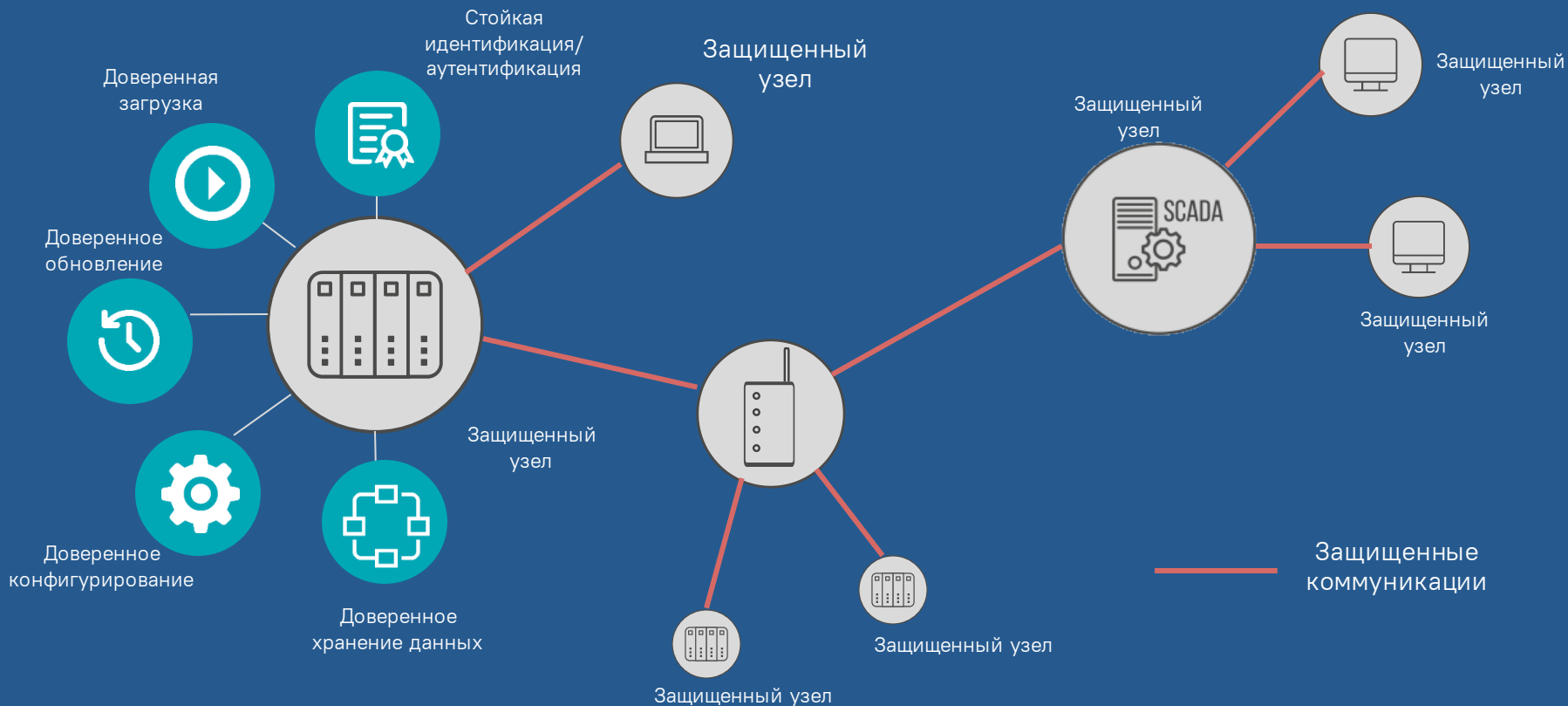
ВВОД В
ЭКСПЛУАТАЦИЮ
УСТРОЙСТВА

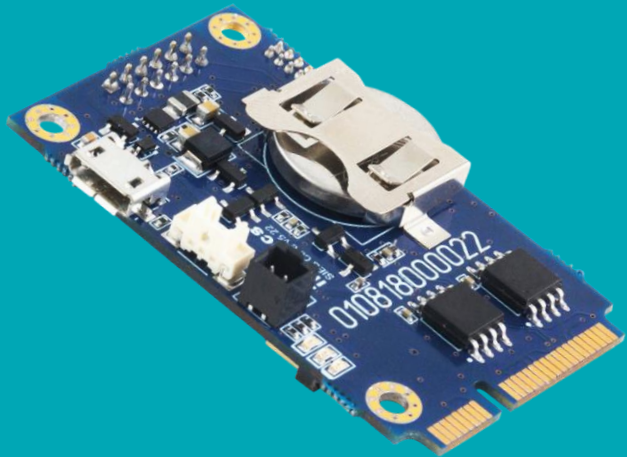
ЭКСПЛУАТАЦИЯ
УСТРОЙСТВА

УПРАВЛЕНИЕ
ОБНОВЛЕНИЕМ И
КОНФИГУРАЦИЕЙ
УСТРОЙСТВА



Концепция защиты конечных устройств





для ИНТЕГРАЦИИ в ПЛК/ ИОТ-шлюзы/УСПД

- Интеграция на аппаратном уровне – USB, UART, SPI
- Интеграция на программном уровне – SIES Core API (RATP+прикладной протокол)
- Возможность использования вне контролируемой зоны при подключении ДНСД
- Наличие SDK под Linux (ARM, x86), Windows, RTOS
- Сертификат СКЗИ класса КСЗ по требованиям ФСБ России

ПАК ViPNet SIES Core

ПО ViPNet SIES Unit

ДЛЯ ИНТЕГРАЦИИ В ИВК И
АРМ КОНФИГУРАТОР



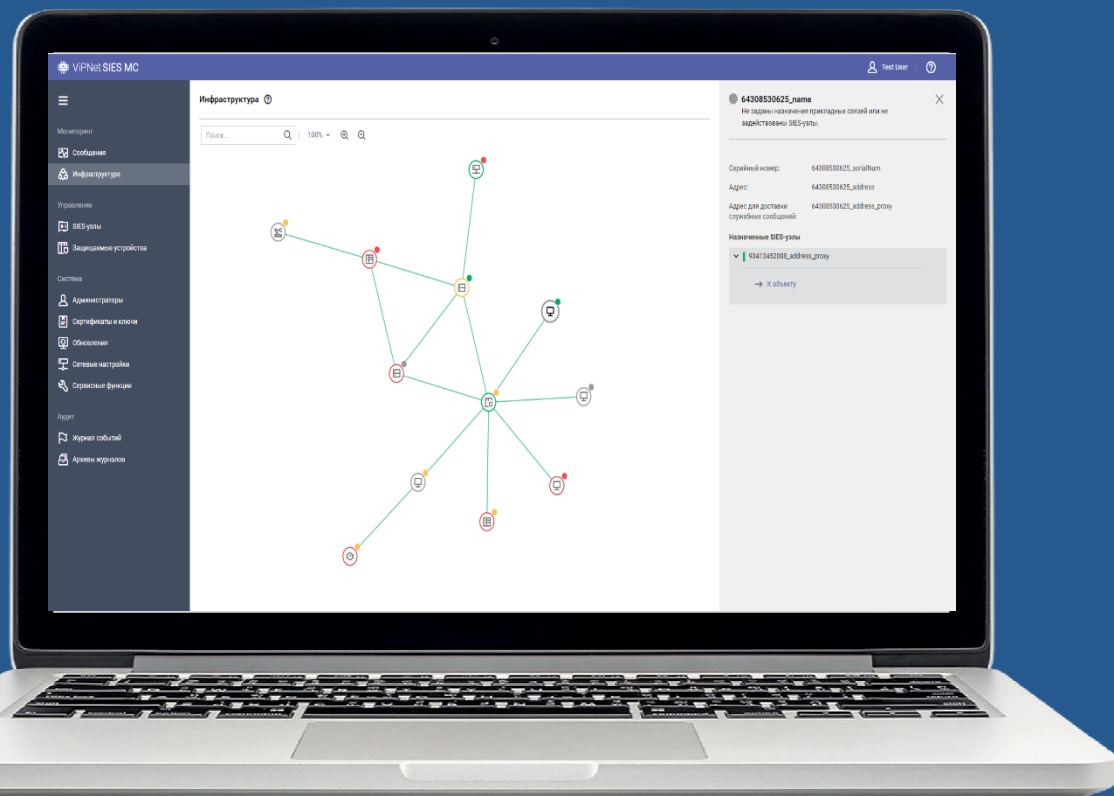
- Интеграция по RESTAPI;
- Поддерживаемые ОС:
 - Windows 7/8/8.1/10 (x86/64)*
 - Windows Server 2008/R2/2012/2012 R2/ 2016 *
 - Debian 9, Ubuntu 16, Ubuntu 18 и др ОС Linux ** (gcc v.6 и выше, systemd система инициализации, x86/64 или ARM, менеджер пакетов deb/rpm формата)
 - Astra Linux Special Edition (Смоленск) 1.6 (x86/64)**
- Возможность установки на выделенный сервер;
- Исполнения с поддержкой различного количества связей: 50, 500, 2000, 10 000 связей;
- Масштабируемость и расширяемость.

