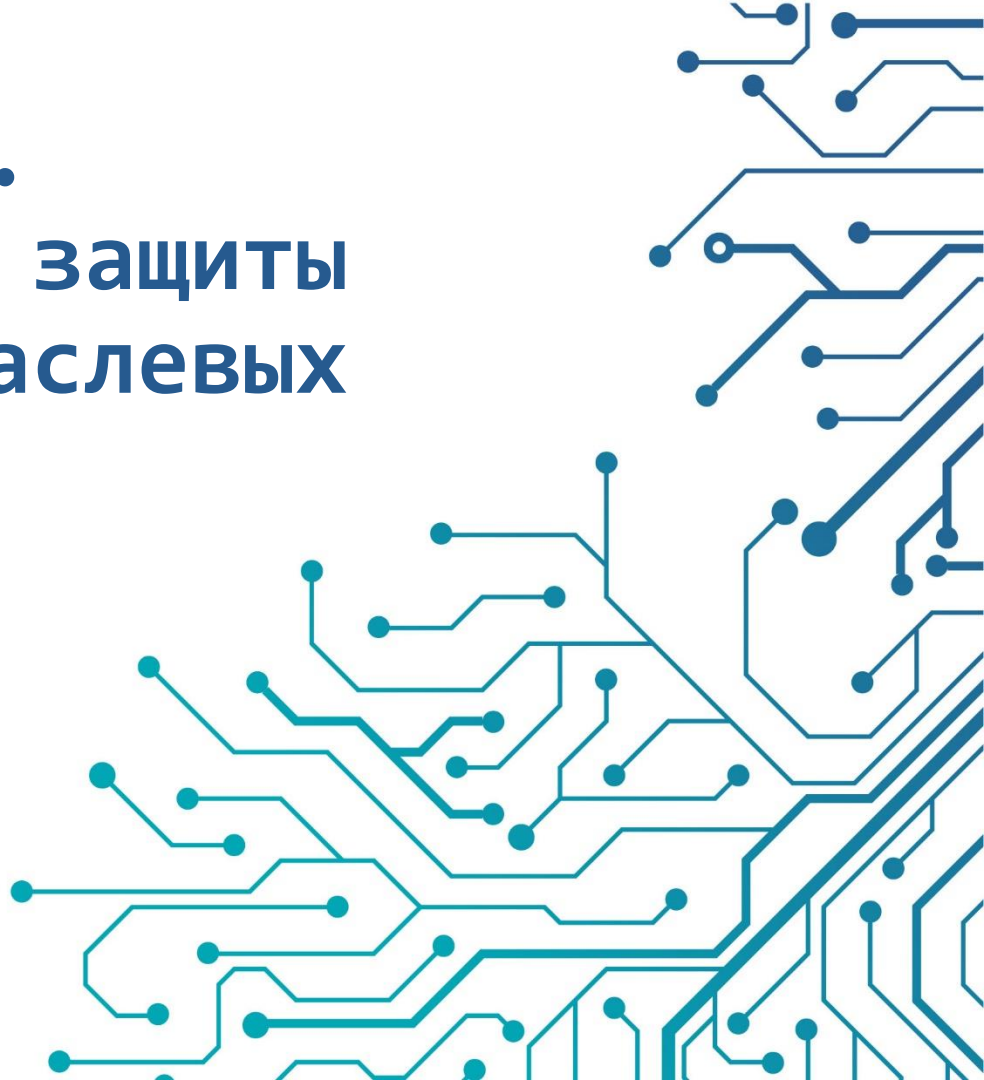


Безопасность КИИ. Опыт обеспечения защиты информации в отраслевых АСУ ТП

Сергей Лыдин

Руководитель направления
отдела клиентских проектов



ИнфоТеКС в цифрах



В **Топ-5**
компаний в сфере
защиты информации
в России



>10 млн
рабочих станций,
защищенных
продуктами VipNet



В **Топ-5**
компаний по количеству
патентов в области
цифровых технологий



>30
лет работы
на рынке ИБ



>60
Продуктов
для защиты
информации



12
офисов
по всей
стране

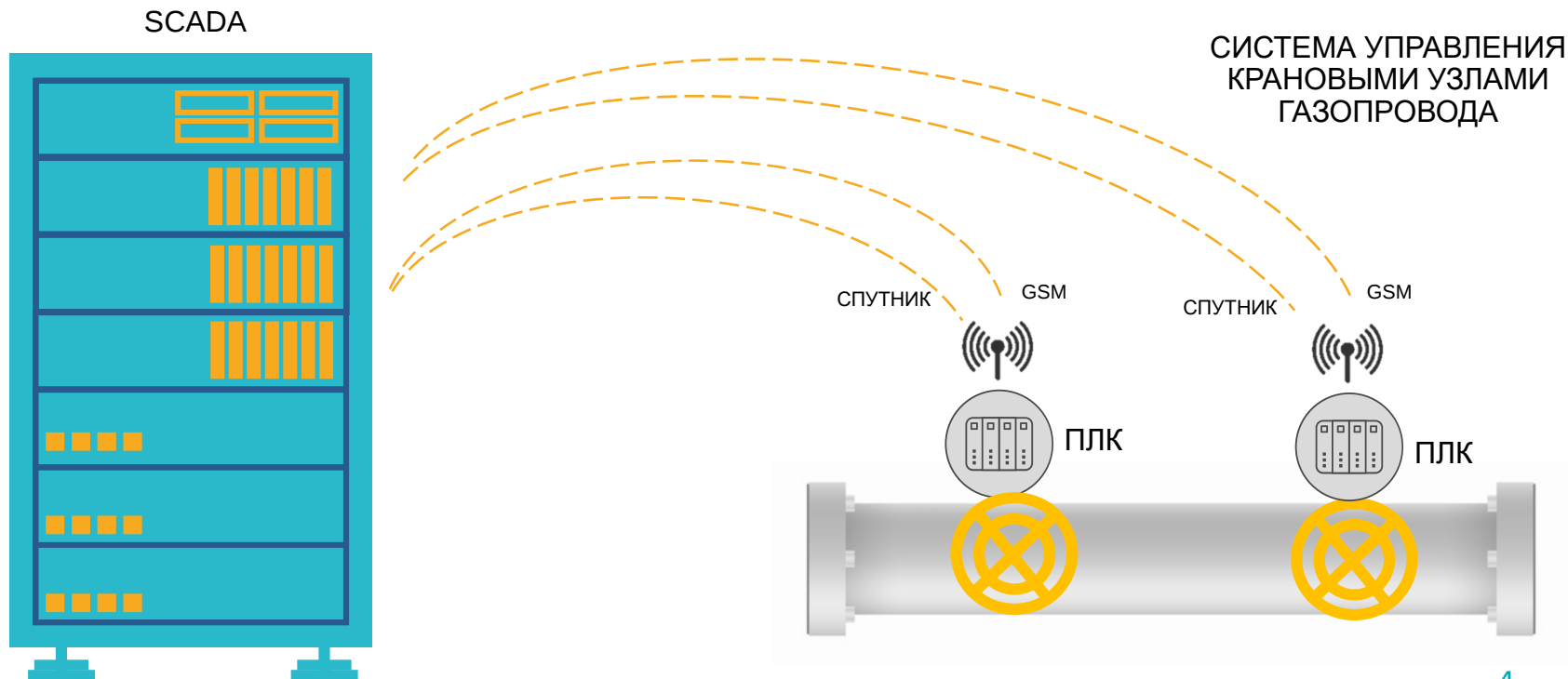


>1600
сотрудников

