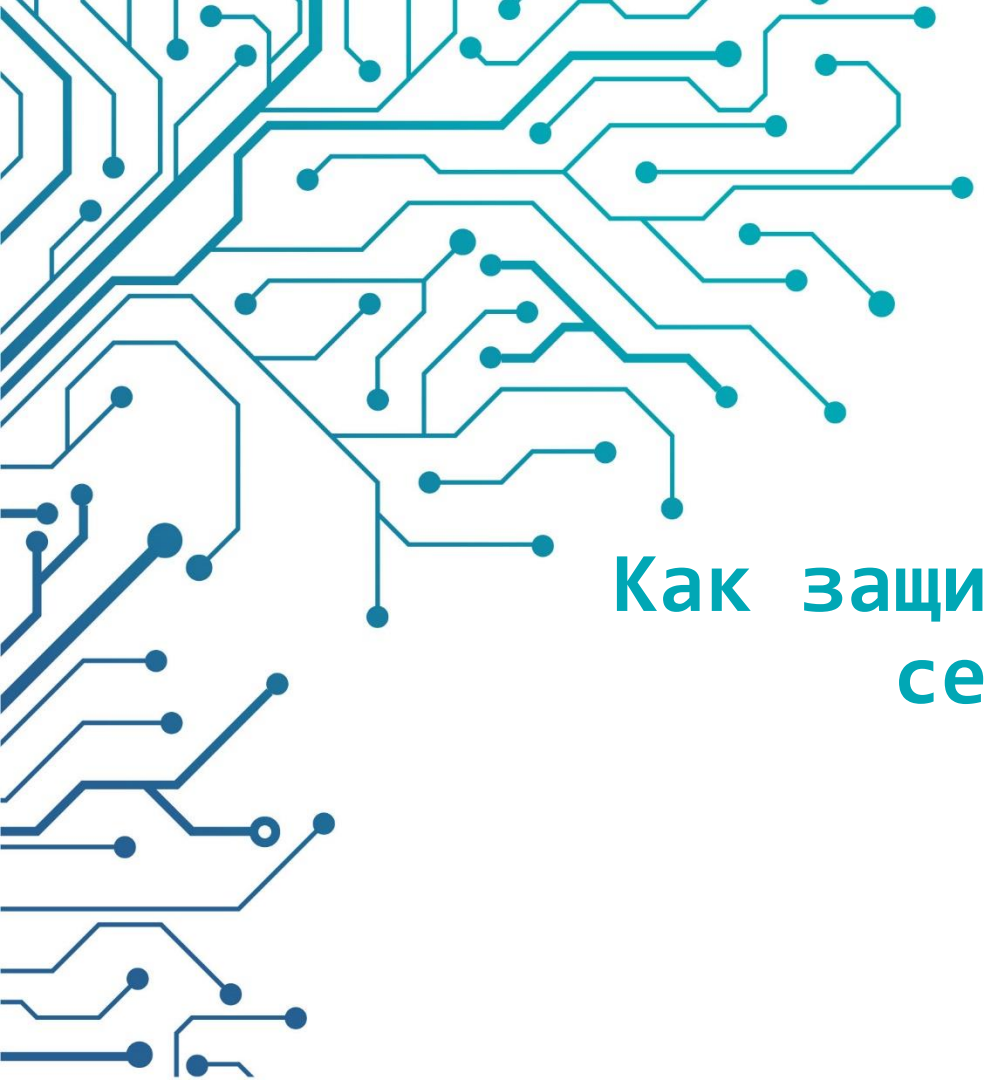
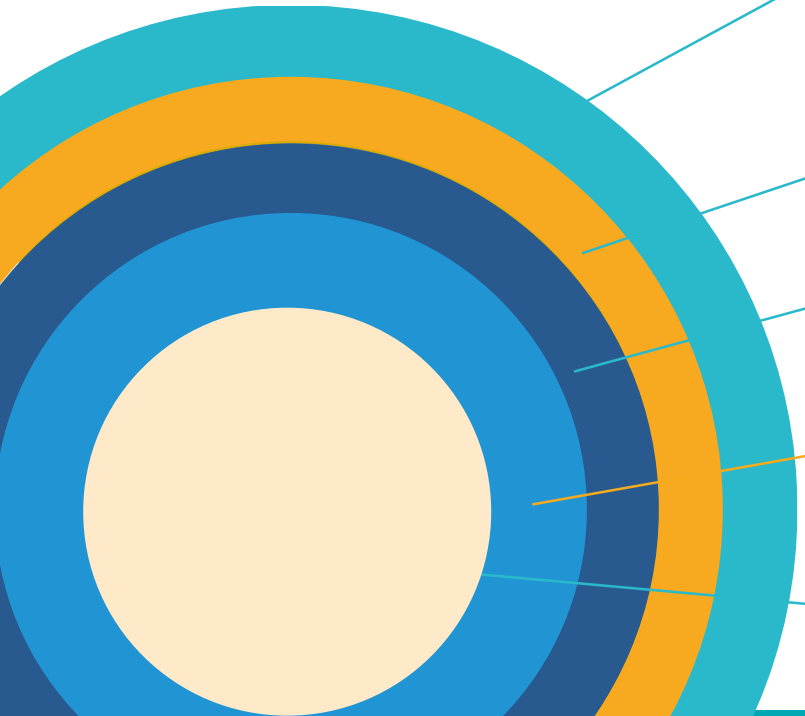


Как защитить промышленные сети в АСУ/IIoT/M2M в соответствии с требованиями РФ

Марина Сорокина,
Руководитель направления


Есть ли что защищать?

Защита каналов – из лучших практик по кибербезопасности АСУ



Policy & procedure: Риск менеджмент, реагирование на компьютерные инциденты, аудит & управление конфигурацией, обучение персонала

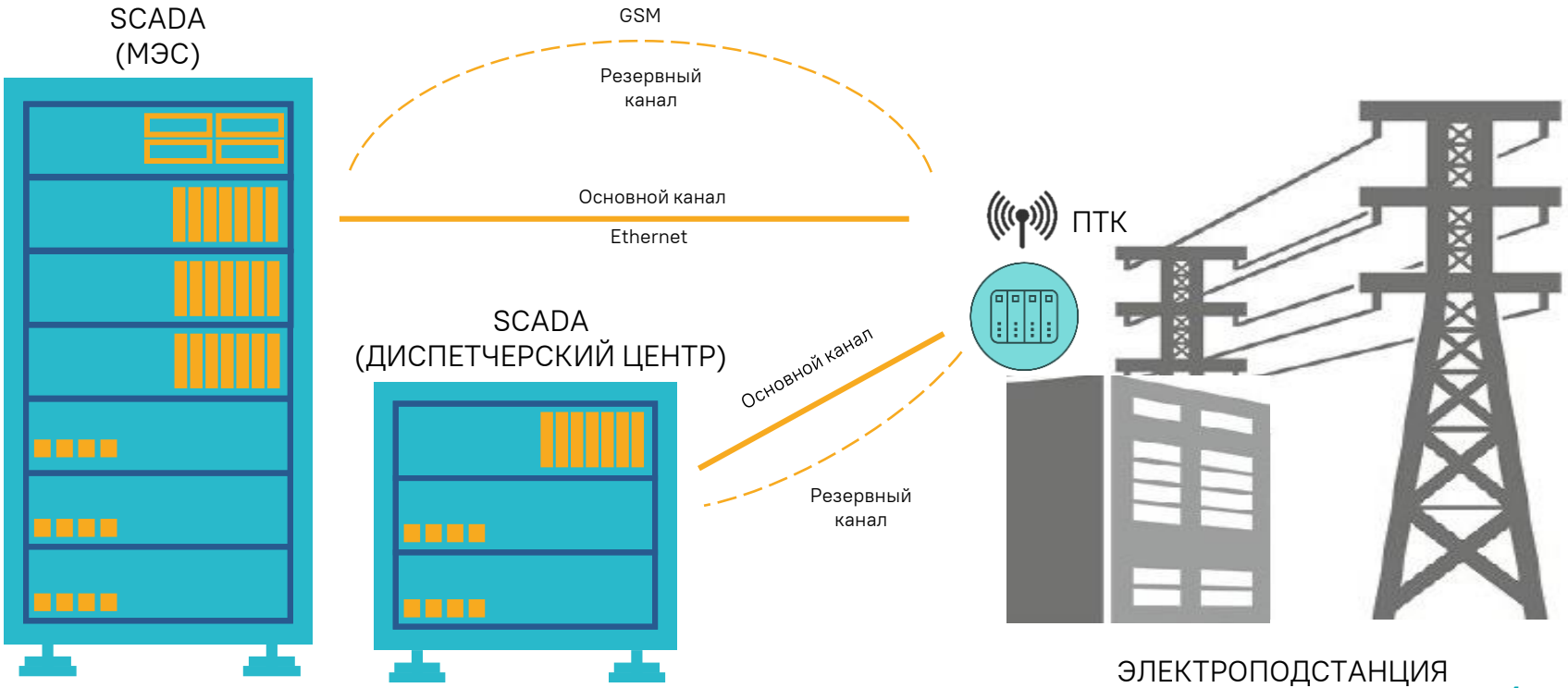
Physical security: Заборы, пропускной контроль, видеонаблюдение, СКУД

Perimeter defense: Межсетевые экраны

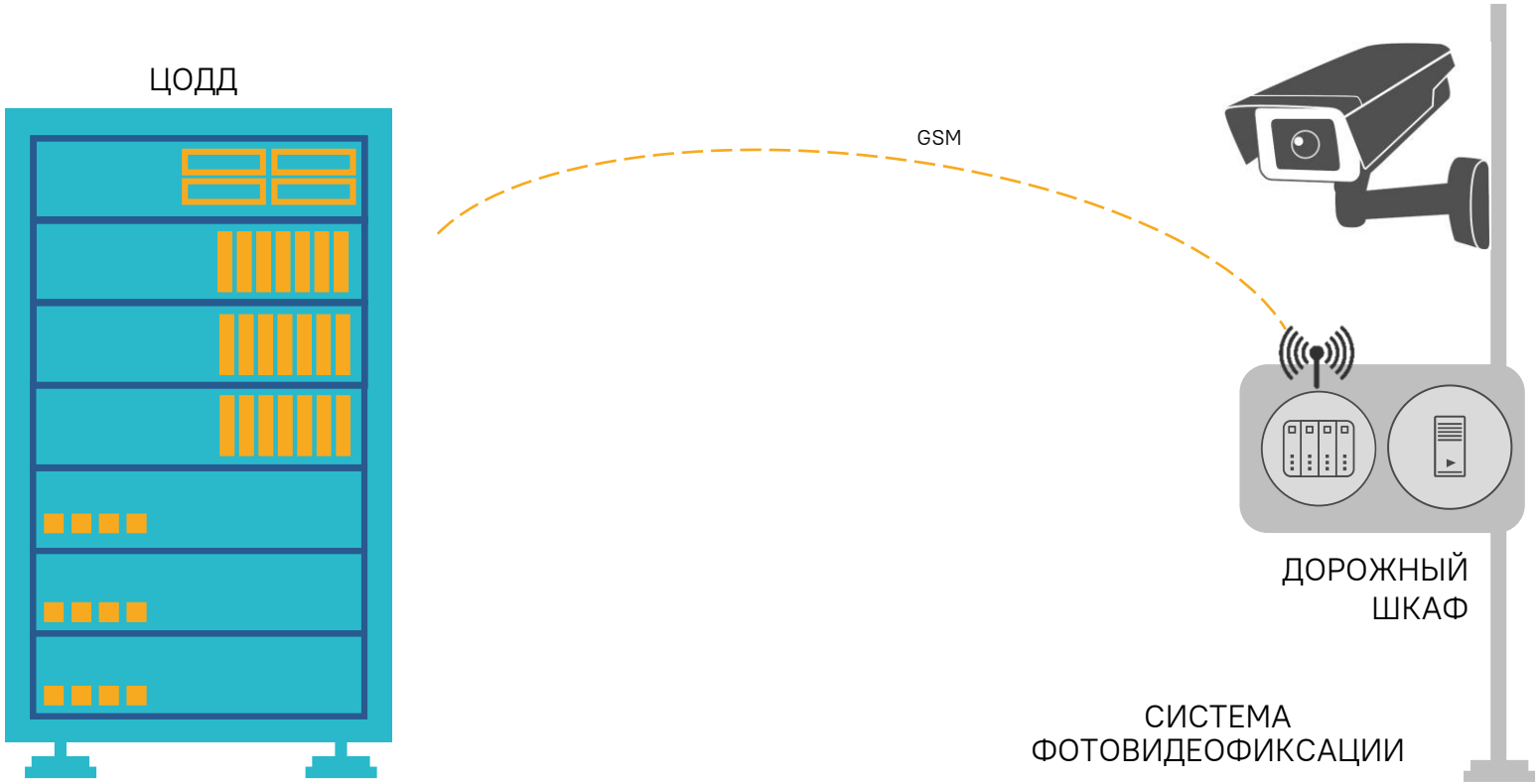
Network security: Криптошлюзы, МЭ, IDS

Host security: Антивирусы, хостовые IDS, белые списки

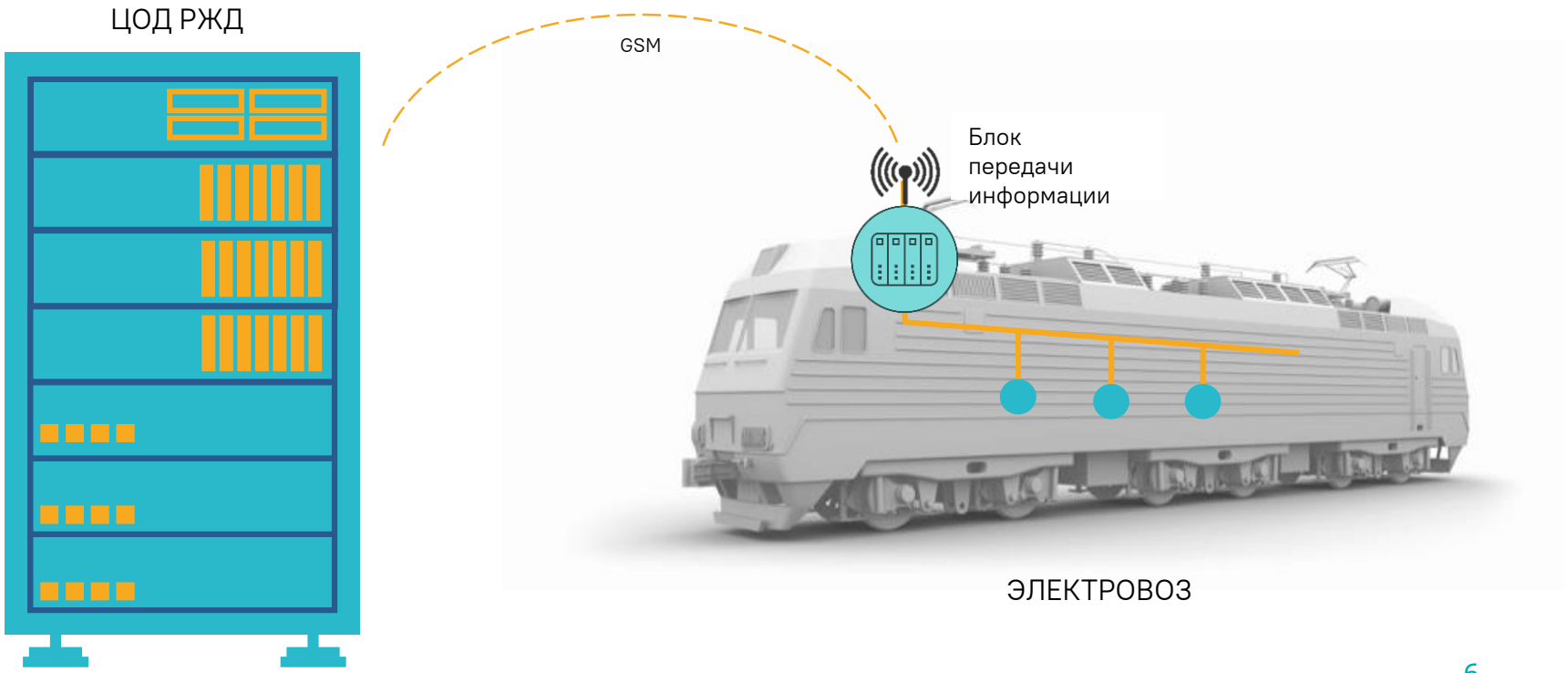
Защита каналов АСУ/IIoT/M2M как задача ИБ