*Сертификат СКЗИ класса КС1 и КС3 по требованиям ФСБ России

** Сертификат СКЗИ класса КС1 и КС3 ожидается в 2021г.

ПАК ViPNet SIES MC

3С infotecs



Ключевой и Удостоверяющий центры



Управление связями в системе



Дистанционная смена ключевой информации



Управление активами



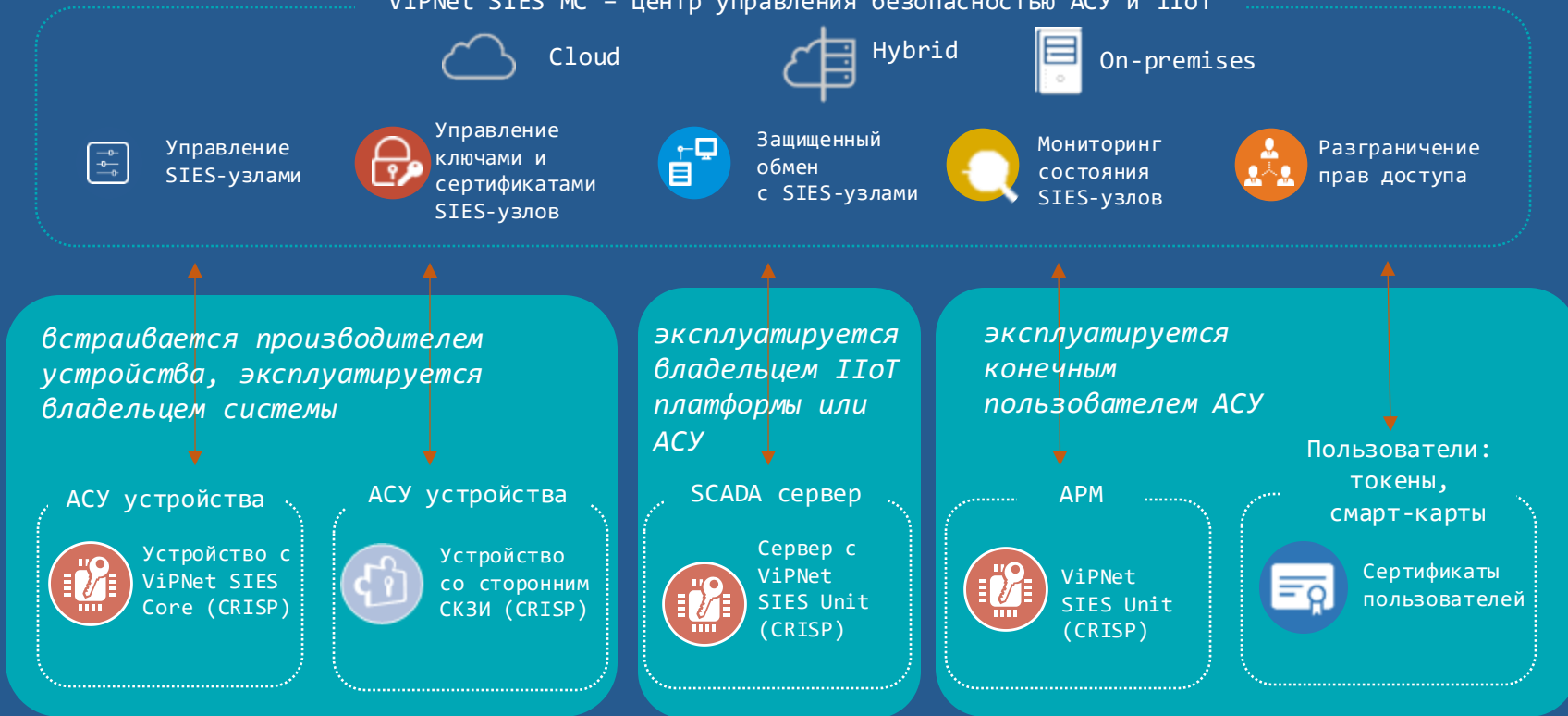
Доступ к интерфейсу по WebUI



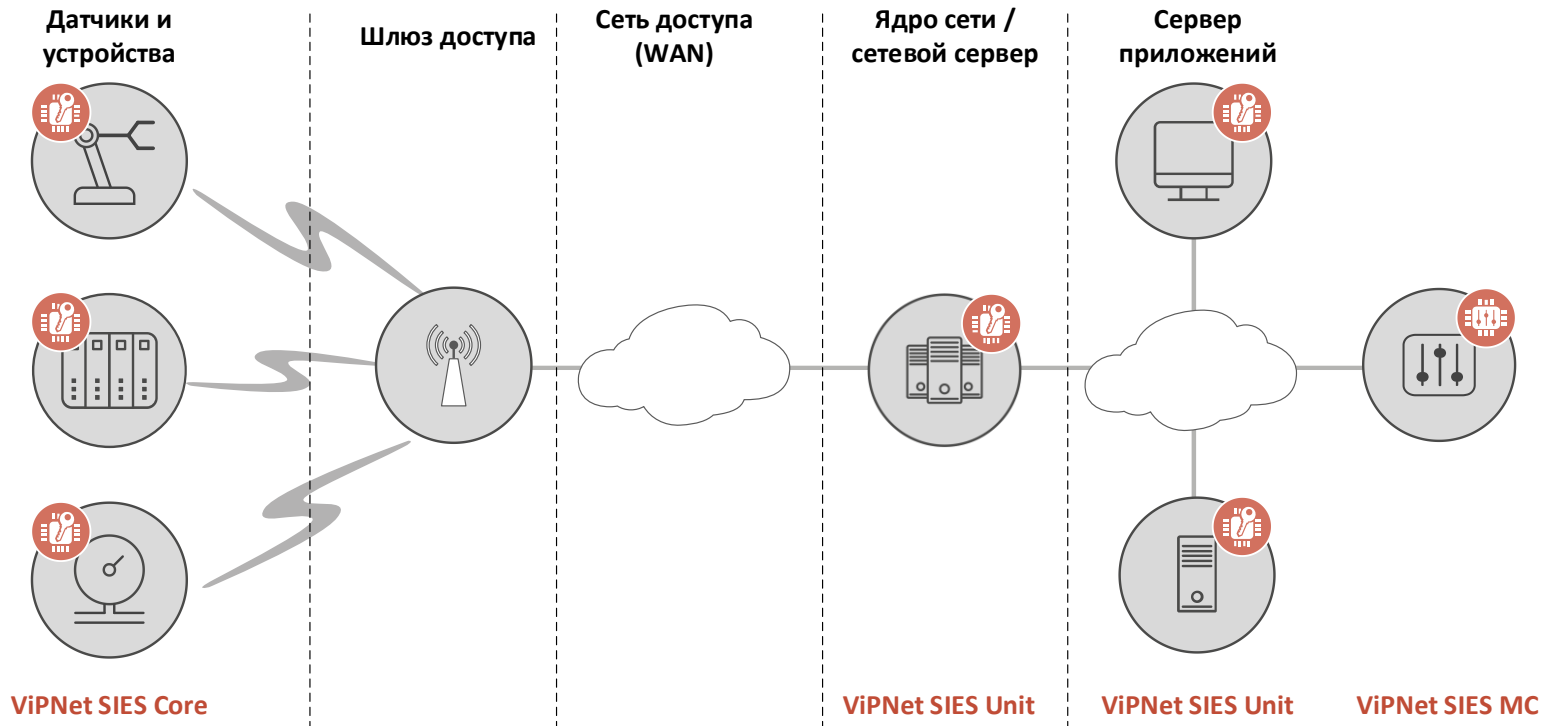
Сертификат по требованиям ФСБ России к СКЗИ класса КСЗ