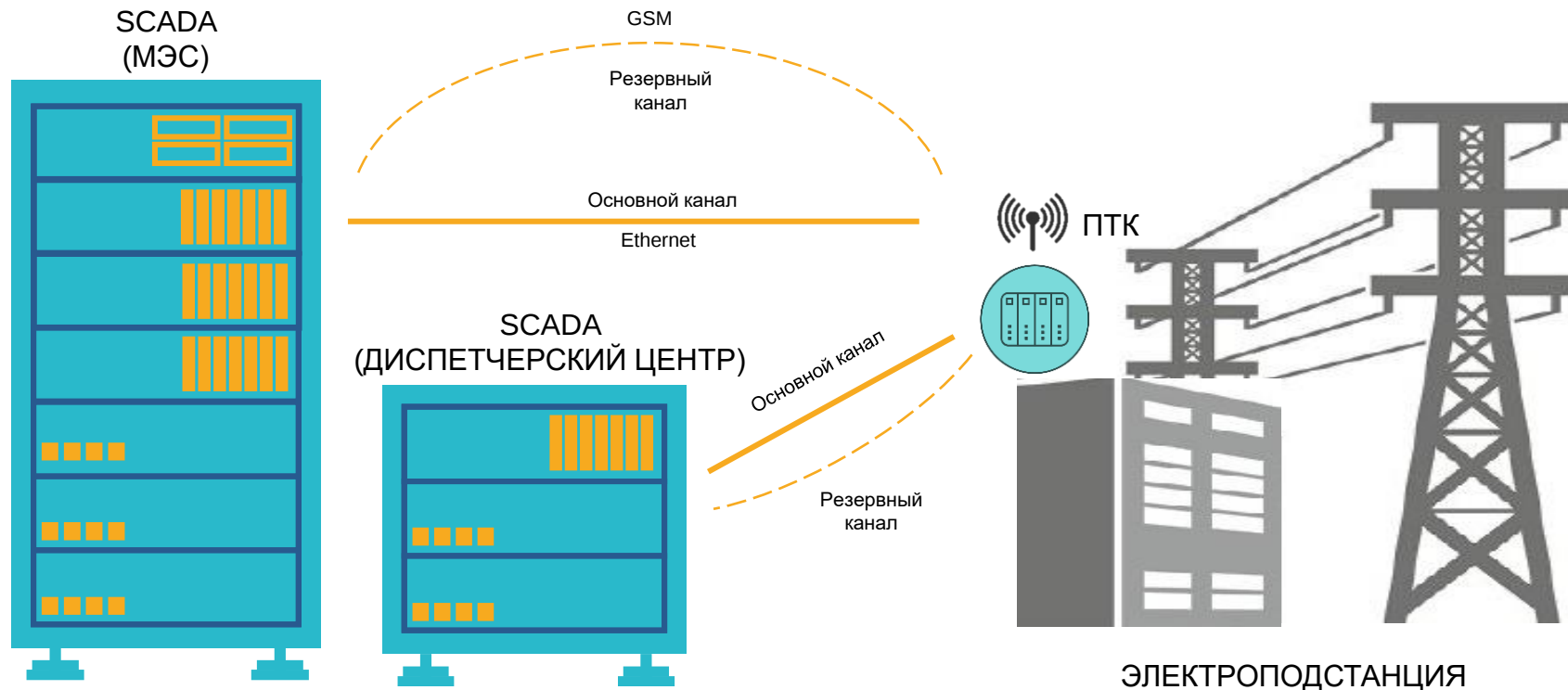
The background features a series of high-voltage power lines and pylons stretching across the frame. The entire image is overlaid with a semi-transparent blue filter. A network diagram is superimposed on the scene, consisting of numerous small blue dots connected by thin white lines, creating a web-like structure that suggests a complex system or data flow.

ЧТО ЗАЩИЩАТЬ?

Объекты защиты

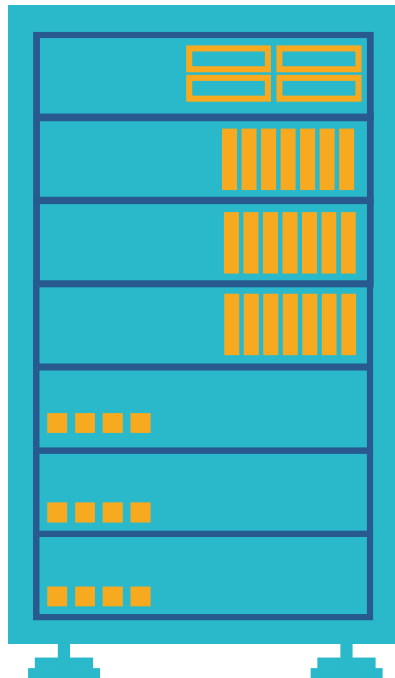


Объекты защиты



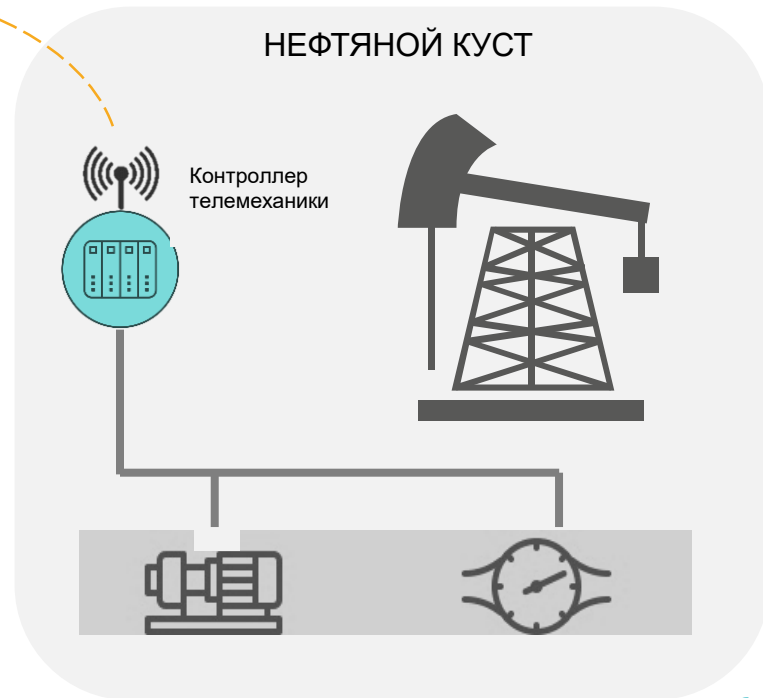
Объекты защиты

SCADA
(ДИСПЕТЧЕРСКИЙ ЦЕНТР)