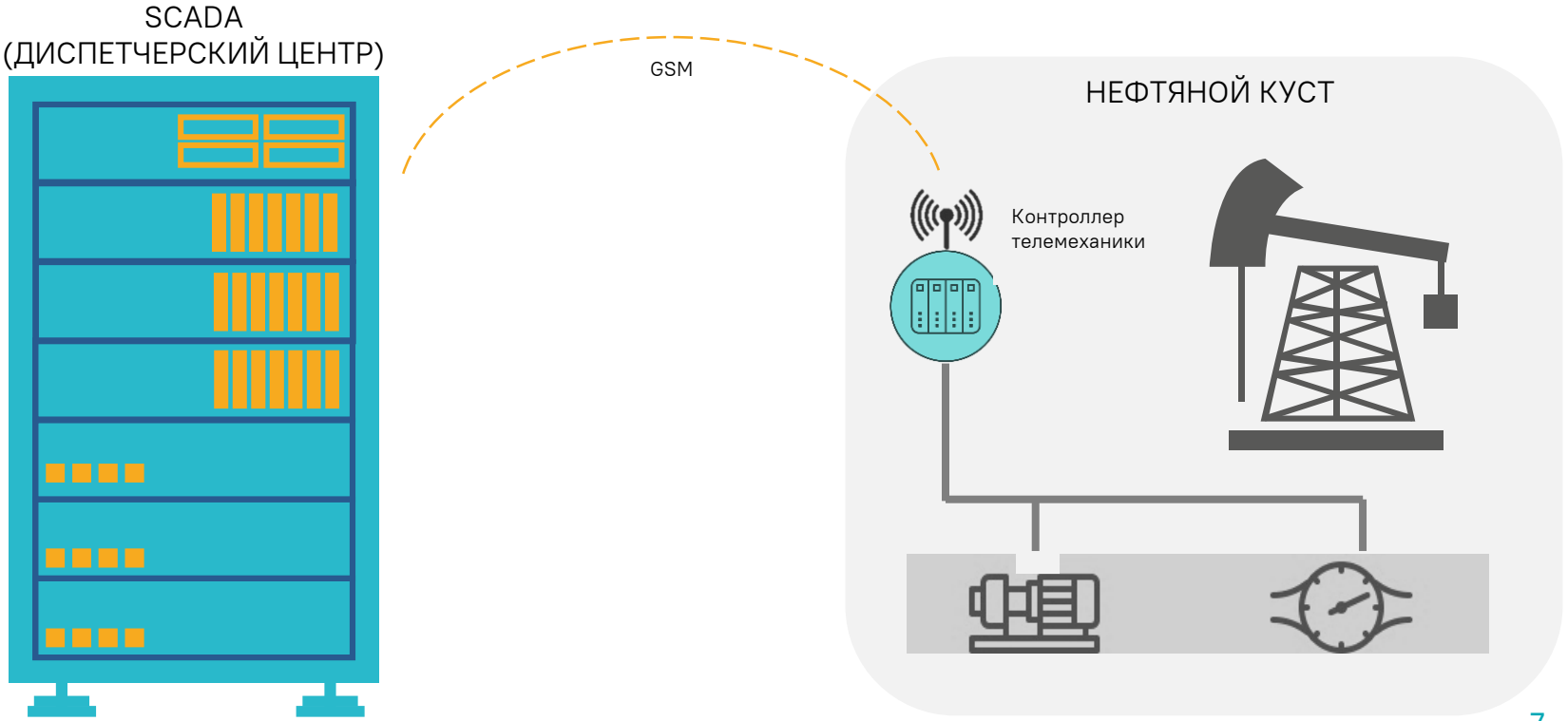
Защита каналов АСУ/IIoT/M2M как задача ИБ



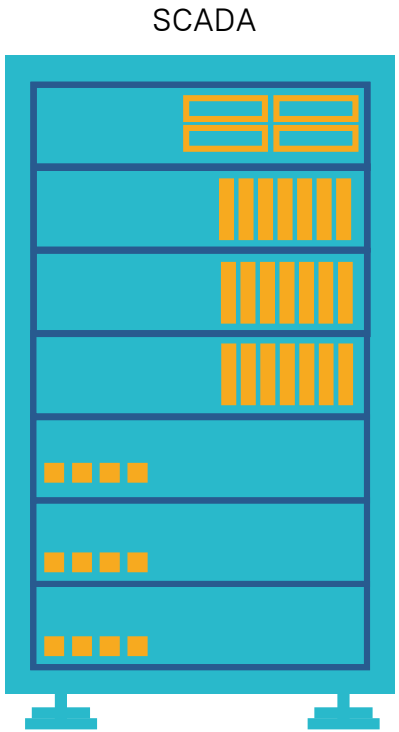
Защита каналов АСУ/IIoT/M2M как задача ИБ

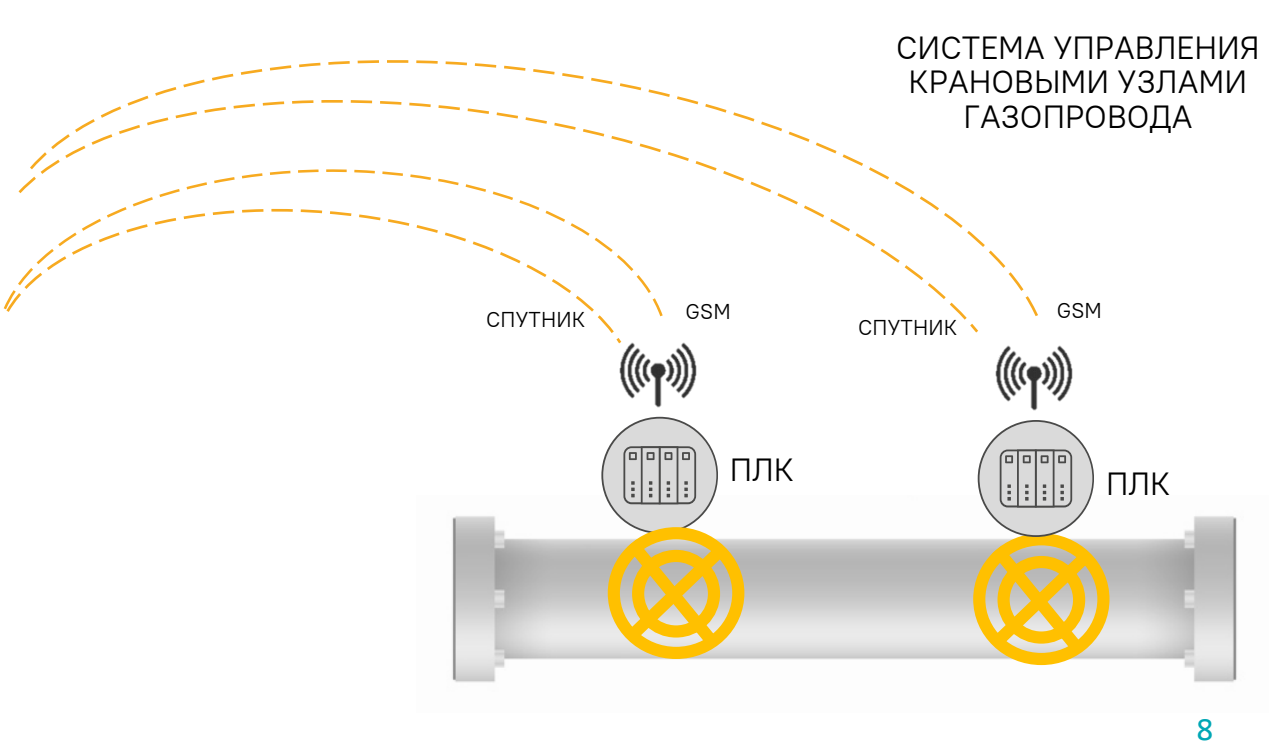


Защита каналов АСУ/IIoT/M2M как задача ИБ

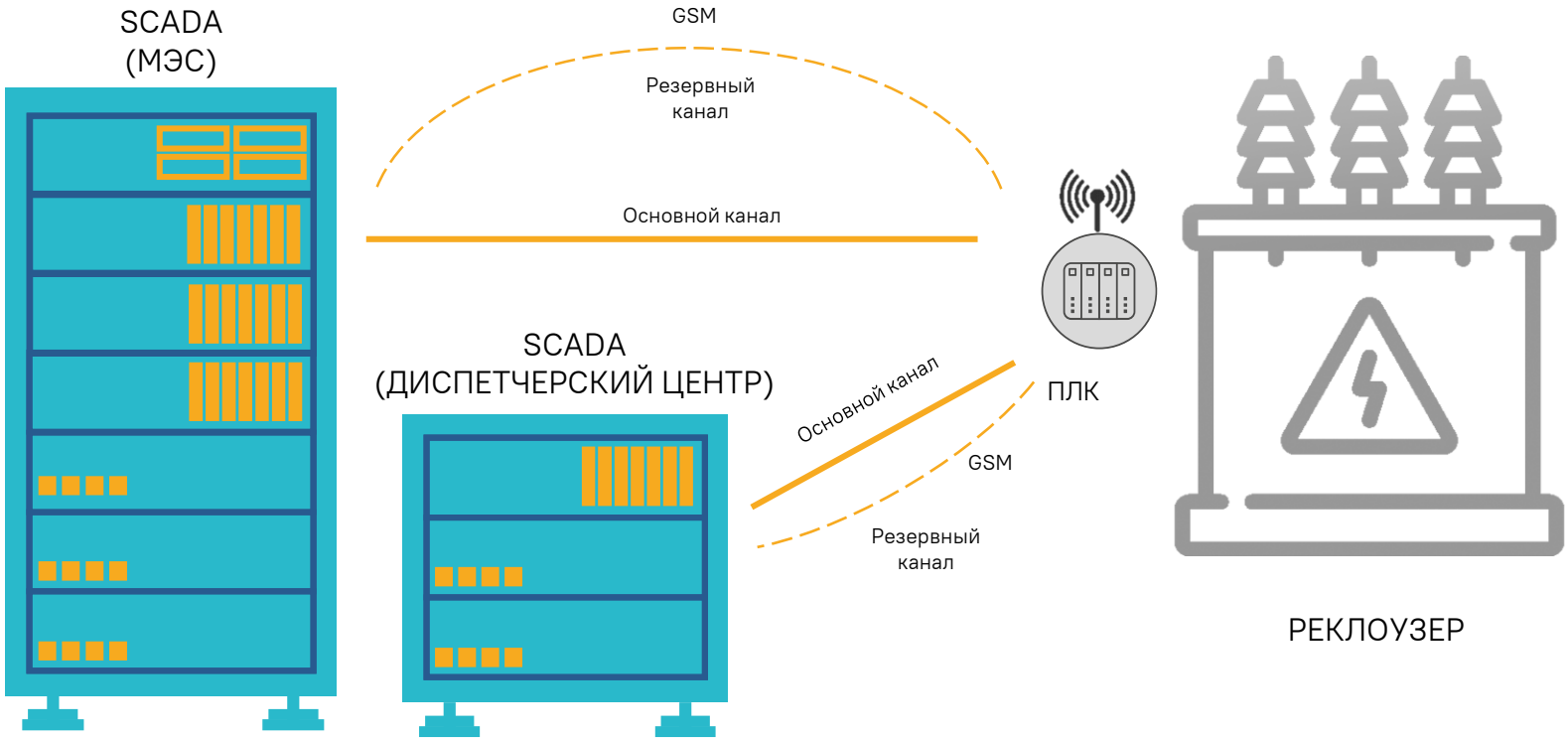


Защита каналов АСУ/IIoT/M2M как задача ИБ

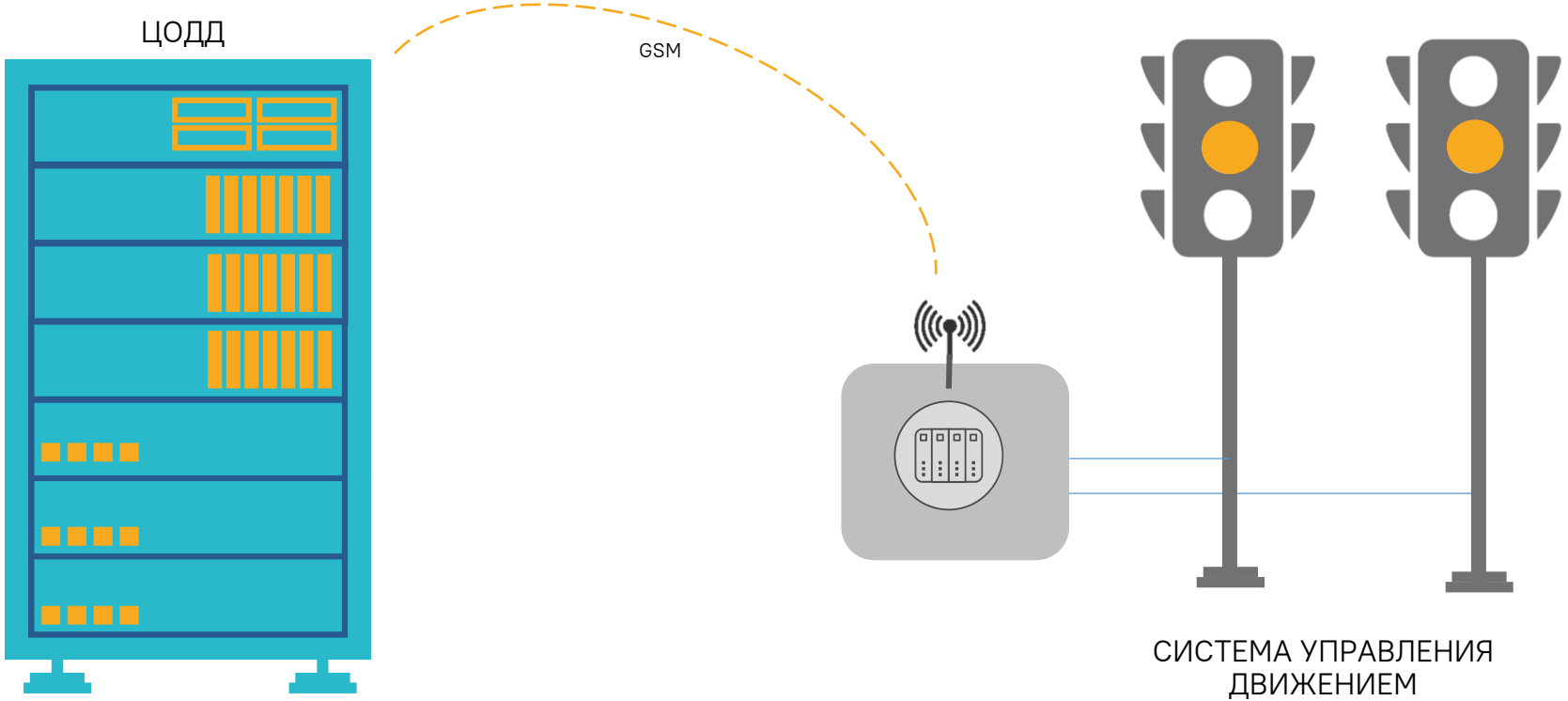




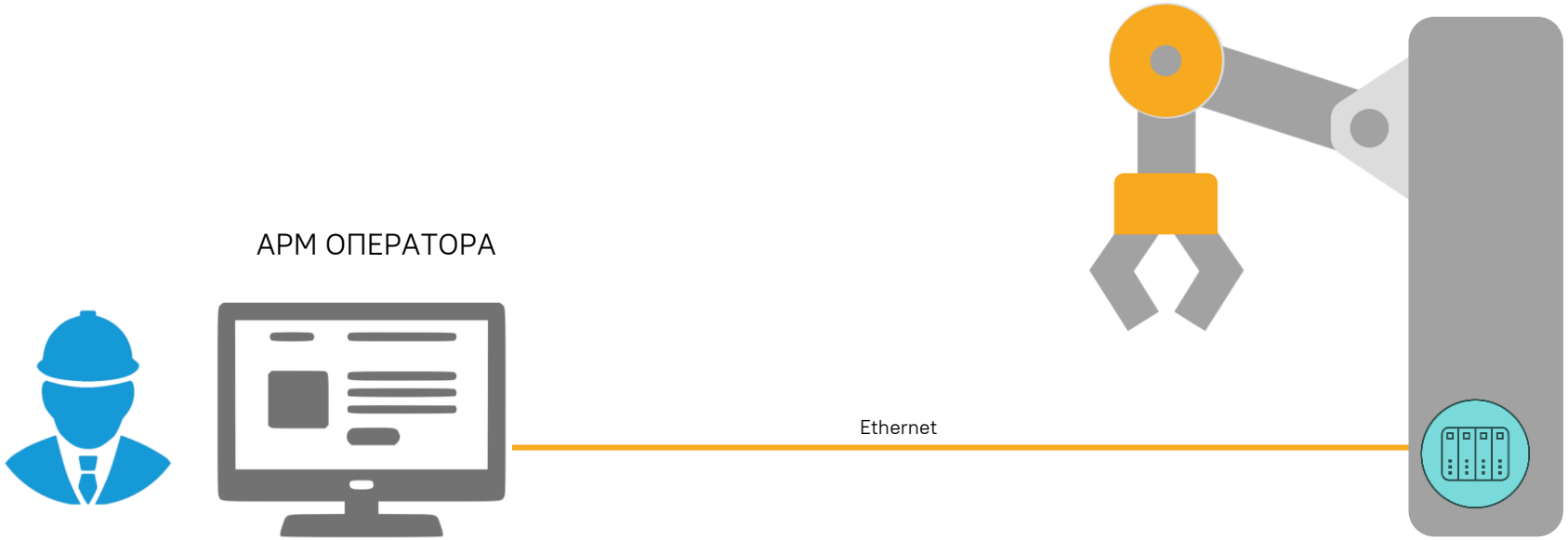
Защита каналов АСУ/IIoT/M2M как задача ИБ