ИБ платформа на основе ViPNet SIES для АСУ и IIoT

ViPNet SIES MC – центр управления безопасностью АСУ и IIoT



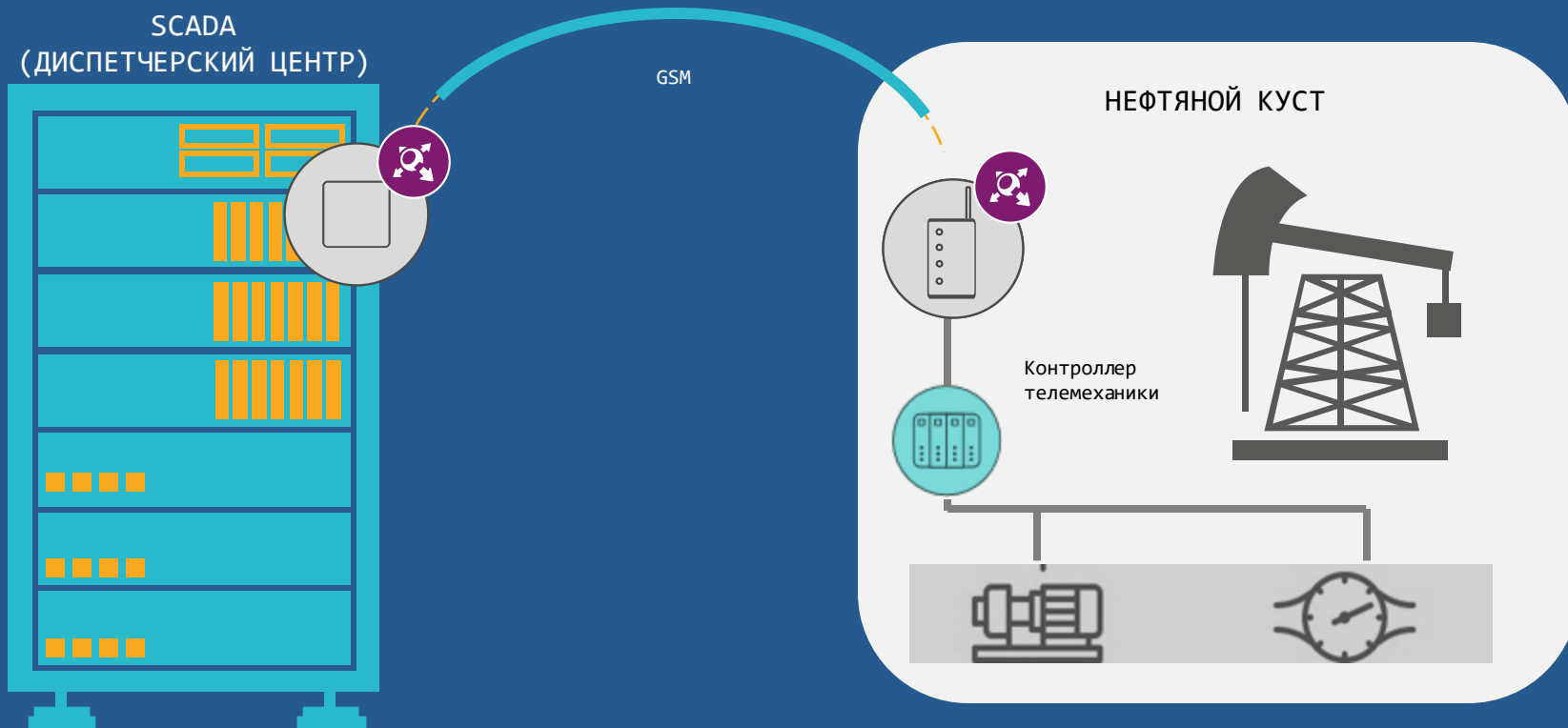
Защищенная IIoT-система