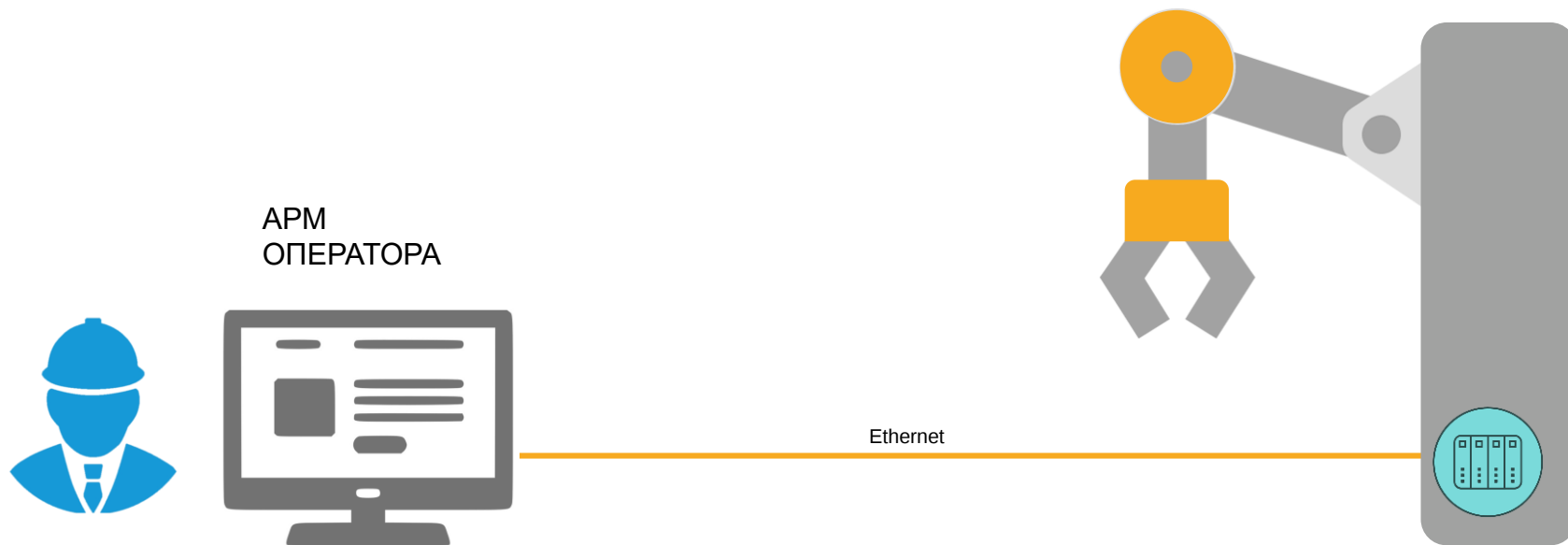


GSM

НЕФТЯНОЙ КУСТ

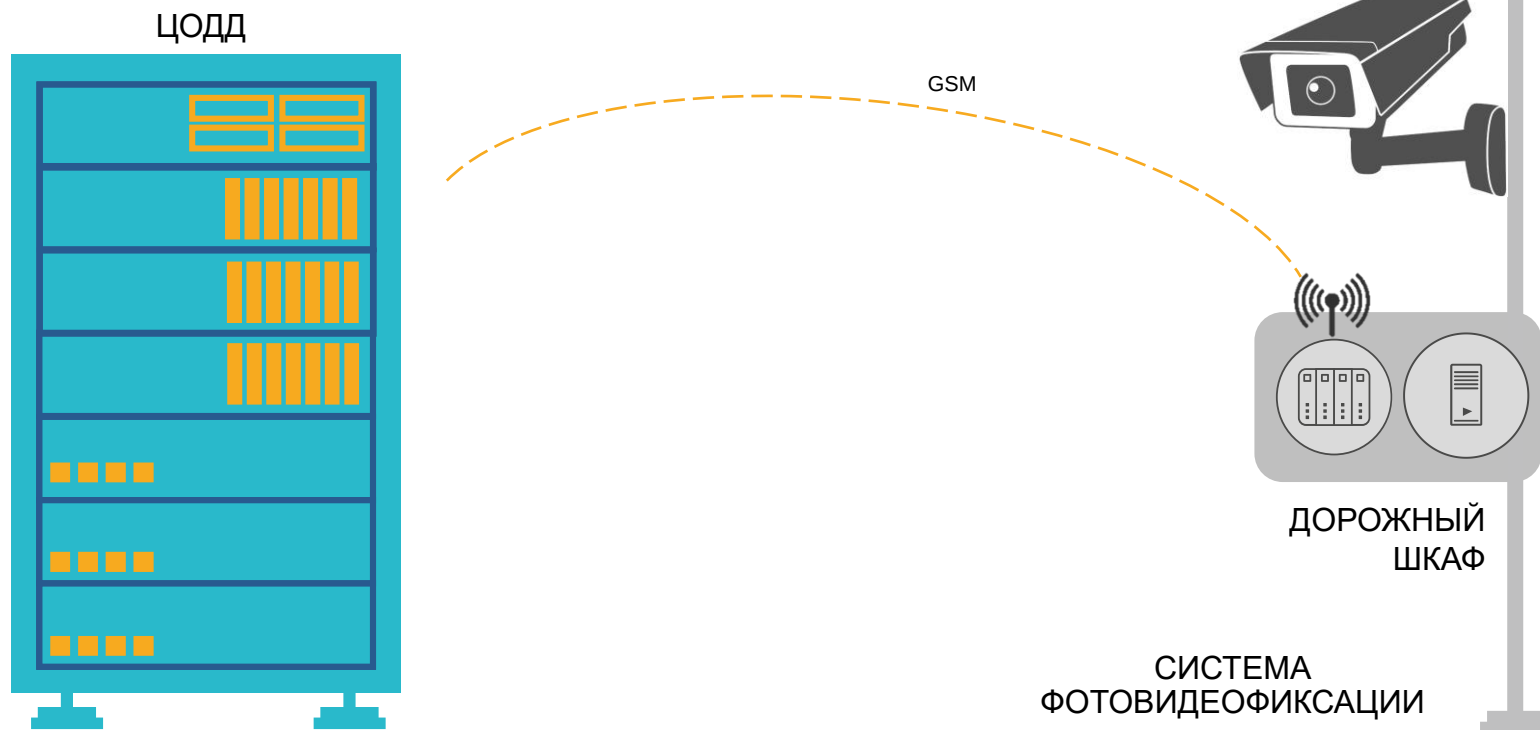


Объекты защиты

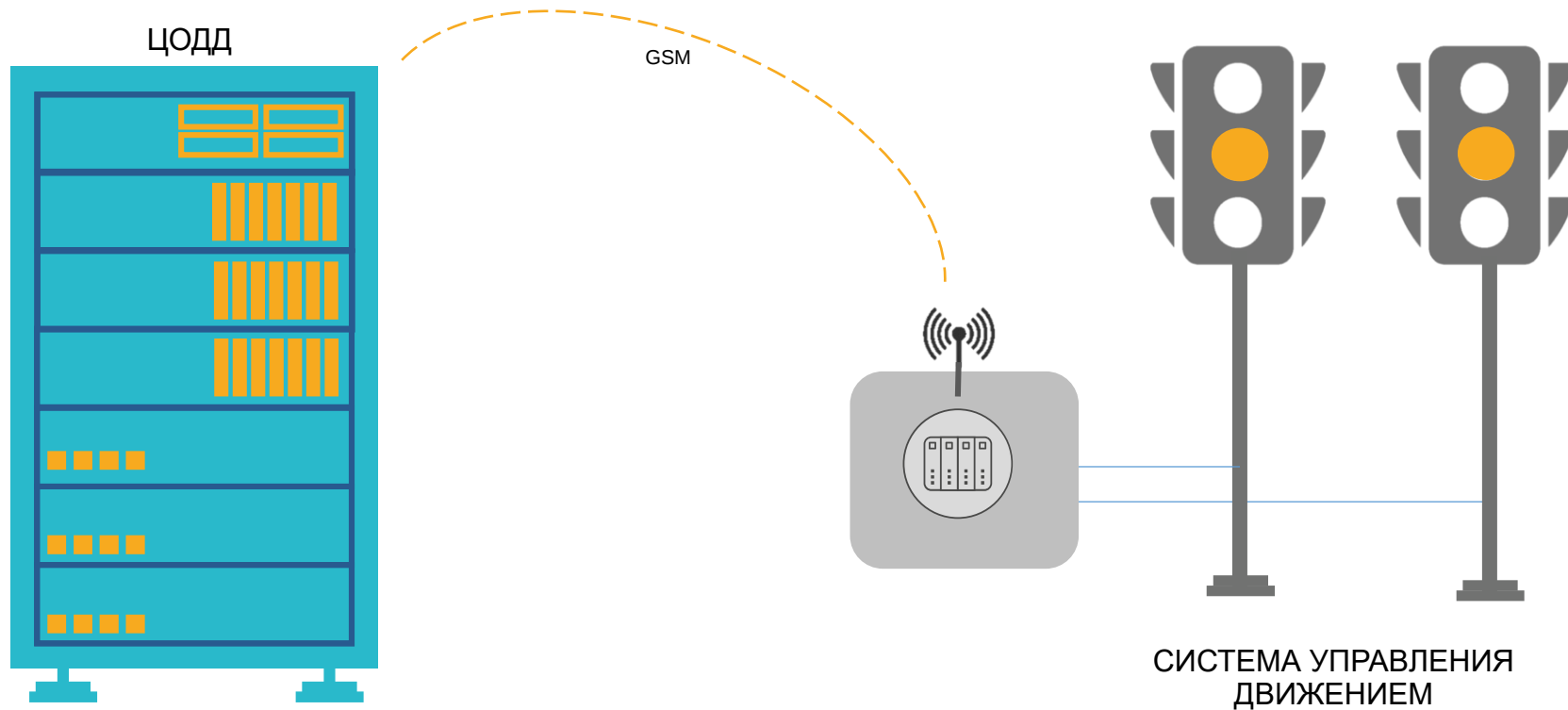


ПРОИЗВОДСТВЕННЫЕ
РОБОТЫ, СТАНКИ С ЧПУ

Объекты защиты



Объекты защиты



Объекты защиты



Объекты защиты



Основные угрозы безопасности информации АСУ ТП

- Несанкционированный доступ к данным (искажение данных)
- Перехват управления (навязывание команд, выведение из строя устройств)
- Подмена устройств (передача некорректных данных, нарушение стабильной работы сети устройств)
- Перепрошивка устройств (организация ботнетов, воздействие на объект управления)

Защищаемая информация АСУ ТП

Защищаемая информация	Возможности криптографии
• Данные (телеметрия, конфигурация и др.) • Команды управления • Программное обеспечение	• Целостность • Конфиденциальность • Аутентичность