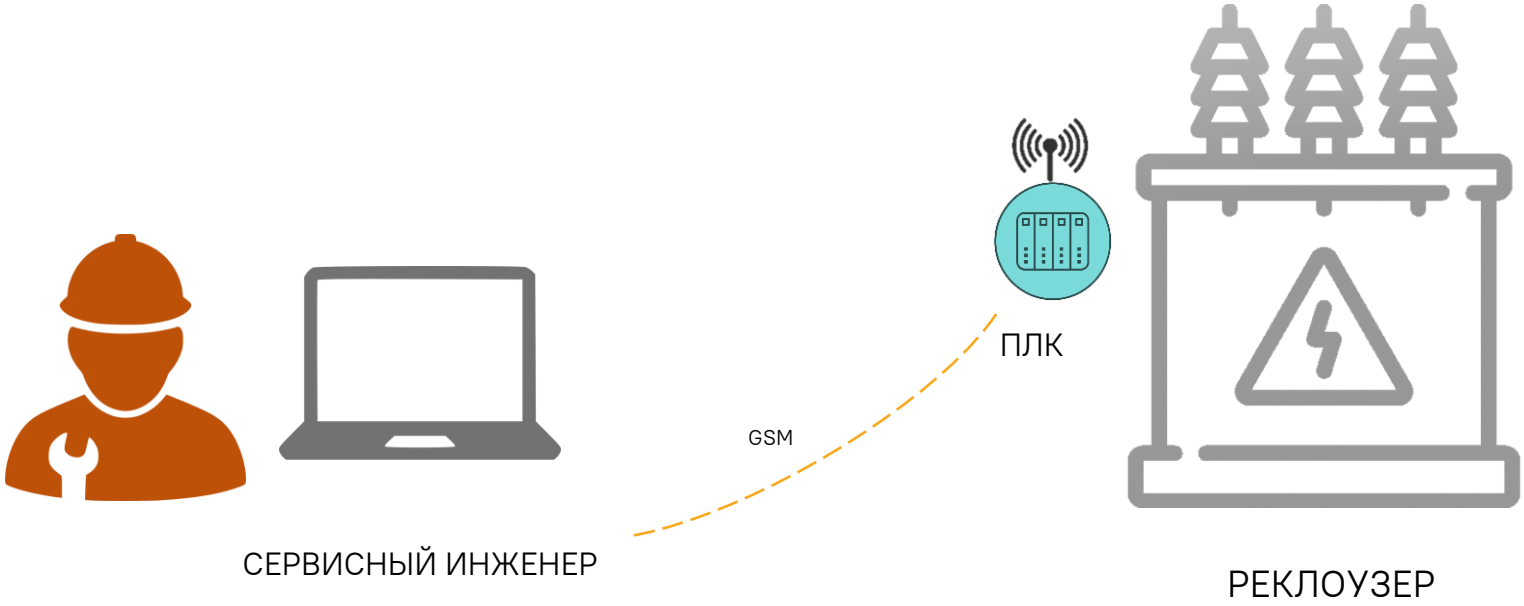
Защита каналов АСУ/IIoT/M2M как задача ИБ



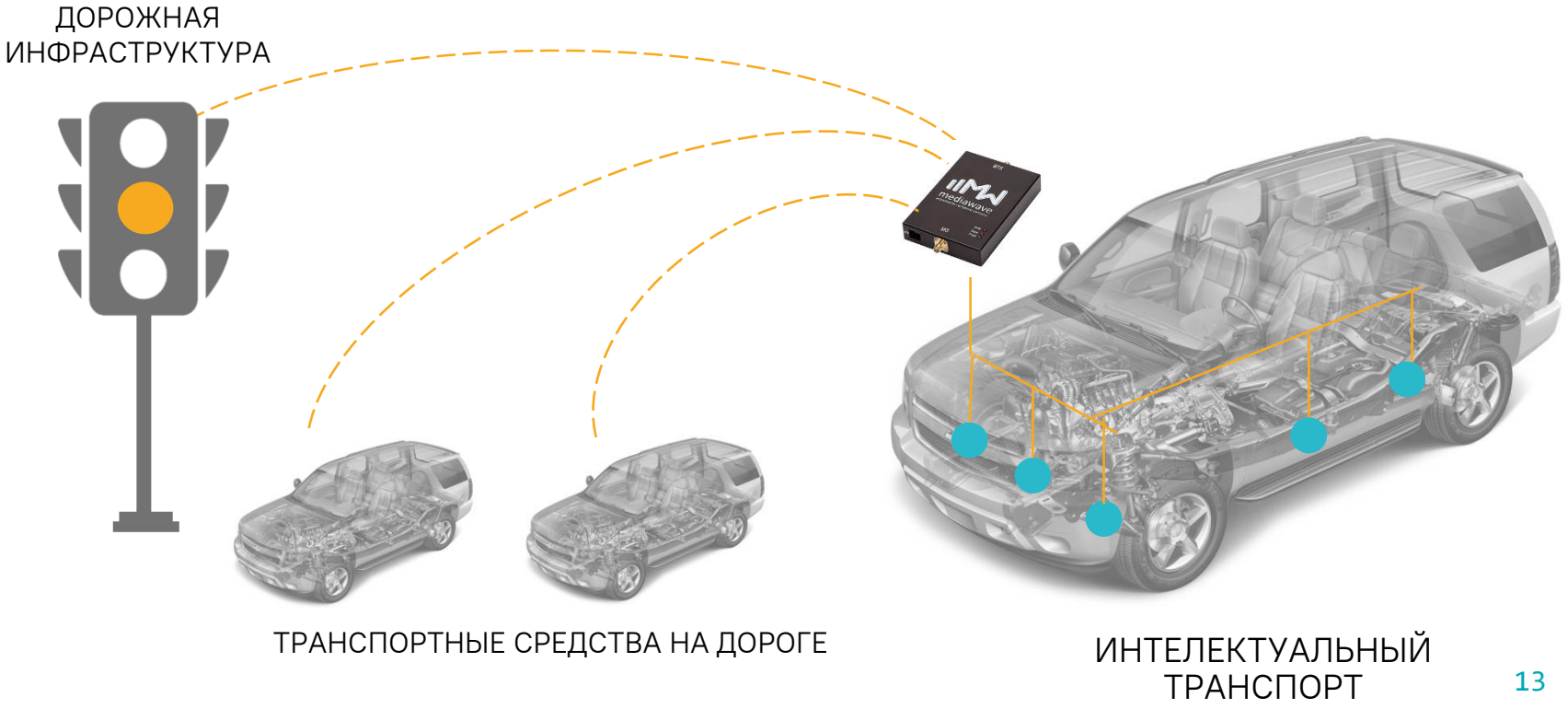
Защита каналов АСУ/IIoT/M2M как задача ИБ



Защита каналов АСУ/IIoT/M2M как задача ИБ

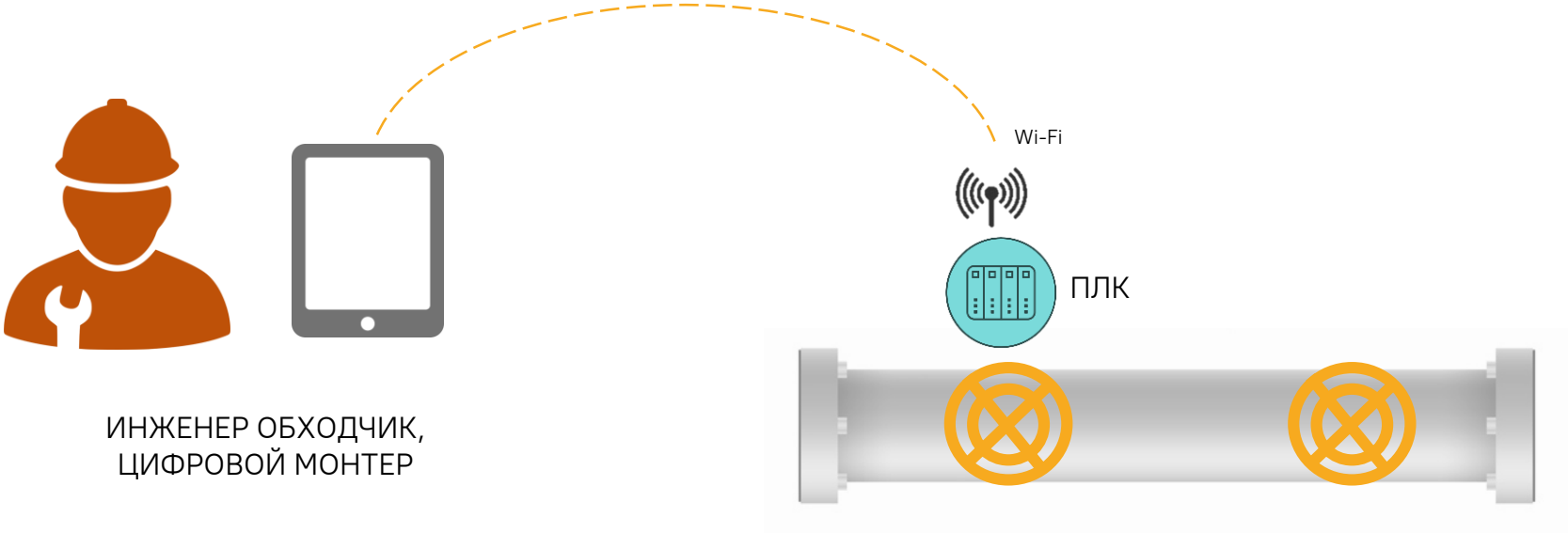


Защита каналов АСУ/IIoT/M2M как задача ИБ



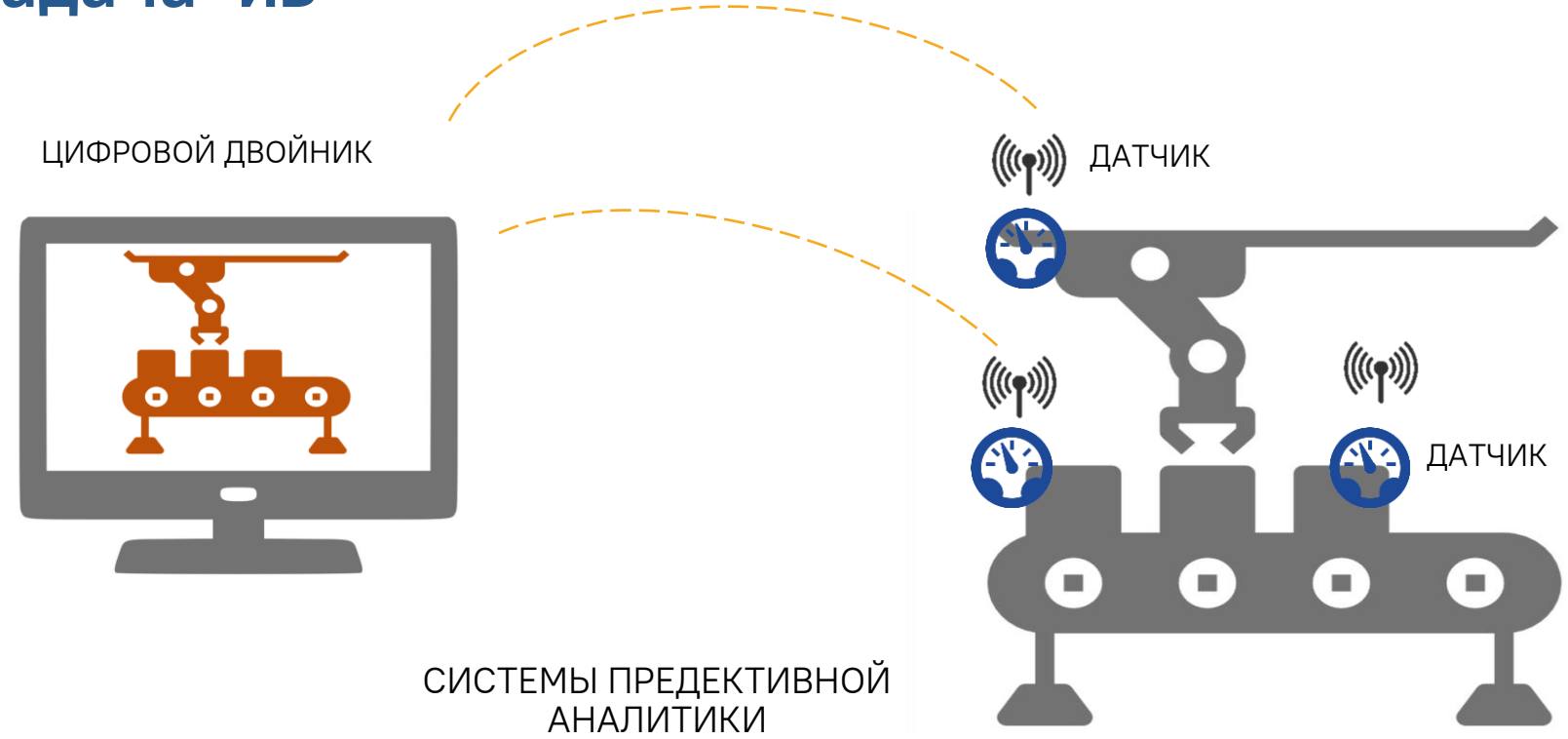
Защита каналов АСУ/IIoT/M2M как задача ИБ

ТОИР



Защита каналов АСУ/IIoT/M2M как задача ИБ

Защита каналов АСУ/IIoT/M2M как задача ИБ

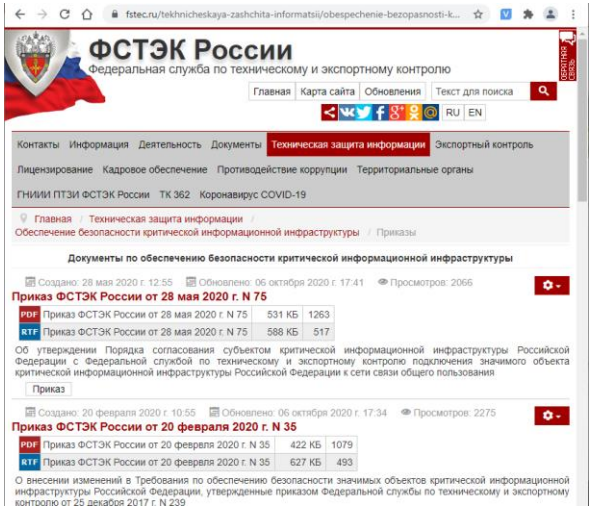


Законодательная база

Защита промышленных сетей согласно требованиям РФ

Обозначение меры	Меры защиты информации
Приказ ФСТЭК России №239 от 25.12.2017 «Об утверждении требований по обеспечению безопасности ЗОКИИ РФ» и Приказ ФСТЭК России №31 от 14.03.2014 «Об утверждении требований к обеспечению защиты информации в АСУ ТП на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»	
ЗИС.1/ЗИС.2	Защита периметра информационной (автоматизированной) системы
ЗИС.2/ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы
ЗИС.3/ЗИС.4	Сегментирование информационной (автоматизированной) системы
ЗИС.5/ЗИС.6	Управление сетевыми потоками
ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы
ЗИС.19	Защита информации при ее передаче по каналам связи
ЗИС.20	Обеспечение доверенных канала, маршрута
ЗИС.27	Обеспечение подлинности сетевых соединений
ЗИС.32	Защита беспроводных соединений
ЗИС.35	Управление сетевыми соединениями
УПД.13	Реализация защищенного удаленного доступа
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем

Приказ №75 ФСТЭК России от 28.05.2020 г.«Об утверждении порядка согласования субъектом КИИ РФ с ФСТЭК подключения ЗОКИИ РФ к сети связи общего пользования»



Процедура согласования для значимого объекта КИИ при подключении его к сети передачи общего пользования.