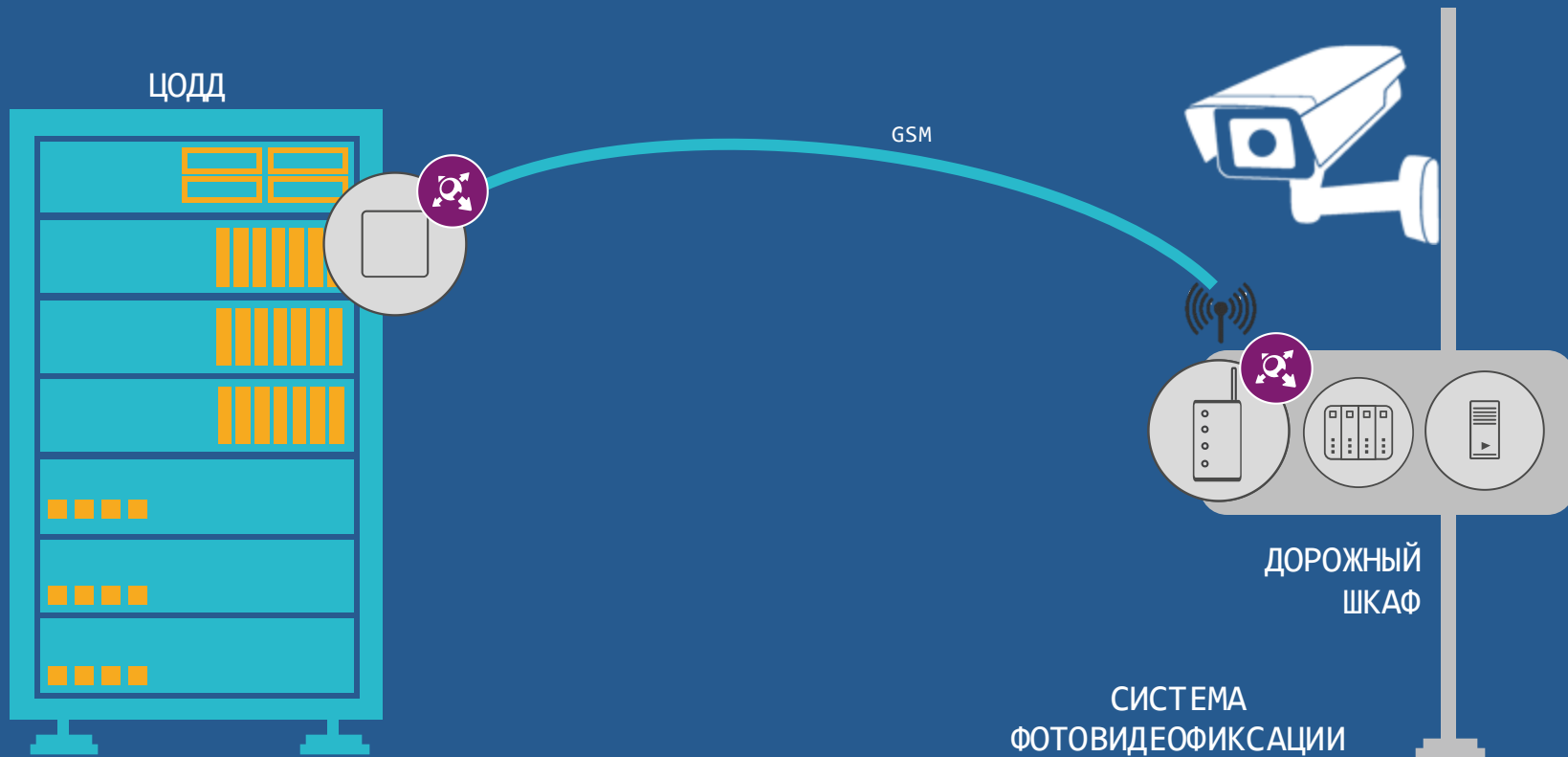


Защищенные АСУ

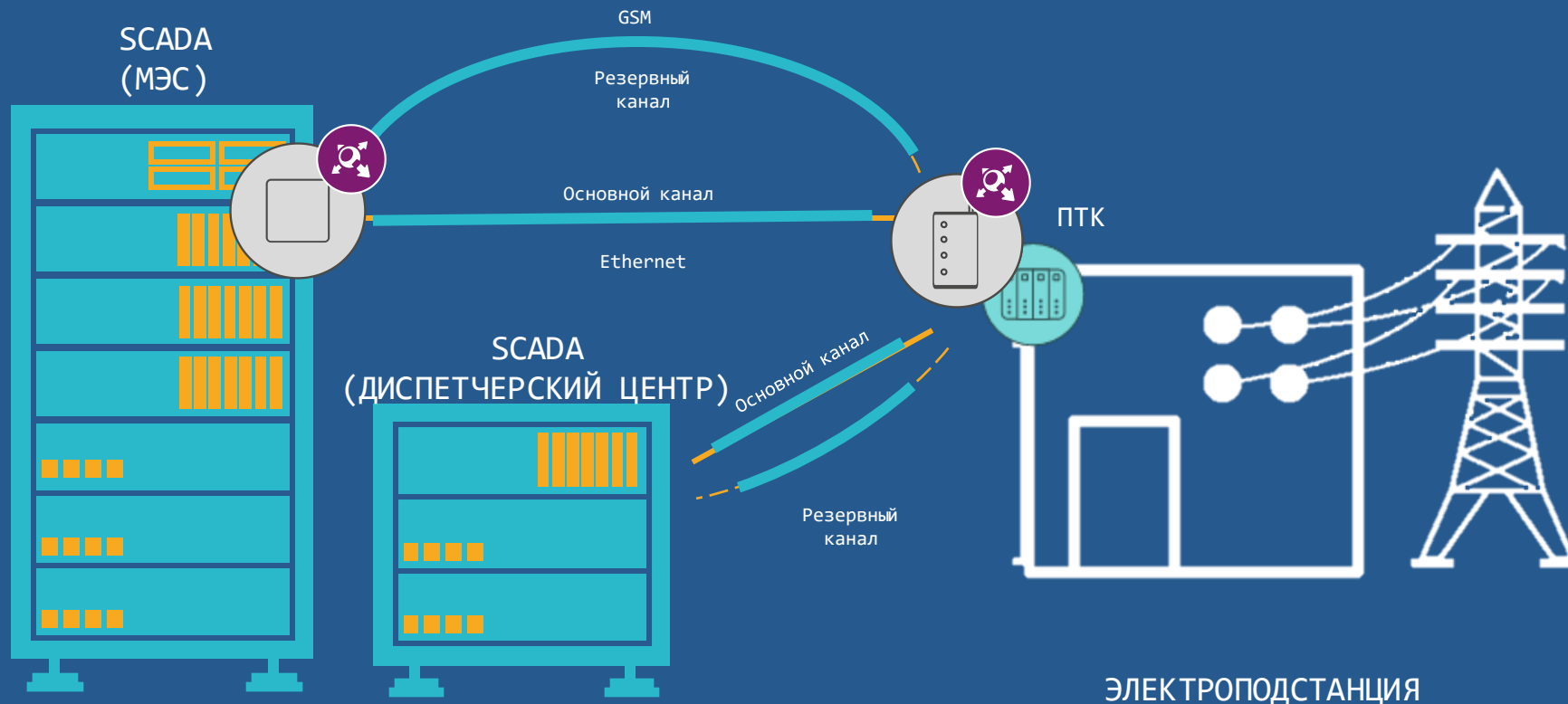
Защита каналов АСУ ТП



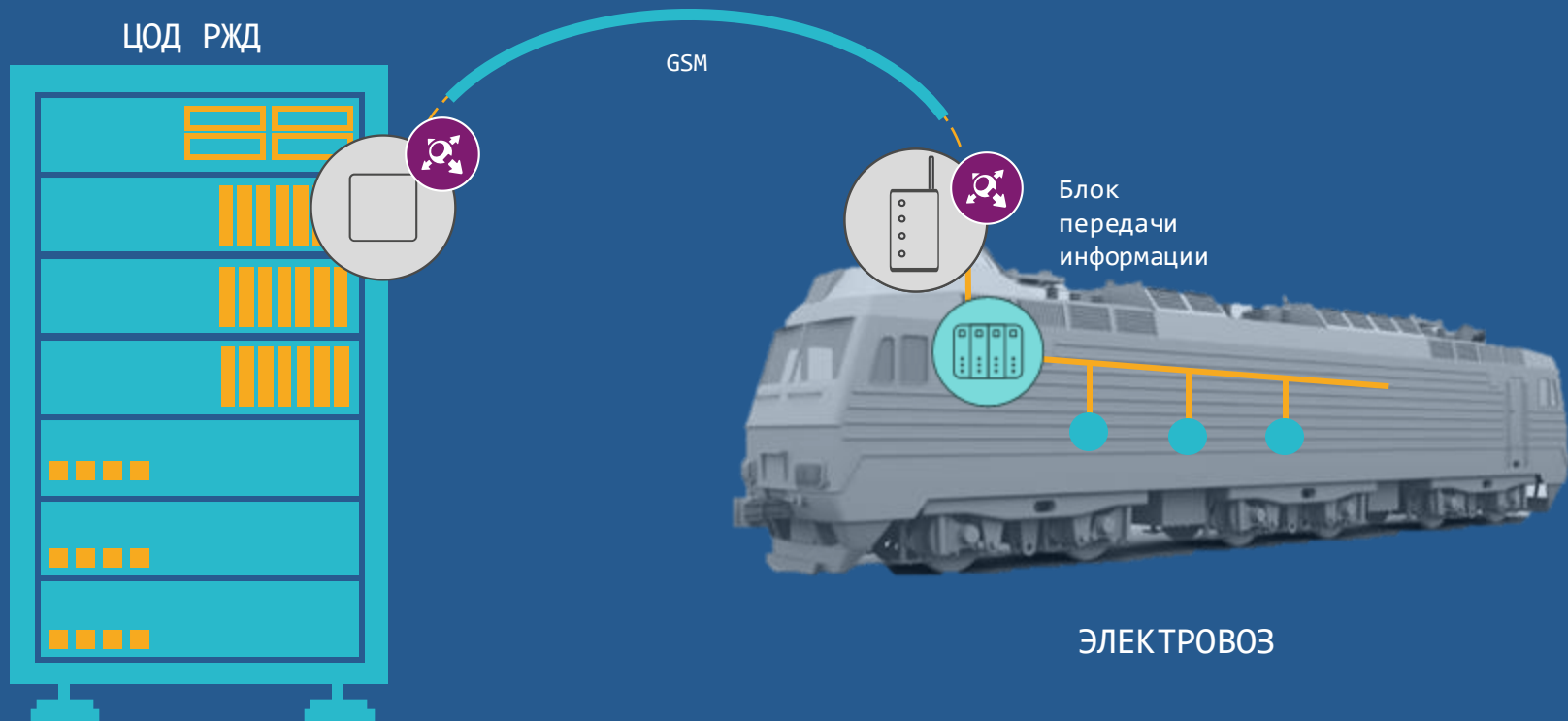
Защита каналов АСУ