Применение наложенных средств защиты информации

Наложённые СЗИ (СКЗИ)

Защита
периметра

Сегментирование

Защита каналов
связи

Применение встраиваемых средств защиты информации

Встраиваемые СЗИ (СКЗИ)

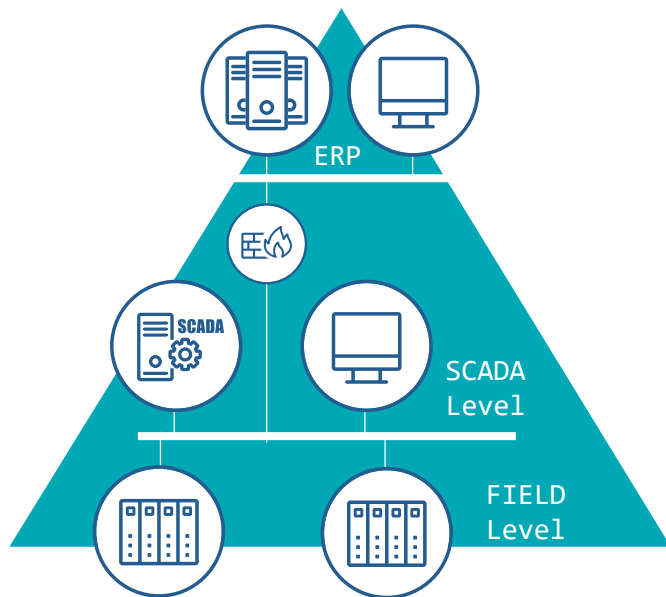
Аутентификация

Доверенная
загрузка

Доверенное
обновление

Доверенные
коммуникации

Изменение архитектуры АСУ ТП в процессе трансформации



Архитектура классической АСУ ТП



Архитектура Industry 4.0

Особенности и ограничения АСУ ТП

- Широкий диапазон объемов информационного обмена и допустимых задержек
- Ограниченные вычислительные ресурсы
- Специализированное ПО (прошивка), часто без операционной системы
- Автономное питание
- Многообразие протоколов и каналов связи
- Аппаратные исполнения для работы в сложных климатических условиях
- Малообслуживаемые условия эксплуатации