Согласование осуществляется в части оценки достаточности применяемых СЗИ для значимого объекта КИИ

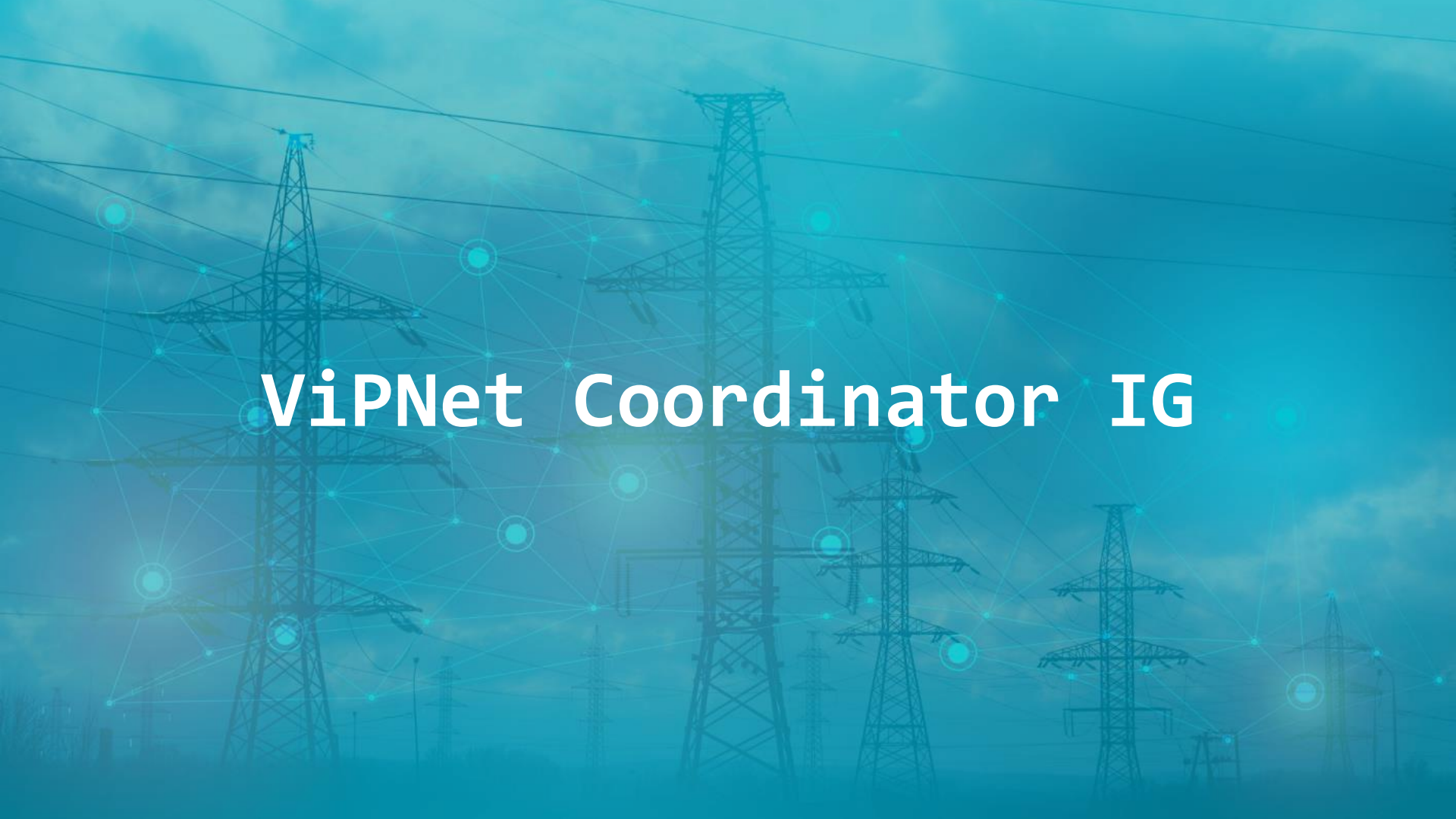
Согласование осуществляется до ввода действия объекта КИИ

Если объект КИИ на момент включения в реестр значимых объектов КИИ имел подключение к сети передачи общего пользования, то согласование не требуется.

СЗИ, необходимые для подключения объекта КИИ к сетям связи общего пользования

Согласно Приказу ФСТЭК России №239 от 25.12.2017 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

	1 КЗ	2 КЗ	3 КЗ
МЭ (ПАК) уровня сети (Тип А или Д)	+	+	+
Граничный маршрутизатор (ПАК)	+	+	+
• с сертификацией по ТДБ	+	-	-
Средство антивирусной защиты	+	+	+
СКЗИ (VPN – шлюз или пр)	+	+	+
СОВ	+	+	


ViPNet Coordinator IG

Исполнения ViPNet Coordinator IG 4

ViPNet Coordinator
IG10 I1
10 Мбит/с

ViPNet Coordinator
IG100 I1
60 Мбит/с

ViPNet Coordinator
IG10 I2
10 Мбит/с
(начиная с 4.3.2)

ViPNet Coordinator IG 4 – идеальный вариант для защиты каналов АСУ и КИИ

VPN – шлюз уровня L3, L2
СКЗИ класса КС3 по требованиям ФСБ России

4 уровень доверия
по требованиям ФСТЭК России

Импортозамещение
Произведено в России

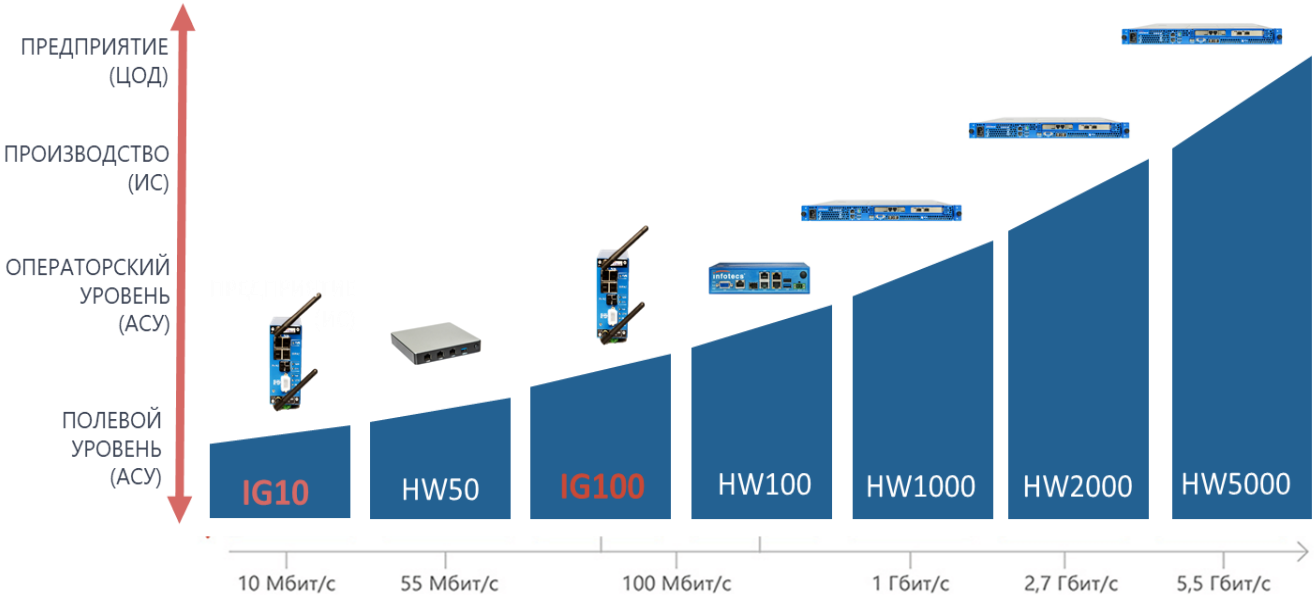
Межсетевой экран
Типа «А» 4 класса
Типа «Д» 4 класса
по требованиям ФСТЭК России

4 класс защищенности по требованиям ФСБ России

Маршрутизатор, беспроводной роутер
Проводные интерфейсы , 3G/4G, Wi-fi, Конвертер RS232/485 - Ethernet

Единая экосистема VIPNet VPN

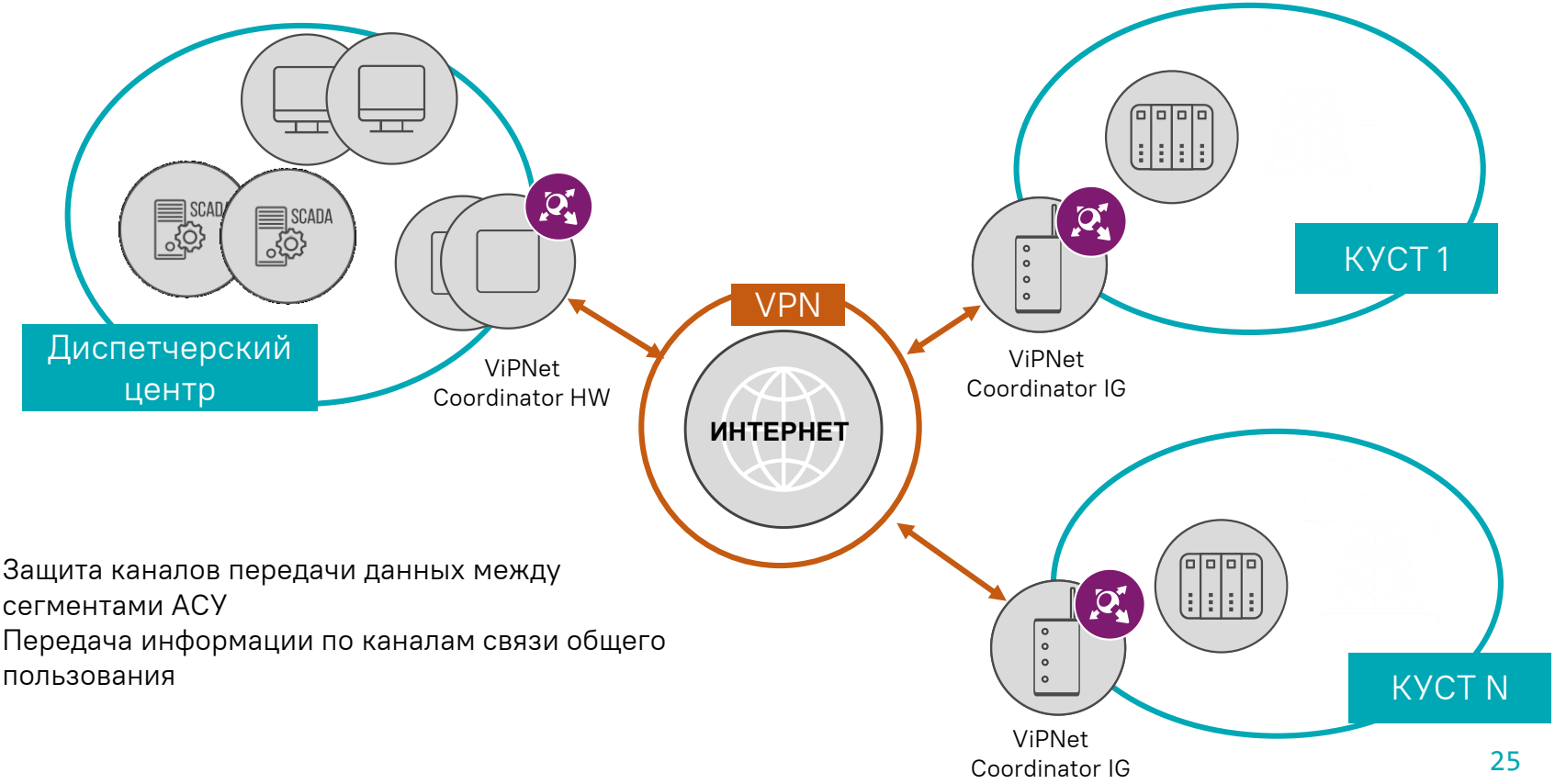
ViPNet Coordinator HW, ViPNet Coordinator VA, ViPNet Coordinator IG



ViPNet Client, ViPNet Client 4U

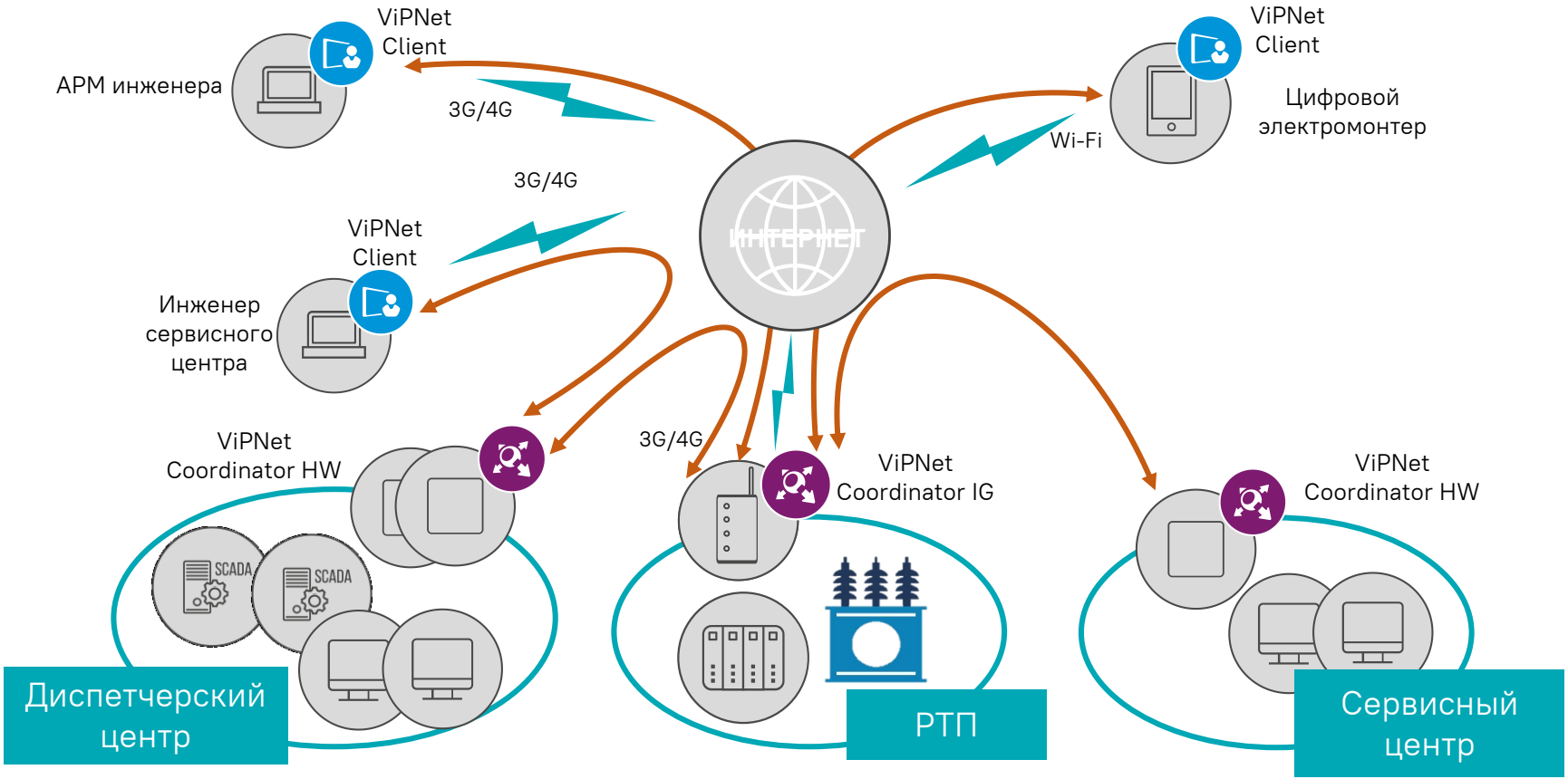
MIPS МЦСТ ЭЛЬБРУС

Защита каналов связи



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

Защищенный удаленный доступ



Сертификаты соответствия по требованиям ФСБ России

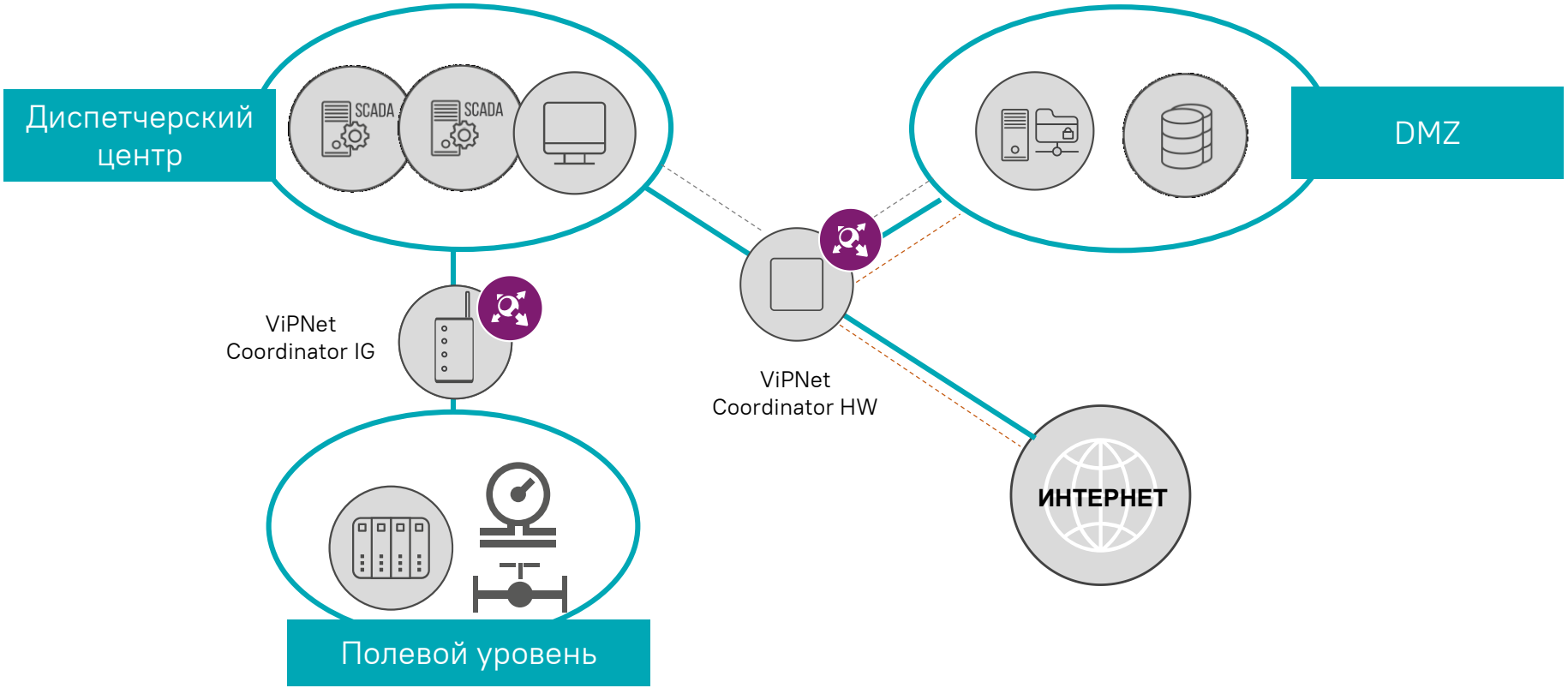
ViPNet Coordinator IG 4.2.4:

- Сертификат № СФ/124-3550 по требованиям к СКЗИ класса КС3;
- Сертификат № СФ/525-3926 по требованиям к МЭ 4 класса защищенности;

ViPNet Coordinator IG 4.3.3:

- Проведение контроля изменений относительно версии 4.2.4;
- Сертификация исполнения ViPNet Coordinator IG10 I2.