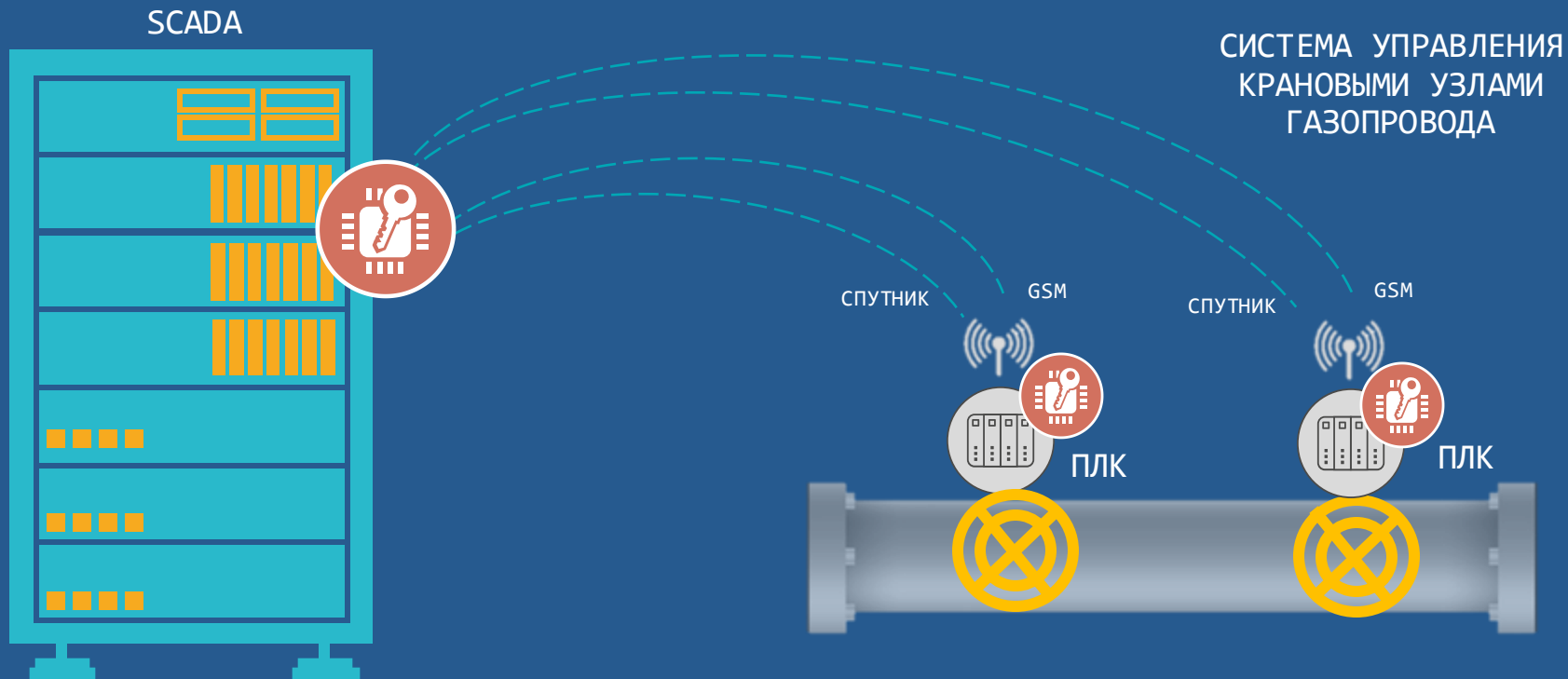
Защита резервируемых каналов АСУ



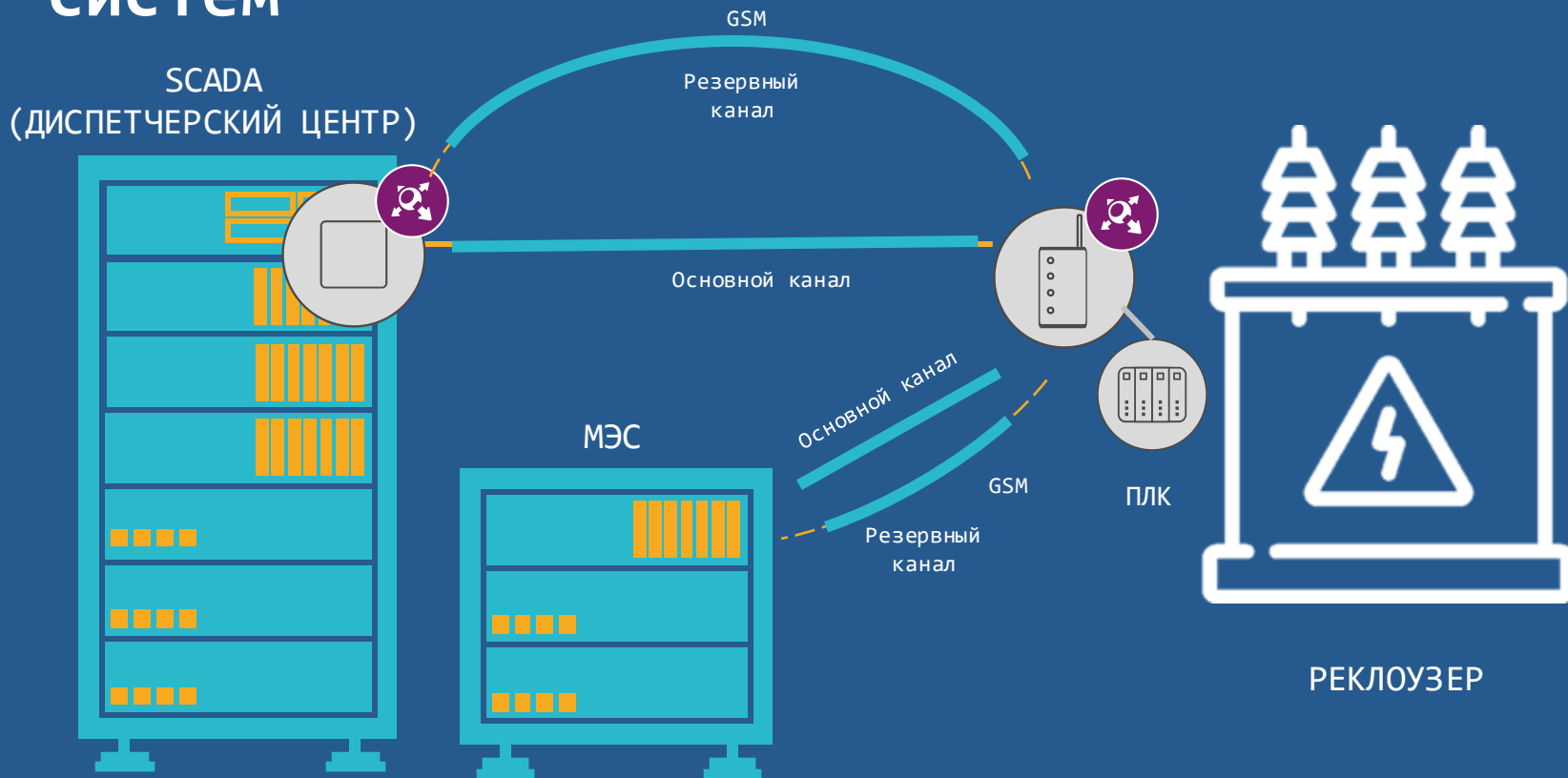
Обеспечение целостности и неизменяемости при передаче данных