Особенности и ограничения АСУ ТП

- Высокая емкость отдельных сетей
- Продолжительный жизненный цикл устройств
- Разнообразие отраслевых стандартов и условий оценки соответствия
- Неопределенность периметра безопасности
- Строгие требования по стоимости для массовых устройств
- Слабые аппаратные возможности для реализации криптографических механизмов
- Достаточно закрытое сообщество компаний, способных разрабатывать прошивки для защищенных микроконтроллеров

The background features a photograph of several high-voltage electrical pylons and power lines stretching across a landscape. The entire image is overlaid with a semi-transparent blue filter. A network diagram, consisting of interconnected nodes and lines, is superimposed on the scene, with some nodes highlighted in a brighter blue. The text 'Законодательная база' is centered in the middle of the image in a white, sans-serif font.

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	Соккрытие 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

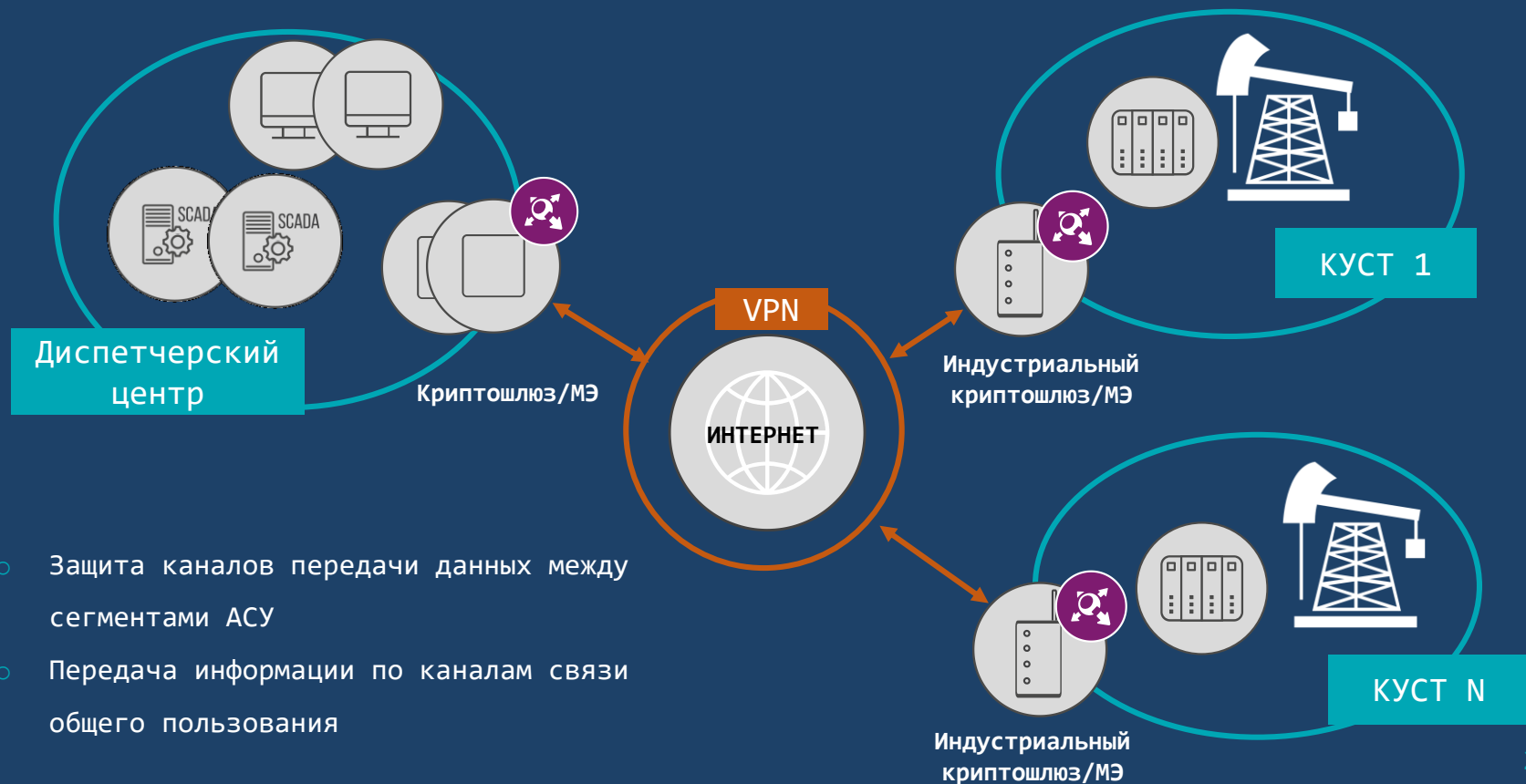
СЗИ, необходимые для подключения объекта КИИ к сетям связи общего пользования