Сегментирование сетей



Правила МЭ для разных режимов работы ViPNet Coordinator IG

- ViPNet PolicyManager
- WebUI
- CLI

√ пром. протоколы тех. Процесса;
х протоколы удаленного обслуживания;
х обновление IG

- GPIO
- ViPNet PolicyManager
- WebUI
- CLI

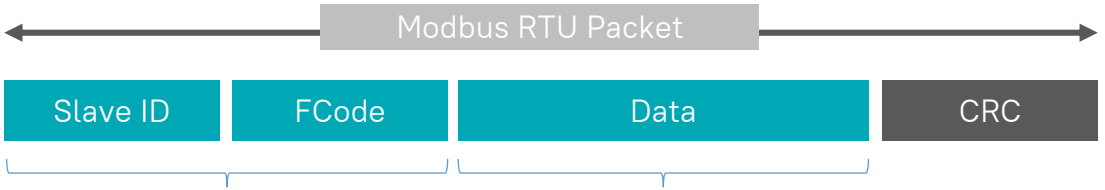
Для аварийного режима

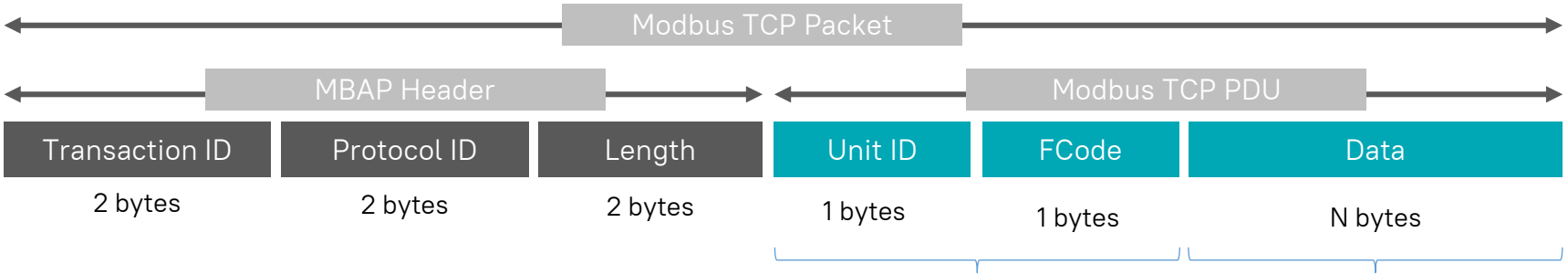
- ViPNet PolicyManager
- WebUI
- CLI

√ пром. протоколы тех. процесса;
√ протоколы удаленного обслуживания;
√ обновление IG

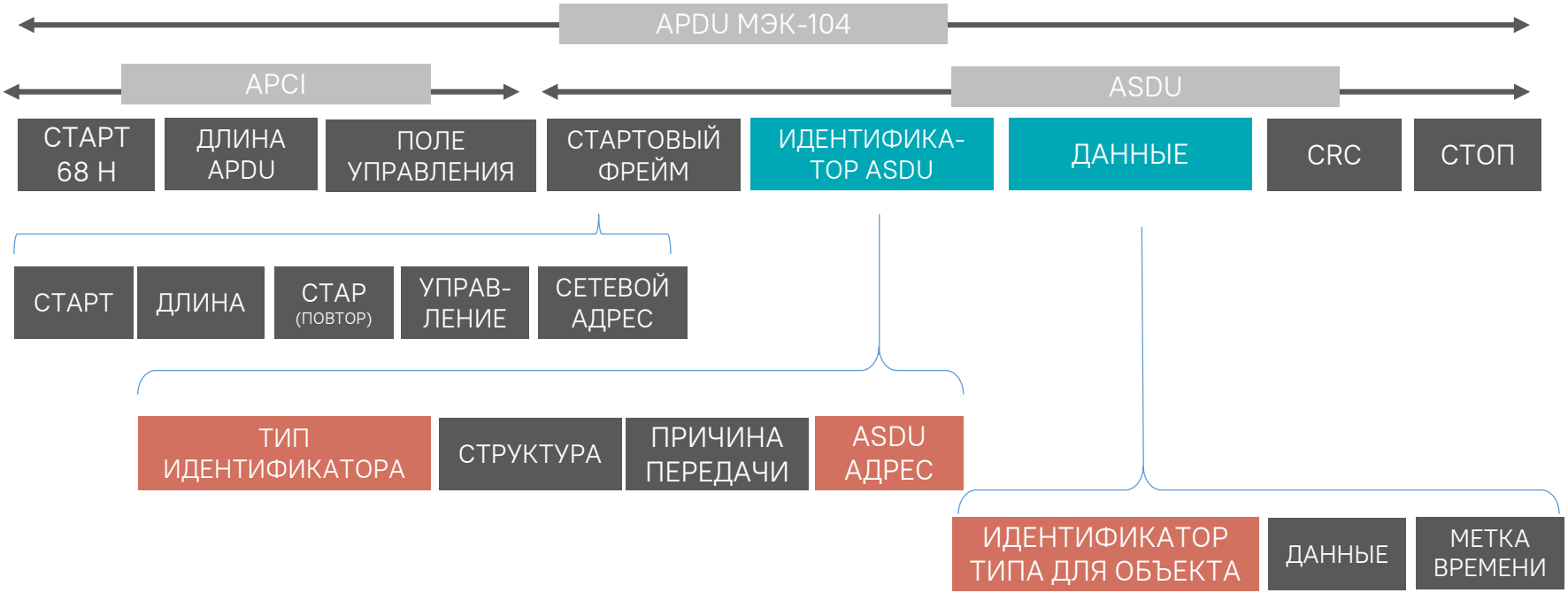
Глубокая фильтрация промышленных протоколов (Modbus TCP)

- Фильтрация по нестандартным портам
- Фильтрация по адресам устройств
- Фильтрация по коду сообщения
- Фильтрация по регистрам записи и чтения





Фильтрация протокола МЭК 60870-5-104



Сертификат соответствия по требованиям ФСТЭК России

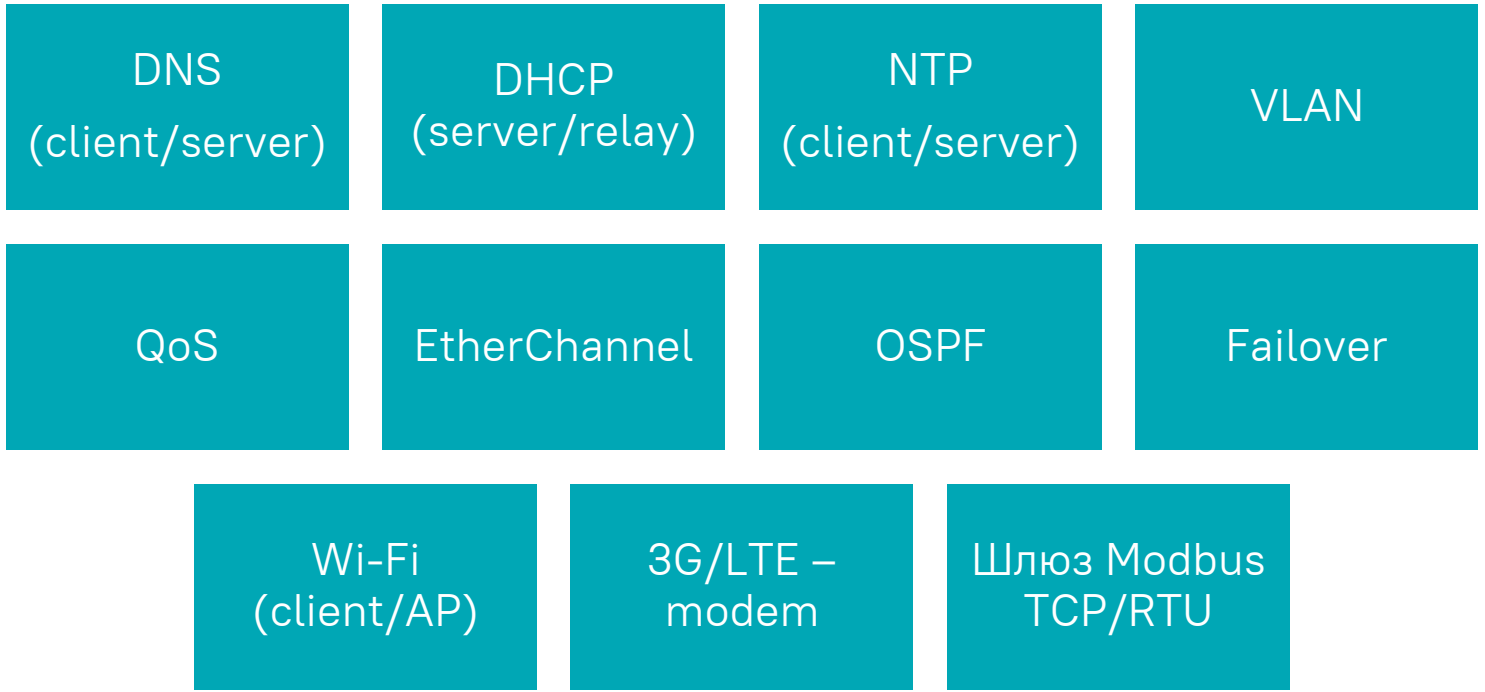
ViPNet Coordinator IG 4.2.4:

- требования к МЭ;
- профиль защиты МЭ типа Д 4 класса защиты (ИТ.МЭ.Д4.ПЗ);
- профиль защиты МЭ типа А 4 класса защиты (ИТ.МЭ.А4.ПЗ);
- 4 уровень доверия по ТДБ (2020 г);

ViPNet Coordinator IG 4.3.3:

- проведение контроля изменений относительно версии 4.2.4.

Сетевые сервисы



Сертификаты и декларации по требованиям Минкомсвязи России

Сертификаты соответсвия на ПАК ViPNet Coordinator IG 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:

- № ОС-4-РД-1385 – на ViPNet Coordinator IG10 I1 и ViPNet Coordinator IG100 I1;
- № ОС-4-РД-1384 – на ViPNet Coordinator IG10 I2;

Декларации соответсвия на ПАК ViPNet Coordinator IG на АП IG10 I1, IG10 I2, IG100 I1 по требованиям:

- к абонентским станциям стандарта GSM-900/1800, UMTS, LTE, LTE-Advanced;
- к оборудованию проводных и оптических систем передачи абонентского доступа.

Реестры РПО, ТОРП, РЭП

- ПО ViPNet Coordinator IG включен в реестр российского ПО – рег.номер 5102 (19.01.2019)
- ПАК ViPNet Coordinator IG включен в реестр телекоммуникационного оборудования российского происхождения (ТОРП) и в единый реестр российской радиоэлектронной продукции (реестр РЭП) (от 29.09.2020):
  - ViPNet Coordinator IG10 I1 – реестровая запись ТКО-517/20
  - ViPNet Coordinator IG10 I2 – реестровая запись ТКО-518/20
  - ViPNet Coordinator IG100 I1 – реестровая запись ТКО-519/20

Российское оборудование в КИИ

Выполнение требований по применению российского ПО и российской радиоэлектронной продукции сегодня

ViPNet Coordinator IG 4.5.2 (конец 2021 г.)

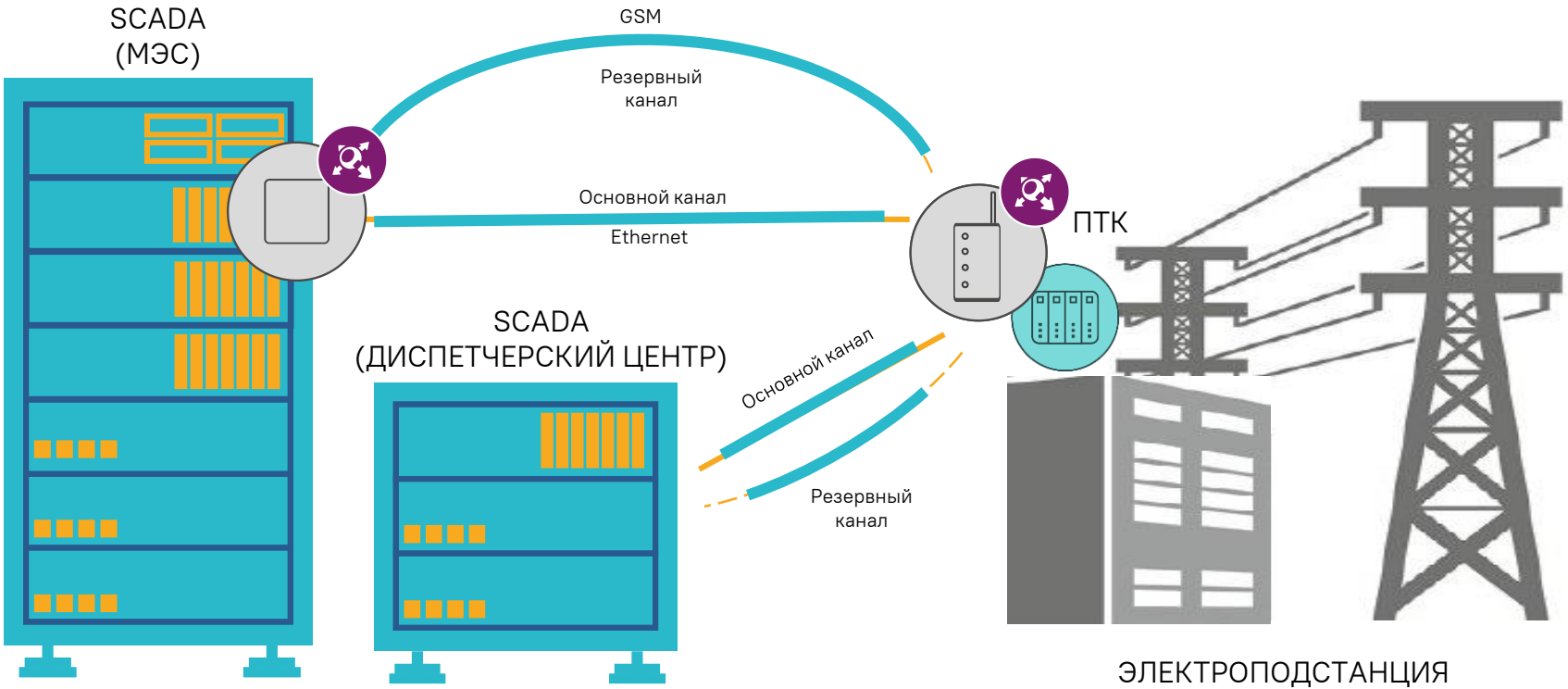
ViPNet Coordinator
IG10 I1
с версии 4.2.3