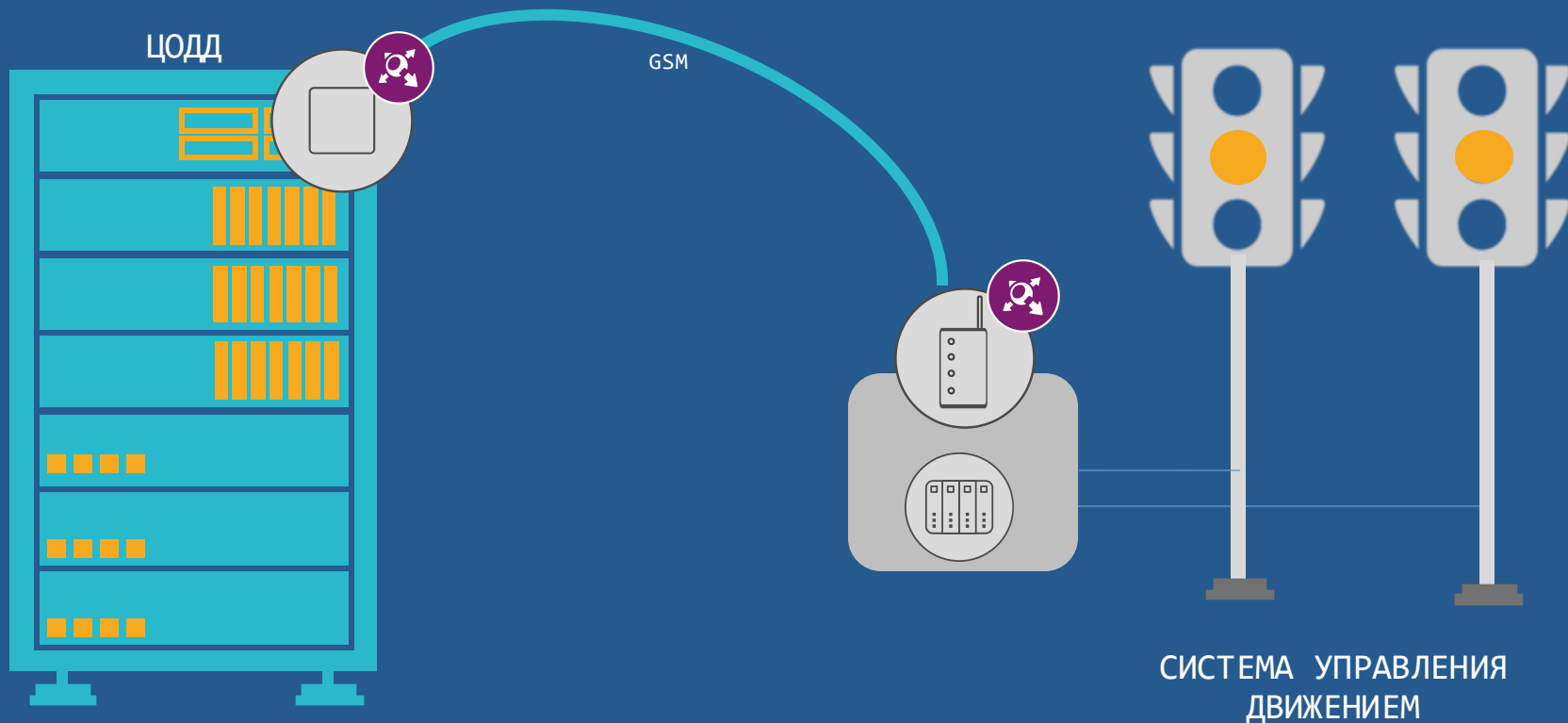
Защита спутниковых каналов в АСУ ТП



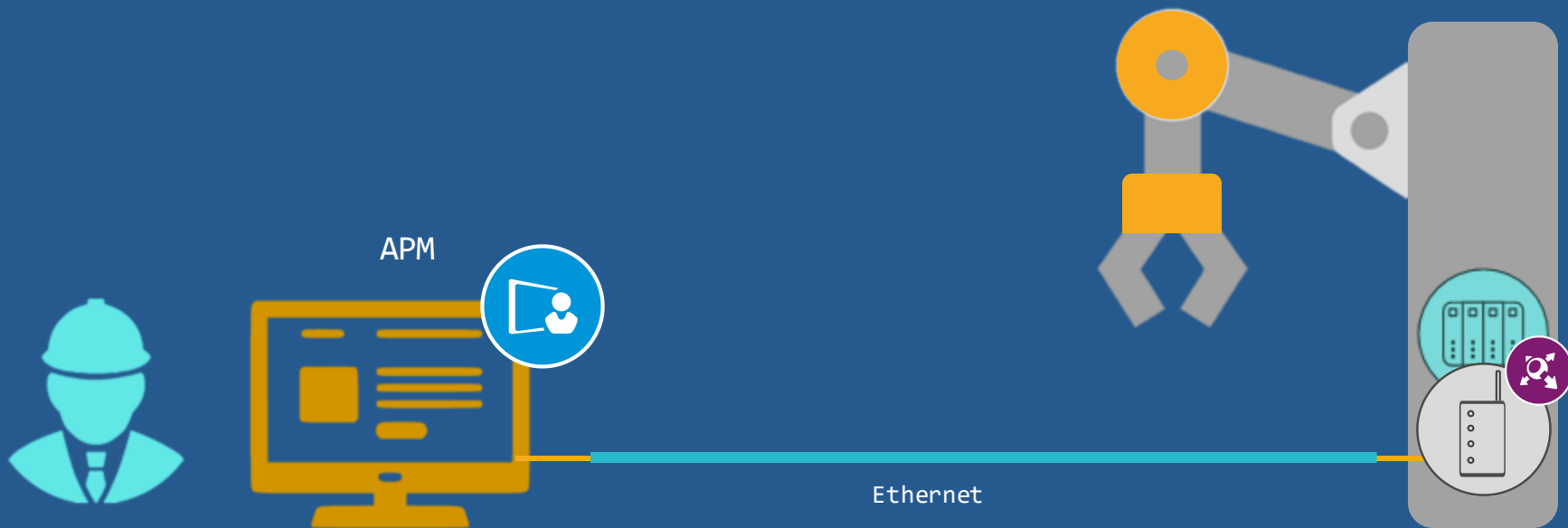
Защита каналов связи до смежных систем



Идентификация объектов при управлении

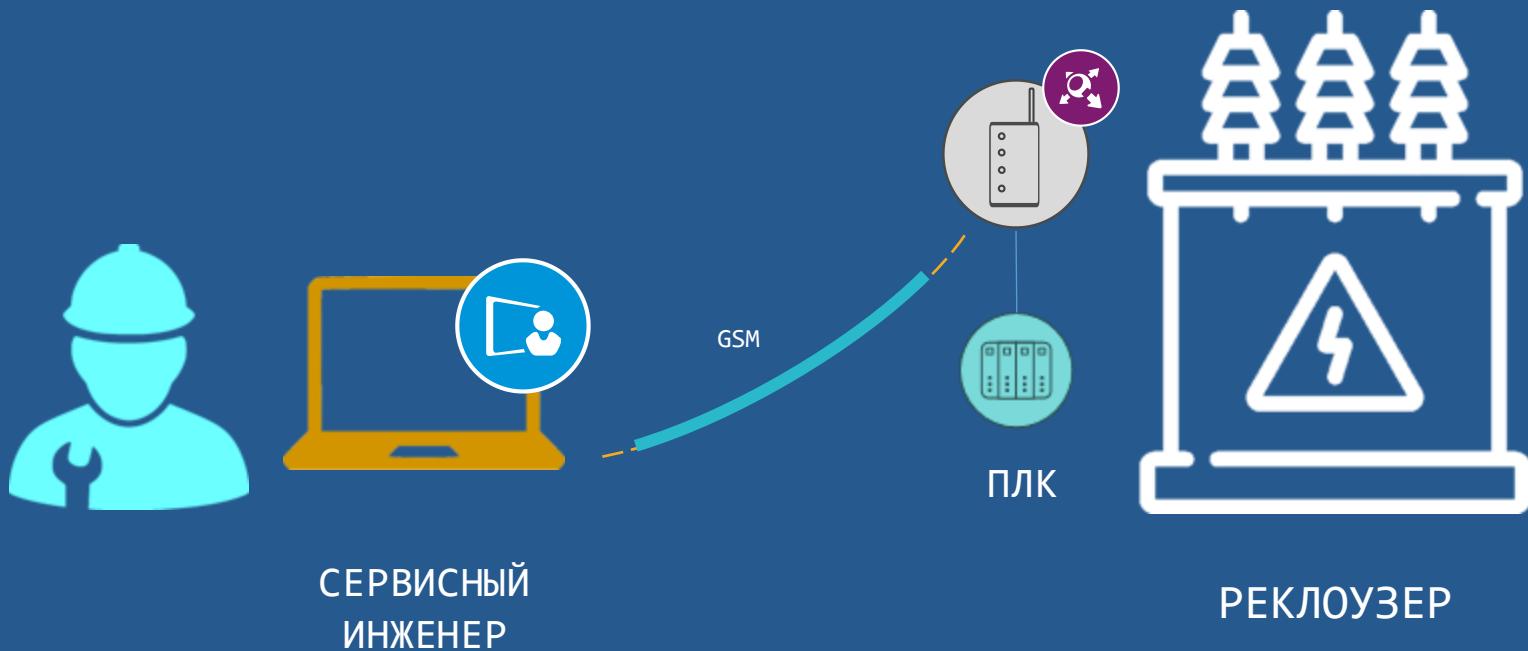


Доверенное конфигурирование



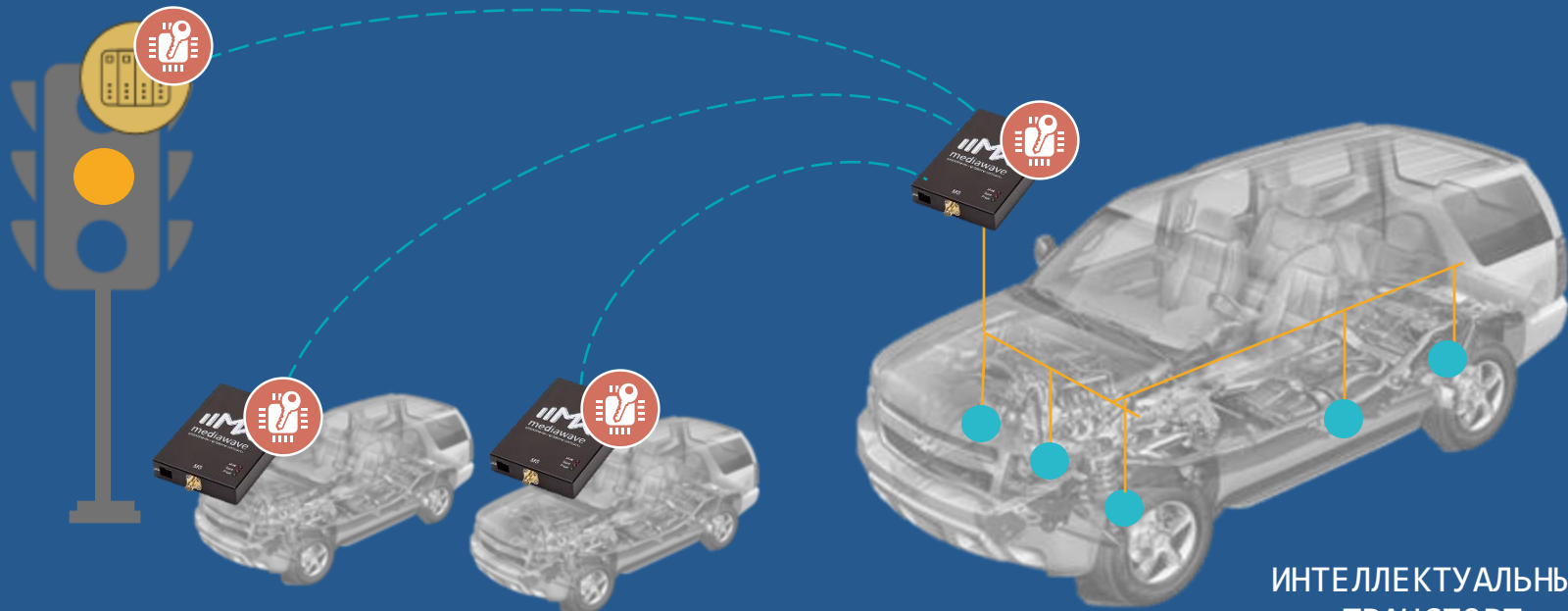
ПРОИЗВОДСТВЕННЫЕ
РОБОТЫ, СТАНКИ С ЧПУ

Удаленное сервисное обслуживание