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

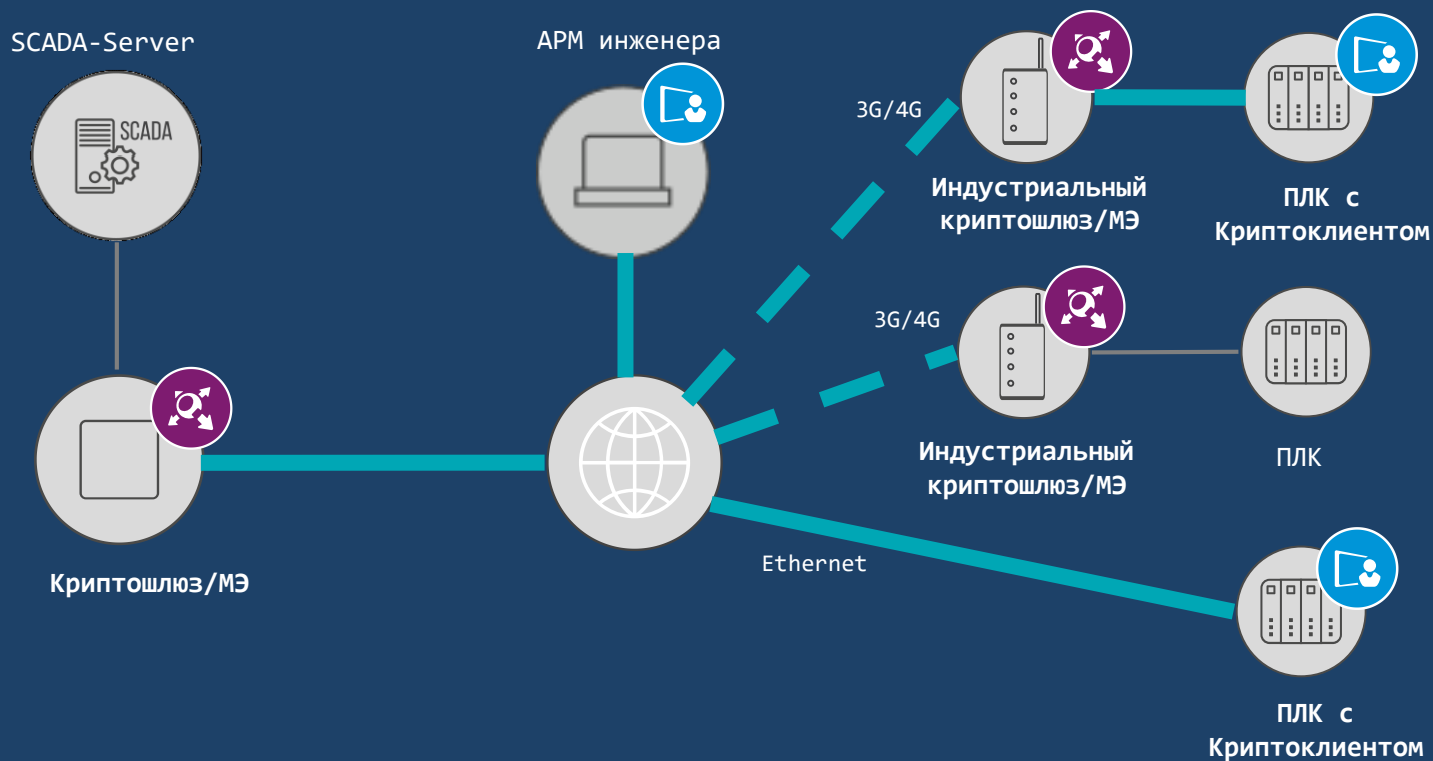
	1 КЗ	2 КЗ	3 КЗ
Межсетевой экран (ПАК) уровня сети (Тип А или Д)	+	+	+
Граничный маршрутизатор (ПАК)	+	+	+
• с сертификацией по требованиям безопасности информации	+	-	-
Средство антивирусной защиты	+	+	+
СКЗИ (например, криптошлюз)	+	+	+
Система обнаружения вторжений	+	+	

Типовые сценарии защиты информации в АСУ ТП

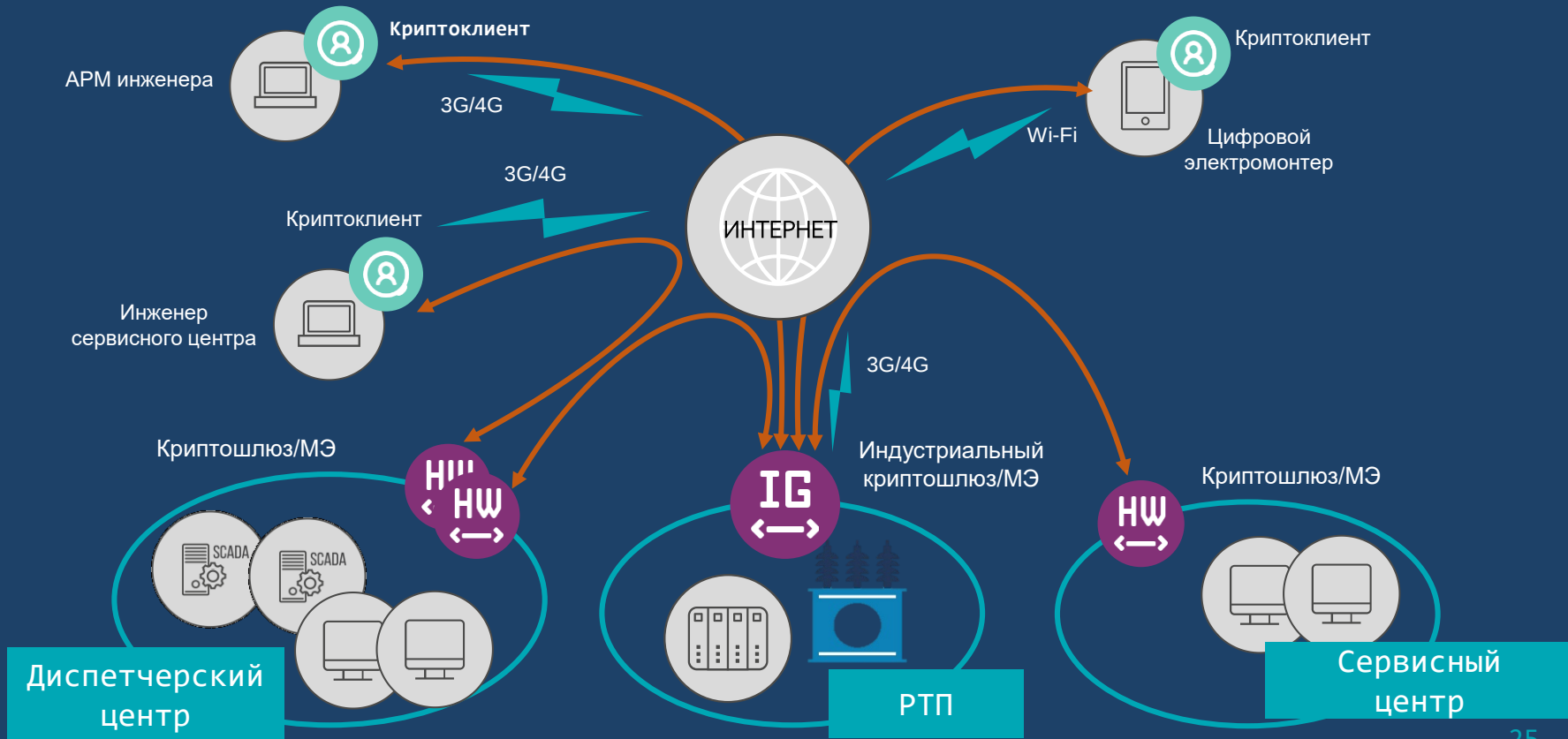
Защита каналов связи (добыча)