ViPNet Coordinator
IG100 I1
с версии 4.2.3

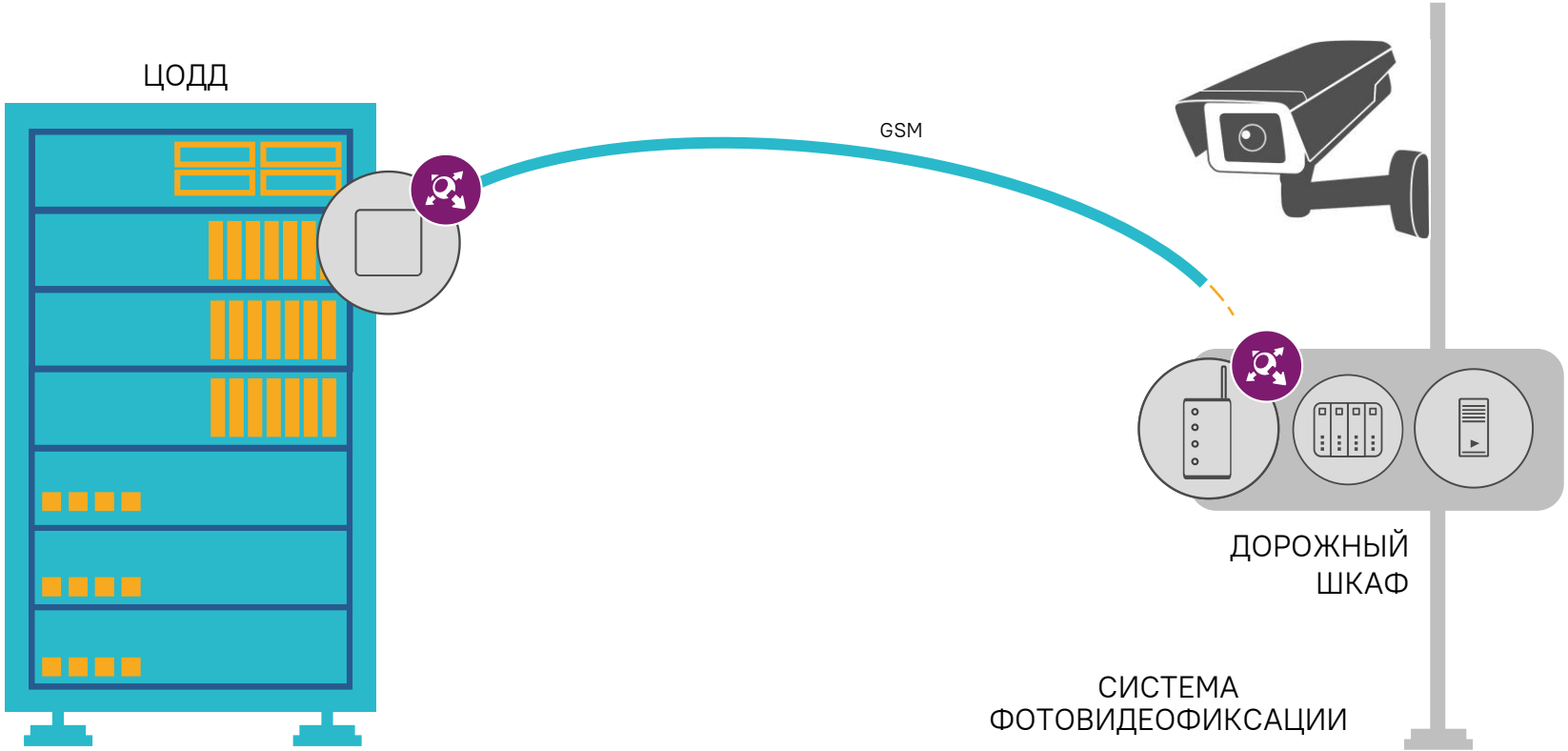
ViPNet Coordinator
IG10 I2
с версии 4.3.3

ViPNet Coordinator
IG100 I4
с версии 4.5.1

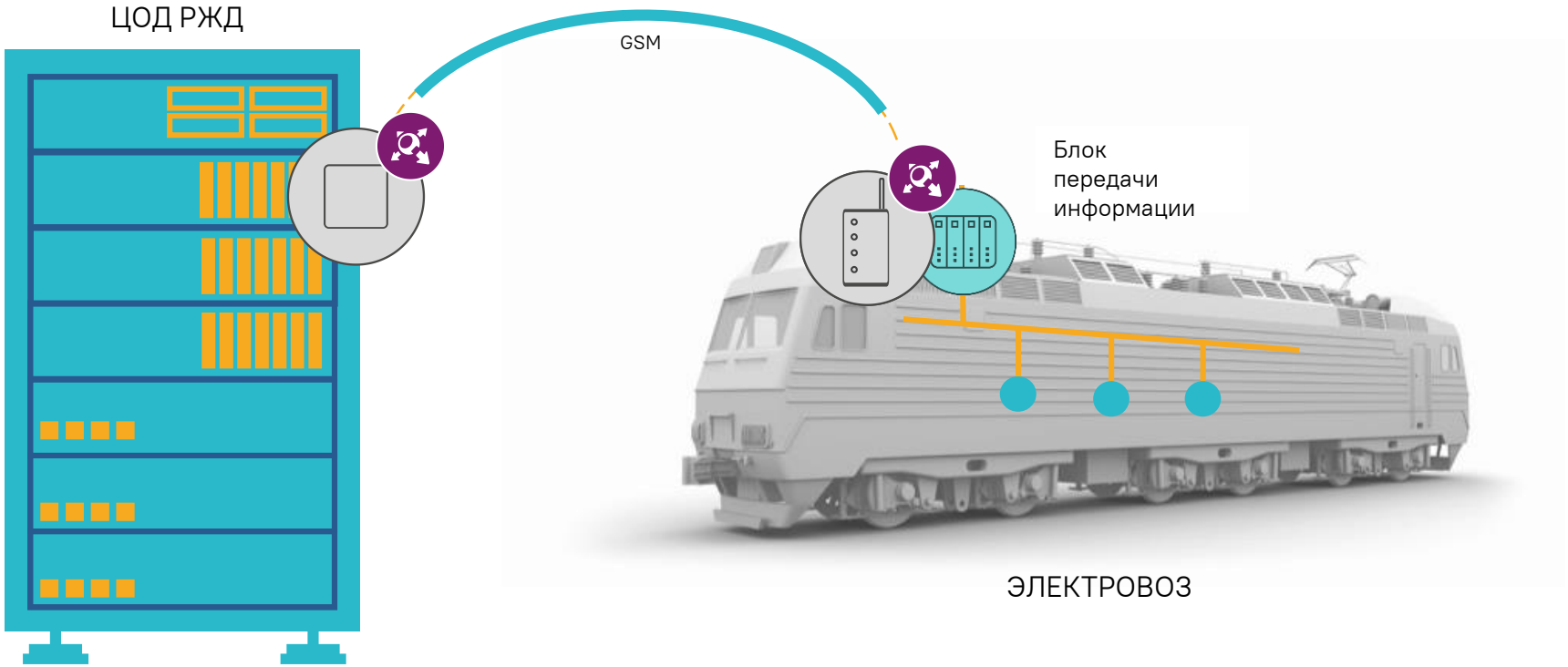
Защита каналов индустриальных ИС и КИИ с помощью ViPNet



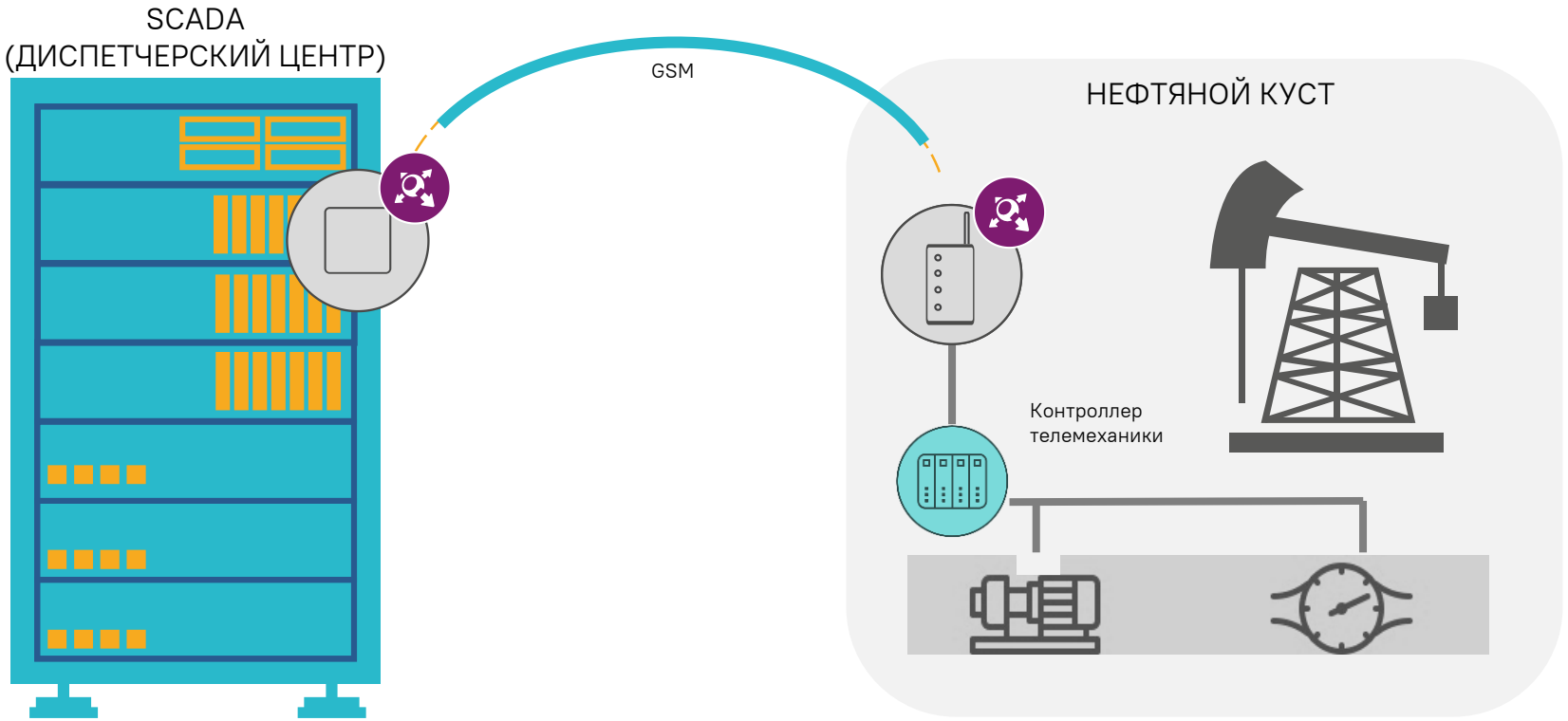
Защита каналов индустриальных ИС и КИИ с помощью ViPNet



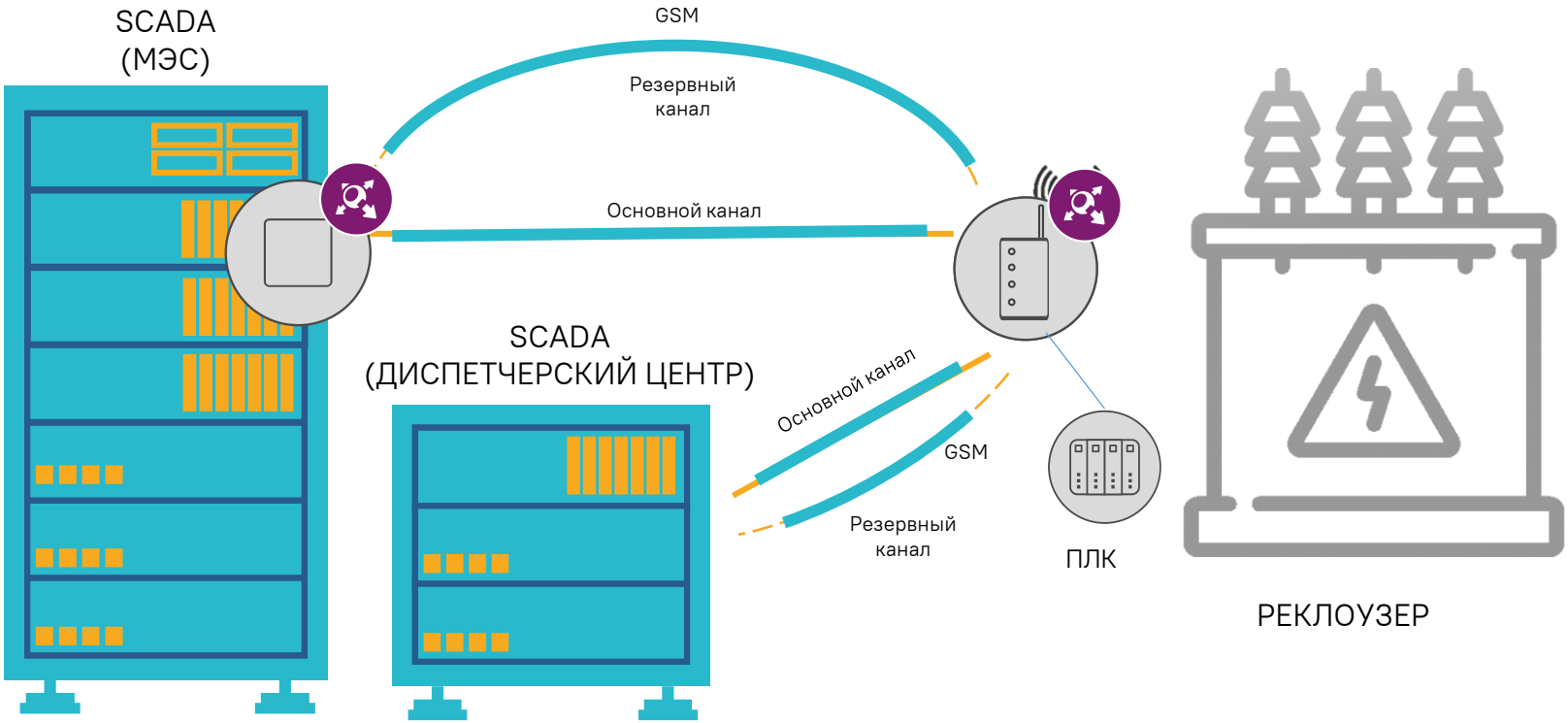
Защита каналов индустриальных ИС и КИИ с помощью ViPNet



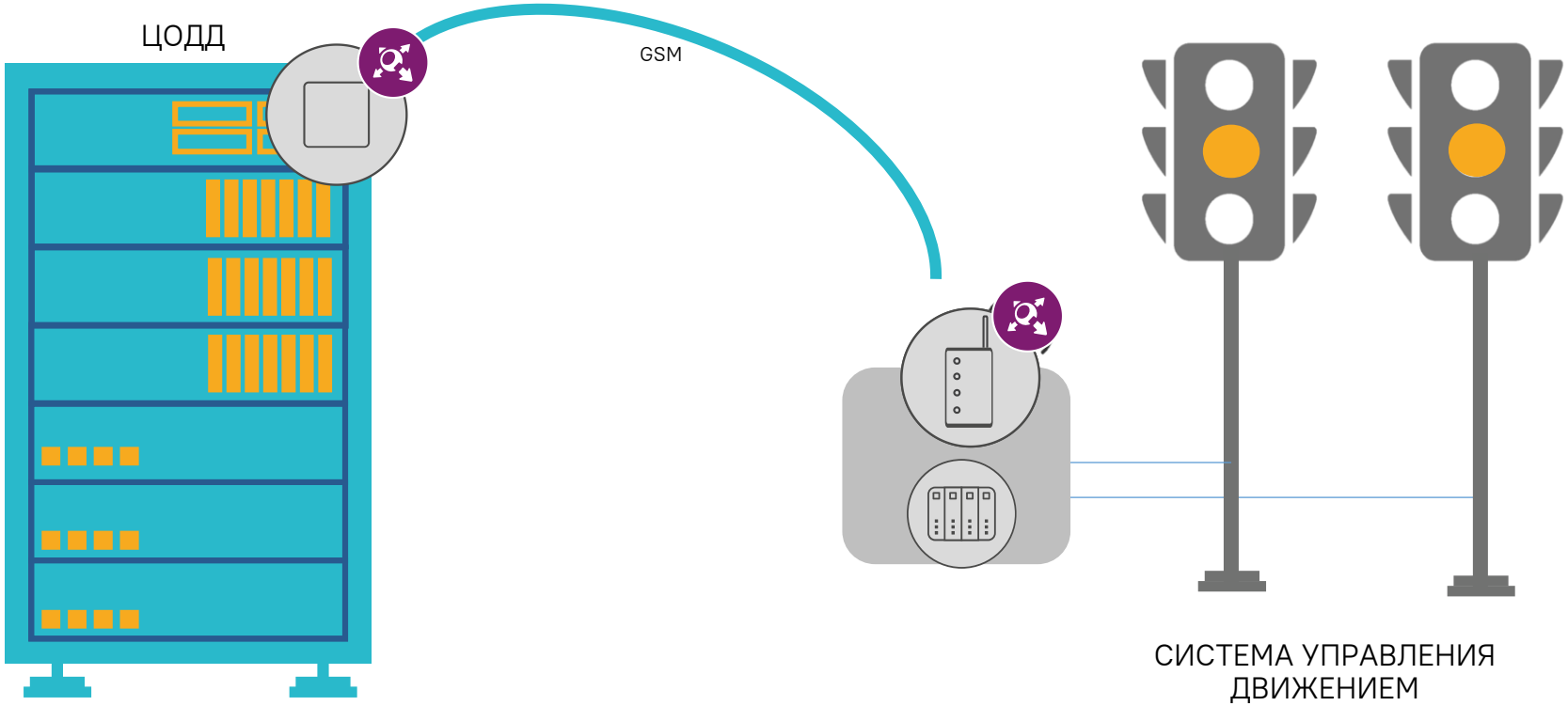
Защита каналов индустриальных ИС и КИИ с помощью ViPNet