Доверенные коммуникации

ДОРОЖНАЯ
ИНФРАСТРУКТУРА

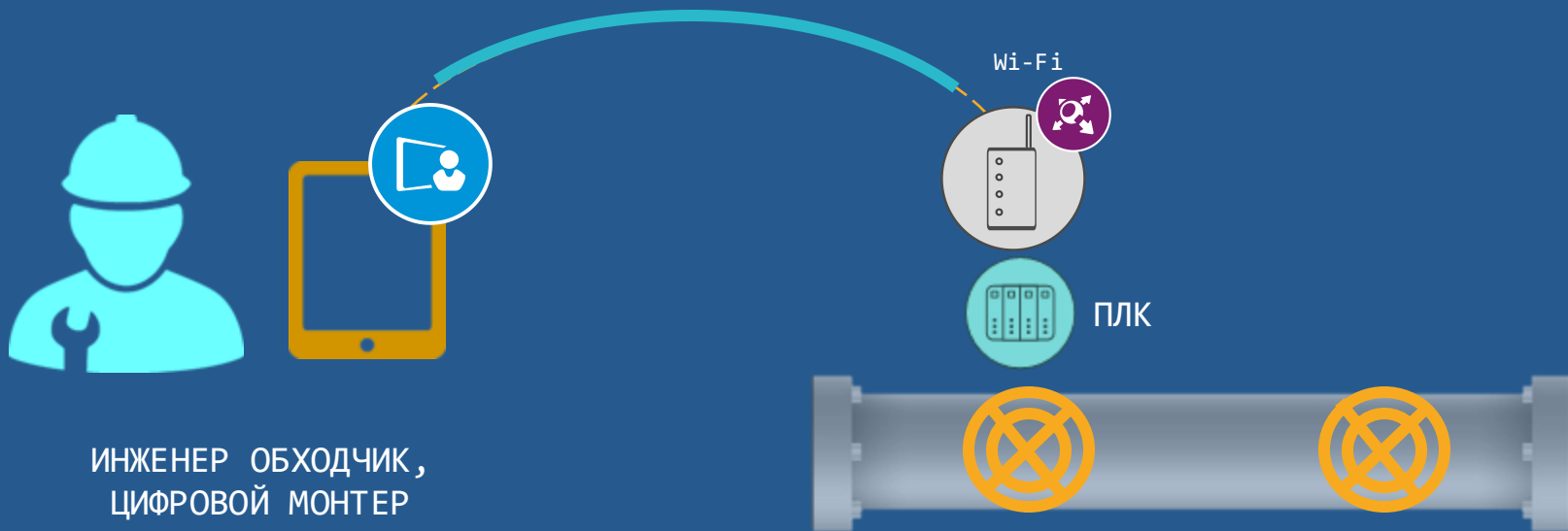


ТРАНСПОРТНЫЕ СРЕДСТВА НА ДОРОГЕ

ИНТЕЛЛЕКТУАЛЬНЫЙ
ТРАНСПОРТ

Техническое обслуживание и ремонт

ТОИР

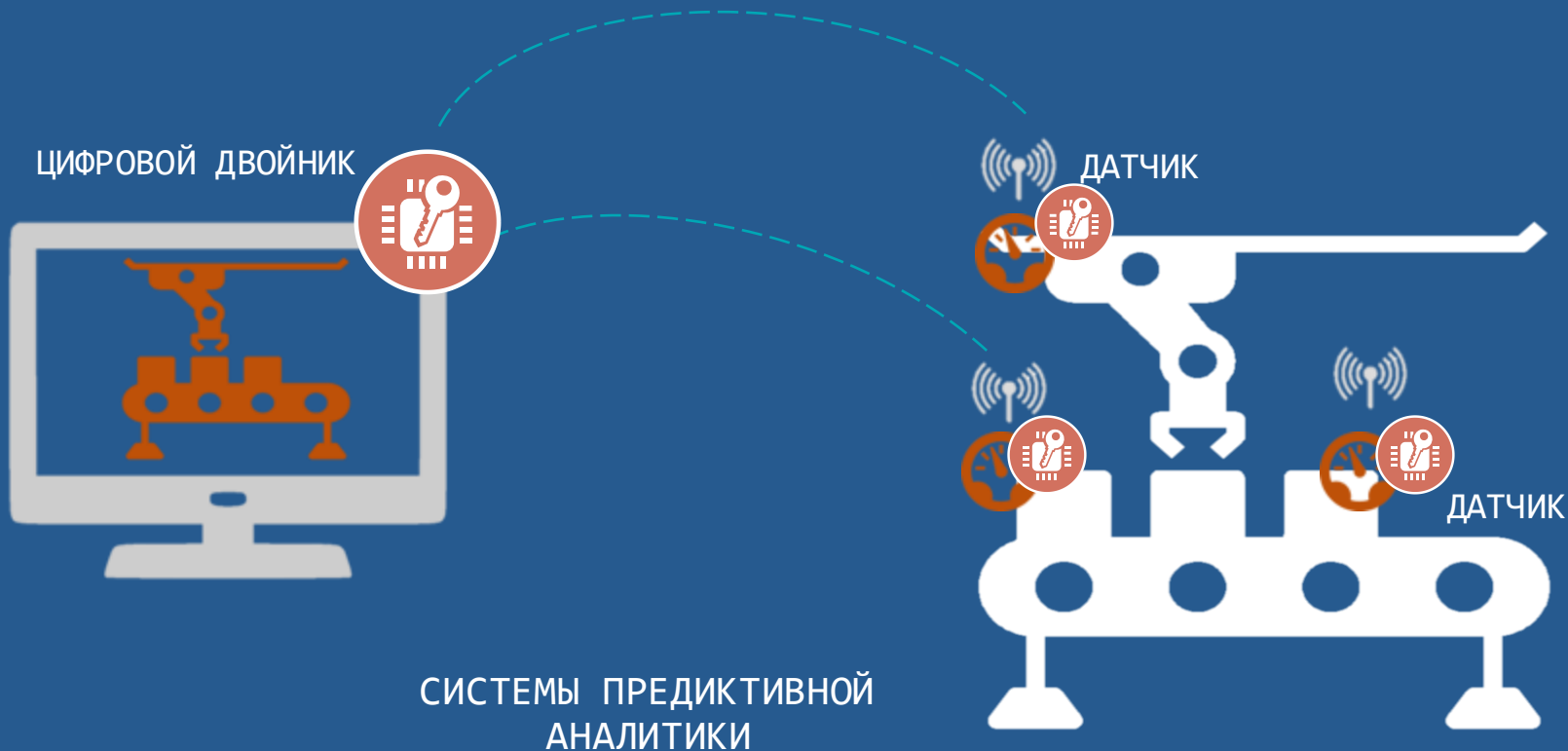


ИНЖЕНЕР ОБХОДЧИК,
ЦИФРОВОЙ МОНТЕР

Дистанционное управление

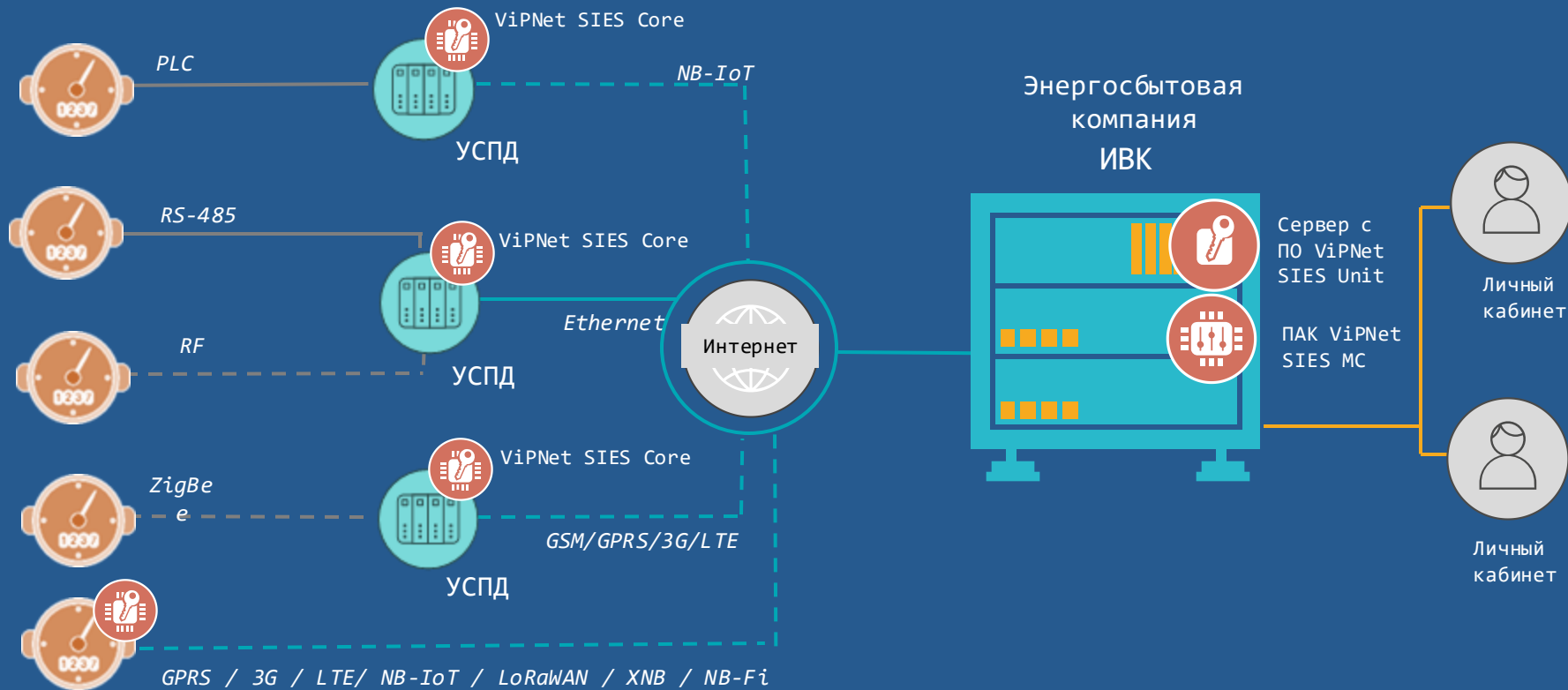


Защита систем сбора информации для предиктивной аналитики



Защита интеллектуальных систем учета электроэнергии

ПРИБОРЫ УЧЕТА (ПУ)





Спасибо за внимание!

Марина Сорокина

e-mail: marina.sorokina@infotecs.ru

Подписывайтесь на наши соцсети



[@infotecs.ru](https://www.instagram.com/infotecs.ru)



[@vpninfectcs](https://www.facebook.com/vpninfectcs)



[@InfoTeCS_Moscow](https://twitter.com/InfoTeCS_Moscow)