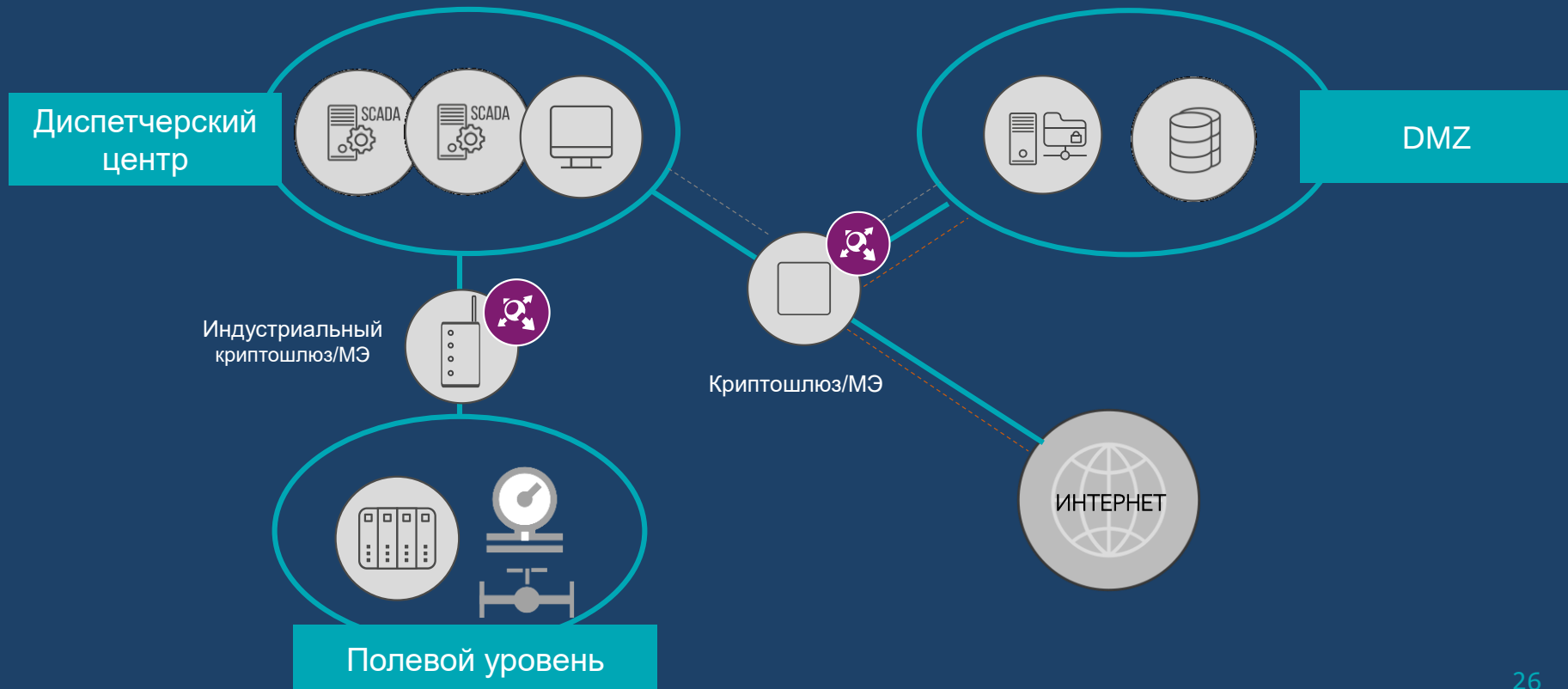
Защита каналов связи контроллеров



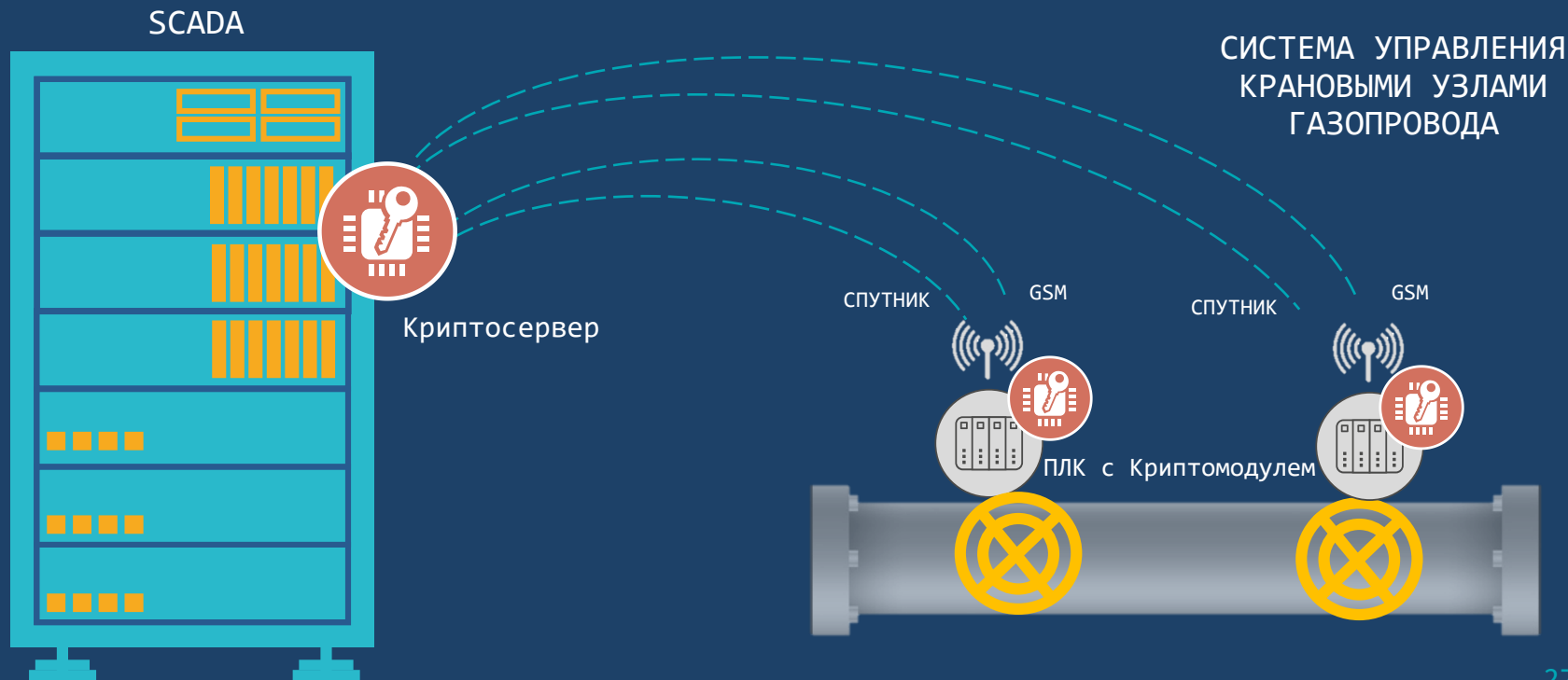
Защищенный удаленный доступ



Сегментирование сети



Защита каналов связи (транспортировка)