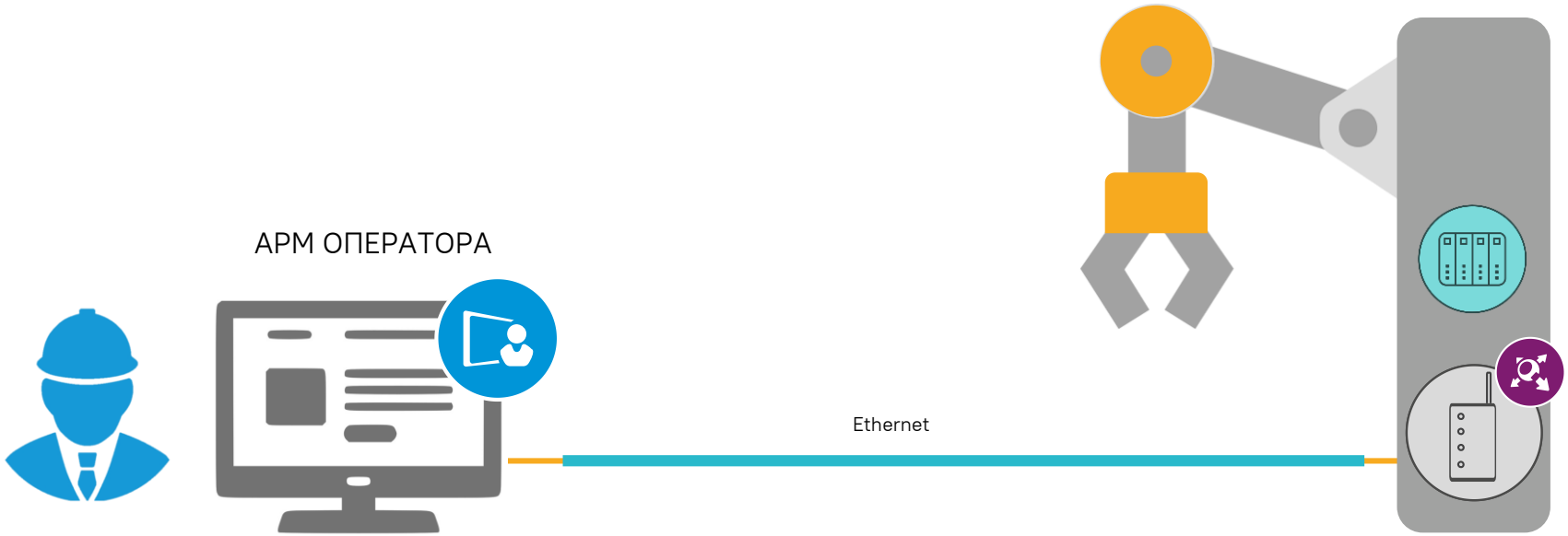
Защита каналов индустриальных ИС и КИИ с помощью ViPNet



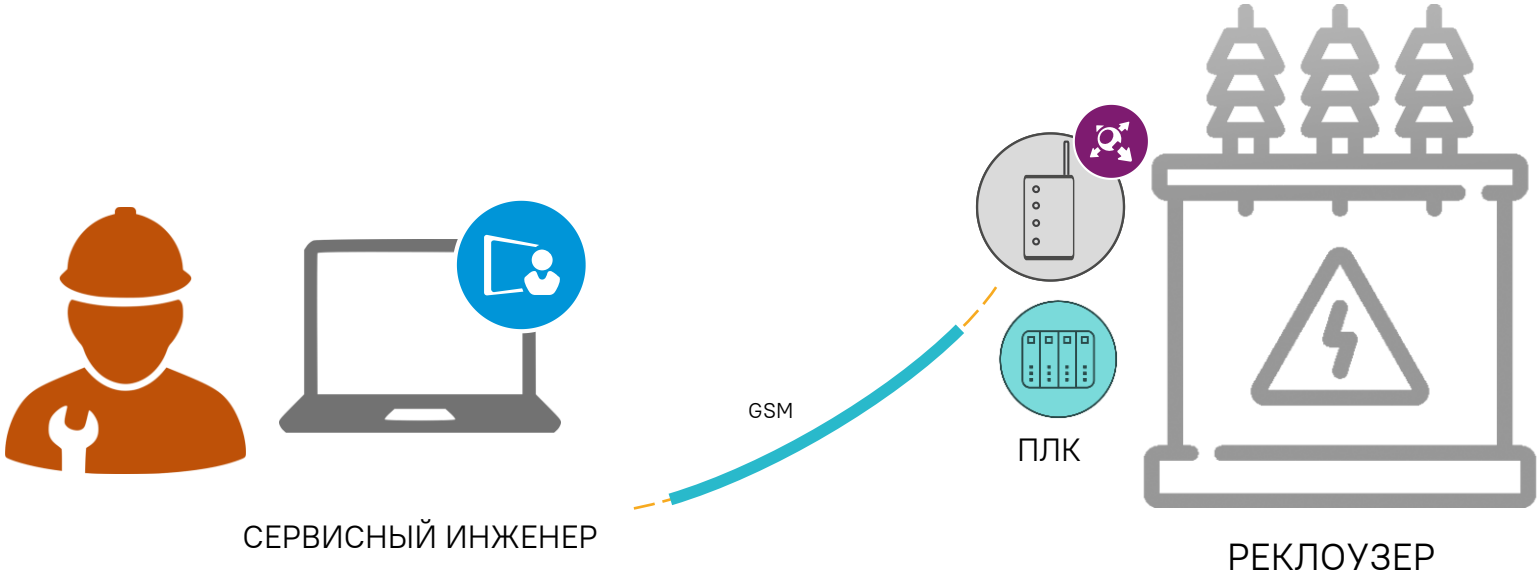
Защита каналов индустриальных ИС и КИИ с помощью ViPNet



Защита каналов индустриальных ИС и КИИ с помощью ViPNet



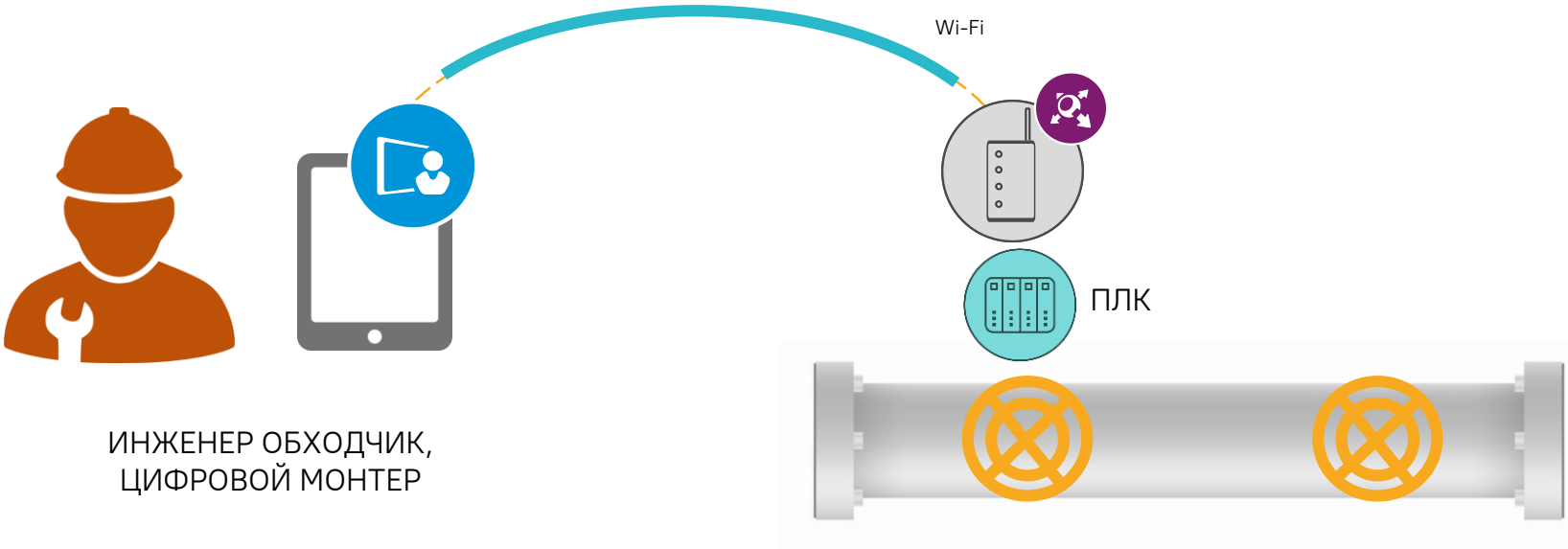
Защита каналов индустриальных ИС и КИИ с помощью ViPNet



Защита каналов индустриальных ИС и КИИ с помощью ViPNet

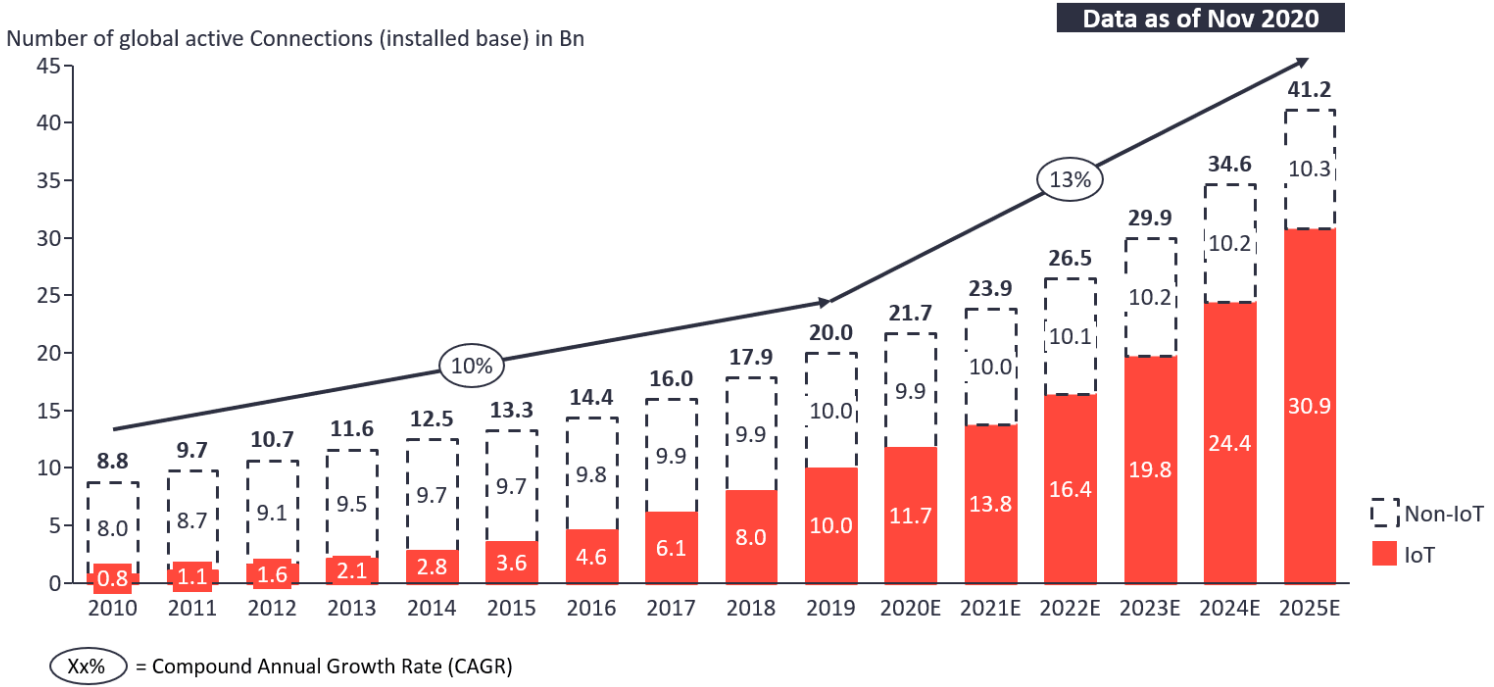
Защита каналов индустриальных ИС и КИИ с помощью ViPNet

ТОИР



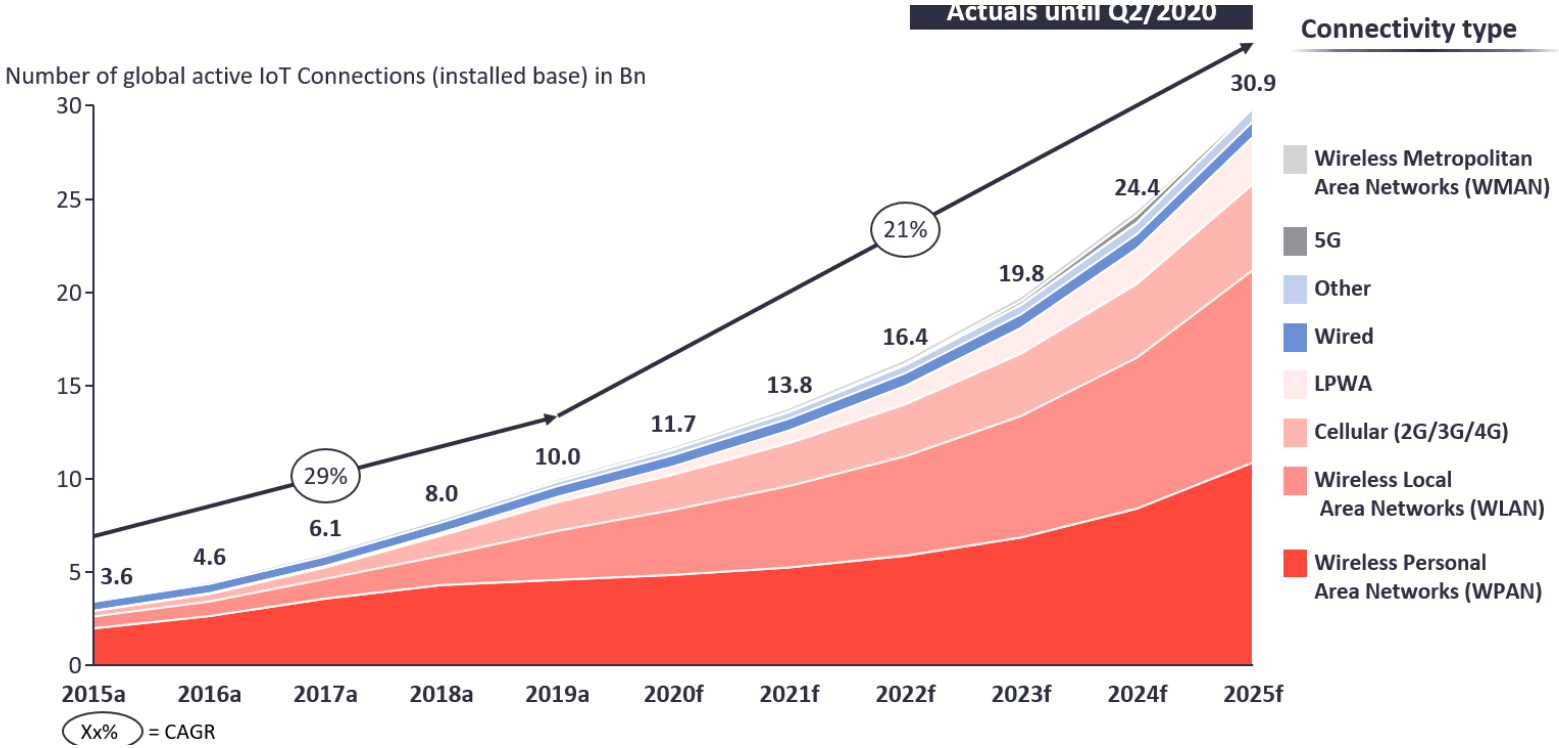

А что с подключенными устройствами и IoT?