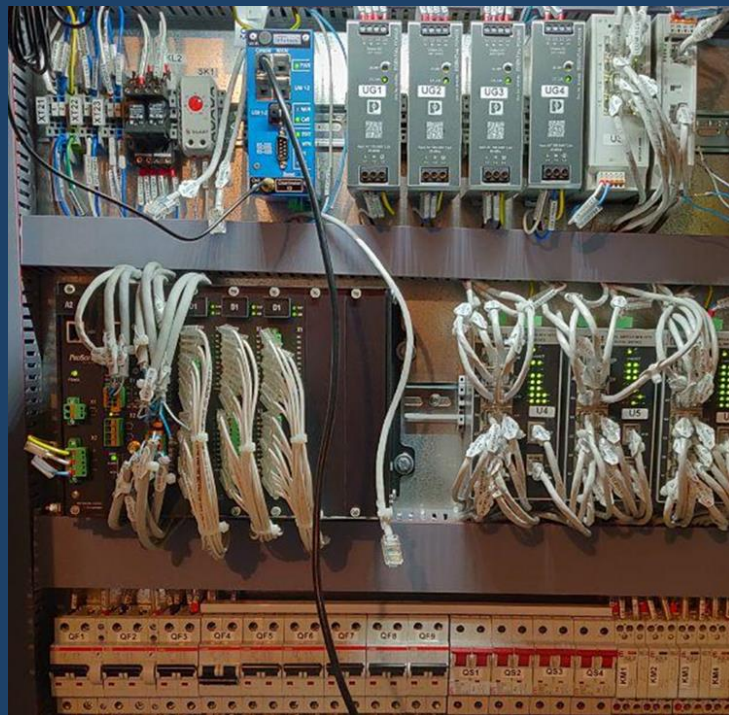


Индустриальный криптошлюз

VIPNet Coordinator IG (IG - Industrial Gateway)

Защищает:

- каналы связи:
 - между сегментами АСУ
 - при подключении к сетям связи общего пользования
- удаленный доступ, в том числе с мобильных устройств
- периметр и сегменты сети



Линейка шлюзов безопасности ViPNet Coordinator IG



ViPNet
 Coordinator
 IG10 I1



ViPNet
 Coordinator
 IG100 I1



ViPNet
 Coordinator
 IG10 I2



ViPNet
 Coordinator
 IG100 I4



ViPNet
 Coordinator
 IG100 I5

Сертифицированные исполнения

Ближайшие планы

Wi-Fi, GSM

Wi-Fi модуль:

- Клиент
- Точка доступа

GSM-модуль:

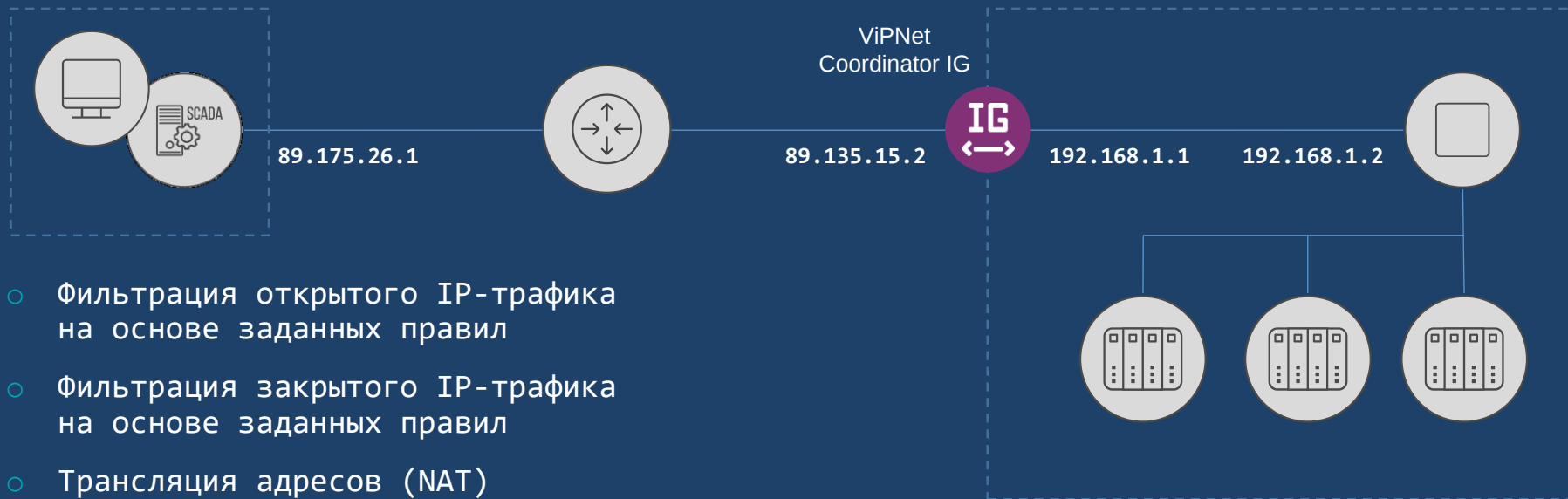
- 3G, LTE

В комплекты входят внешние антенны

Внимание! Wi-Fi и GSM-модули устанавливаются только на производстве!



Межсетевой экран



- Фильтрация открытого IP-трафика на основе заданных правил
- Фильтрация закрытого IP-трафика на основе заданных правил
- Трансляция адресов (NAT) для открытого IP-трафика
- Фильтрация на прикладном уровне трафика протоколов Modbus и МЭК 60870-5-104

ViPNet Coordinator IG



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) (продление от 06.2022г.)

Встраиваемые средства криптографической защиты информации



SECURITY FOR
INDUSTRIAL AND
EMBEDDED SOLUTIONS

ViPNet SIES

Встраиваемые криптографические
средства защиты информации:

- для устройств автоматизации
на всех уровнях АСУ
- для IIoT-устройств



Спасибо за внимание!

Сергей Лыдин

e-mail: sergey.lydin@infotecs.ru

Подписывайтесь на наши соцсети



https://vk.com/infotecs_news



https://t.me/infotecs_news