Количество подключенных устройств (включая IoT)



SOURCE: https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/

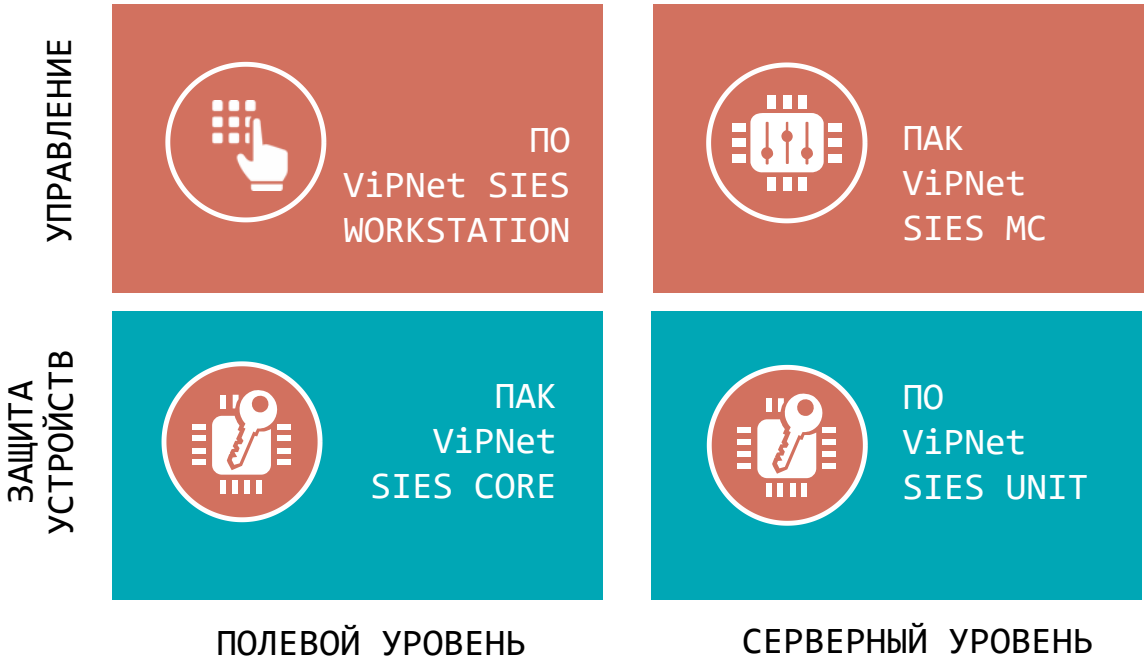
Количество подключенных устройств (включая IoT)



SOURCE: https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/


ViPNet SIES

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

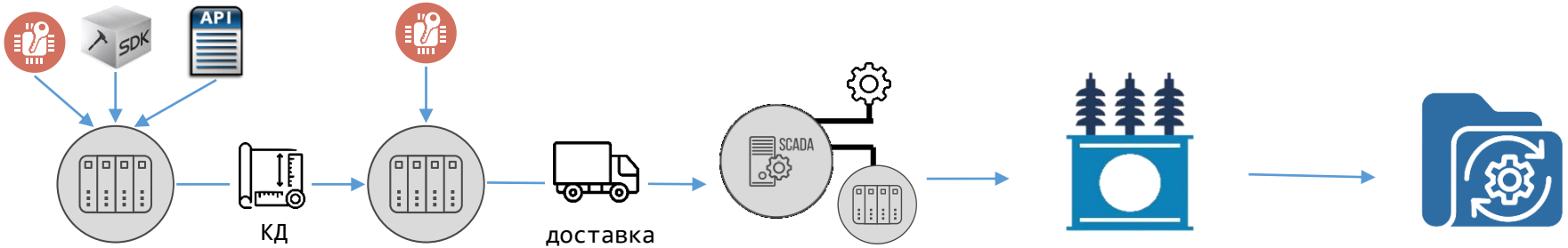
РАЗРАБОТКА УСТРОЙСТВА

ПРОИЗВОДСТВО УСТРОЙСТВА

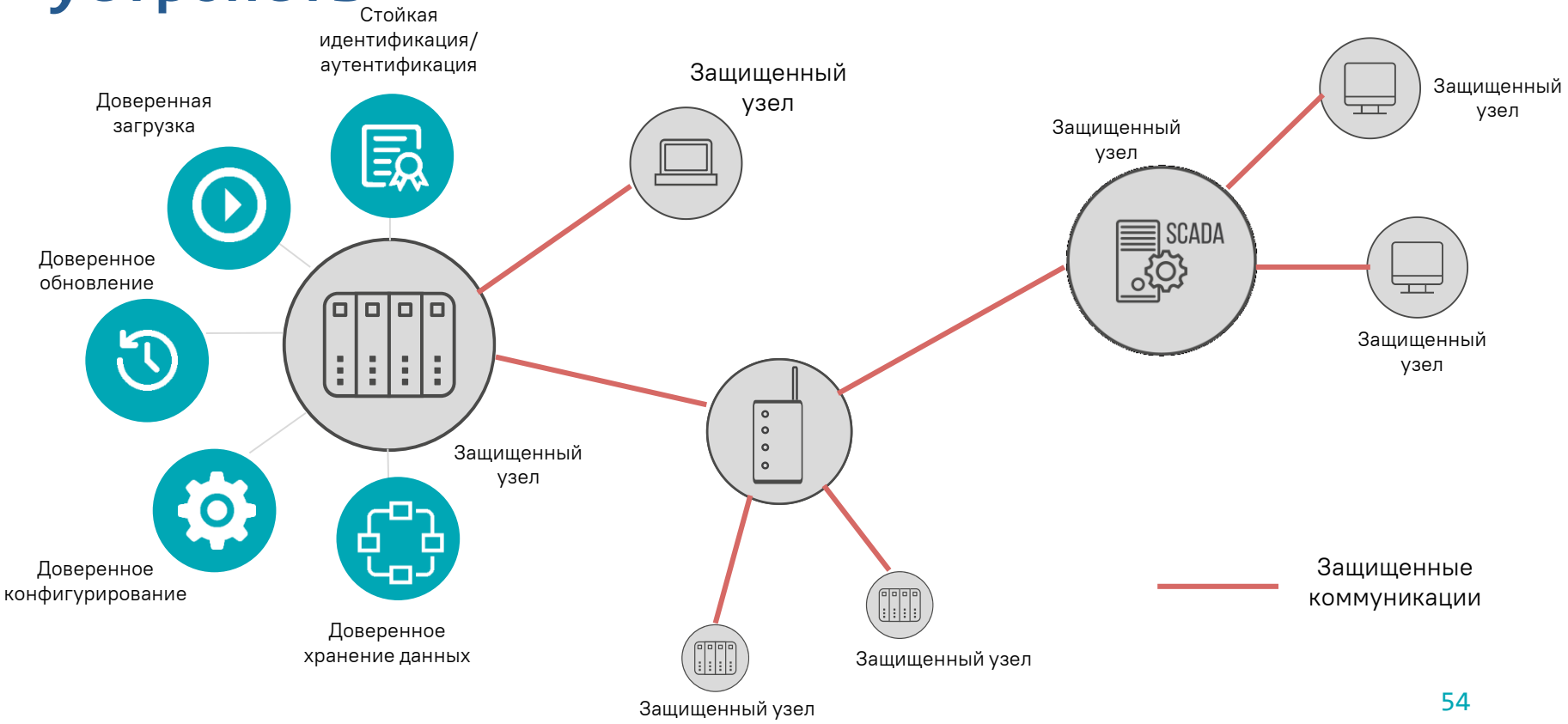
ВВОД В ЭКСПЛУАТАЦИЮ УСТРОЙСТВА

ЭКСПЛУАТАЦИЯ УСТРОЙСТВА

УПРАВЛЕНИЕ ОБНОВЛЕНИЕМ И КОНФИГУРАЦИЕЙ УСТРОЙСТВА



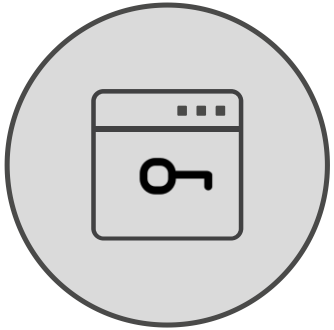
Концепция защиты конечных устройств



Компоненты решения ViPNet SIES

ViPNet SIES Core

- Форм-фактор: SOM-модуль, PCI Express® Full-Mini Card
- Интерфейс встраивания: UART, USB, SPI
- API: RATP + SIES API



ViPNet SIES Unit

- Форм-фактор: ПО
- ОС: Windows (32/64-разрядные) 8/8.1/10, Windows Server 2008 K2/2012/ 2012 K2/ 2016, Debian 9, Ubuntu 16, Ubuntu 18, Astra Linux Special Edition (Смоленск) 1.6
- API: RESTful API

Сертификаты соответствия по требованиям ФСБ России

ViPNet SIES Core 2.0.2:

- Сертификат по требованиям ФСБ России к СКЗИ класса КС3;

ViPNet SIES Core 2.2:

- Проведение контроля изменений относительно версии 2.0.2

SIES Unit в составе ViPNet PKI Client :

- Сертификат по требованиям ФСБ России к СКЗИ класса КС1 и КС3;

ViPNet SIES Unit 2.0:

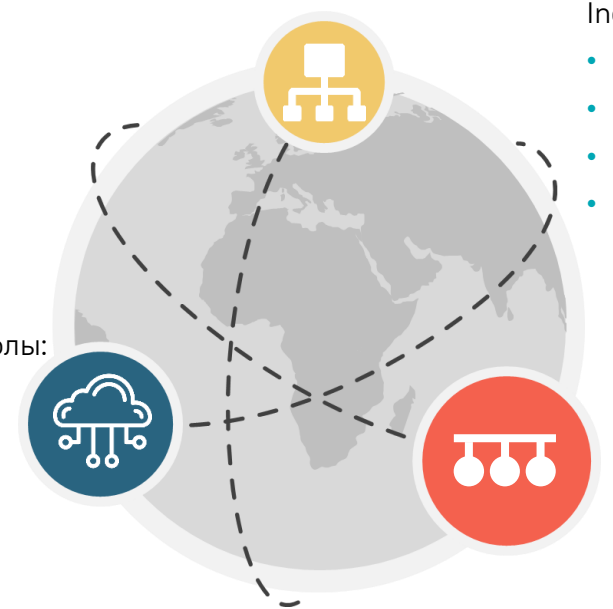
- Сертификация, ожидание Q3 2021 г.

Криптографические операции для защиты промышленных протоколов

- Зашифрование/расшифрование по CRISP (ГОСТ 34.12-2018, ГОСТ 34.13-2018, Р 1323565.1.029-2019)
- Создание имитовставки/ проверка имитовставки по CRISP (ГОСТ 34.12-2018, ГОСТ 34.13-2018, Р 1323565.1.029-2019)
- Создание ЭП/проверка ЭП в CMS (ГОСТ 34.10-2018)
- Зашифрование/ расшифрование в CMS (ГОСТ 28147-89)
- Создание хэш/проверка хэш (ГОСТ 34.11-2018)

IIoT – протоколы:

- NB-IoT
- LoRaWan
- XNB
- MQTT



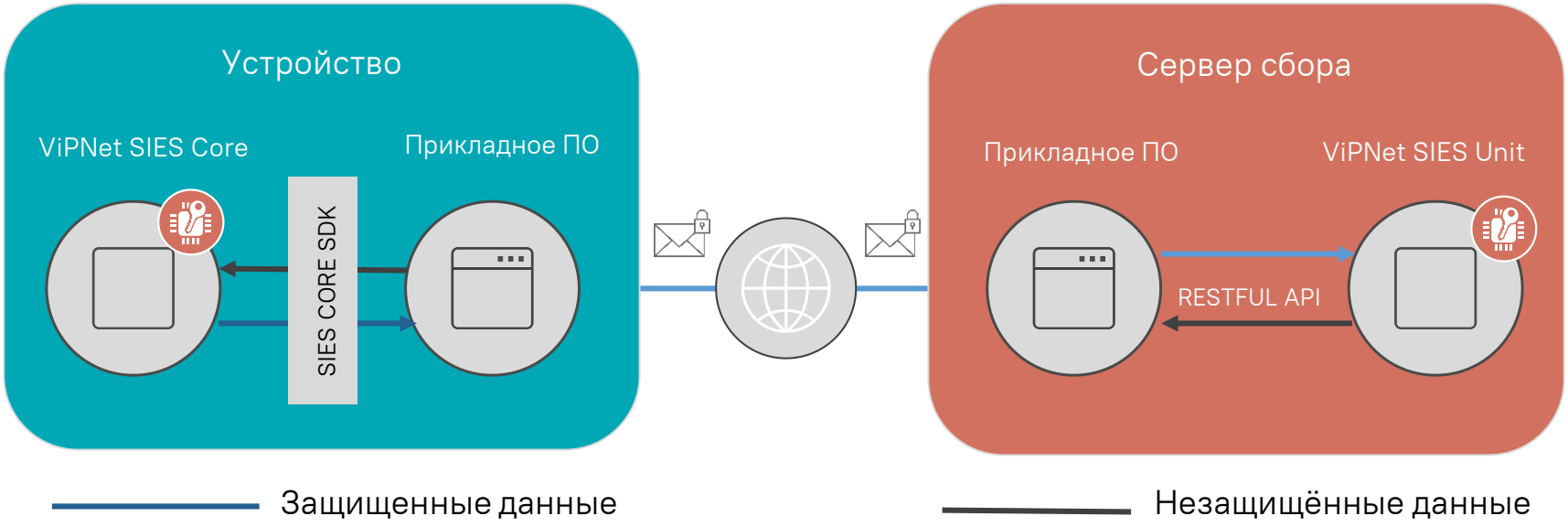
Industrial Ethernet:

- МЭК 60870-5-104
- Modbus TCP
- GOOSE
- СПОДЭС/СПОДУС

Fieldbus:

- МЭК 60870-5-101
- Modbus RTU

Решение ViPNet SIES



ИБ платформа на основе ViPNet SIES для АСУ и IIoT

Сертификаты соответствия по требованиям ФСБ России

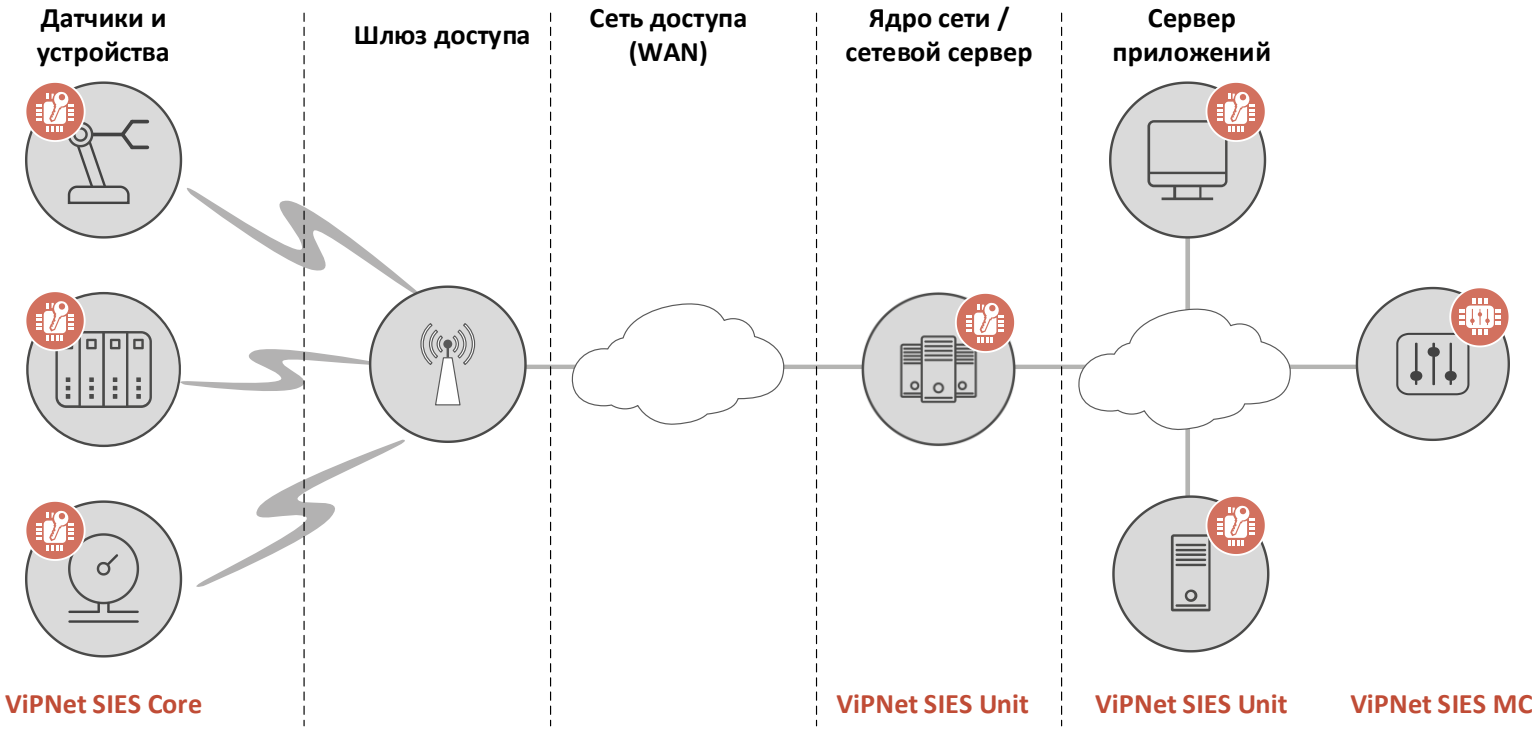
ViPNet SIES MC 2.0.2:

- Сертификат по требованиям ФСБ России к СКЗИ класса КС3;

ViPNet SIES MC 2.2:

- Проведение контроля изменений относительно версии 2.0.2

Защищенная IIoT-система



Спасибо за внимание!

Марина Сорокина

e-mail: marina.sorokina@infotecs.ru

Подписывайтесь на наши соцсети

@infotecs.ru

@vpninfotecs

@InfoTeCS_Moscow