Безопасность КИИ применительно к ЦПС, соответствующих стандарту МЭК 61850

Причина перехода на ЦПС (МЭК 61850) ?

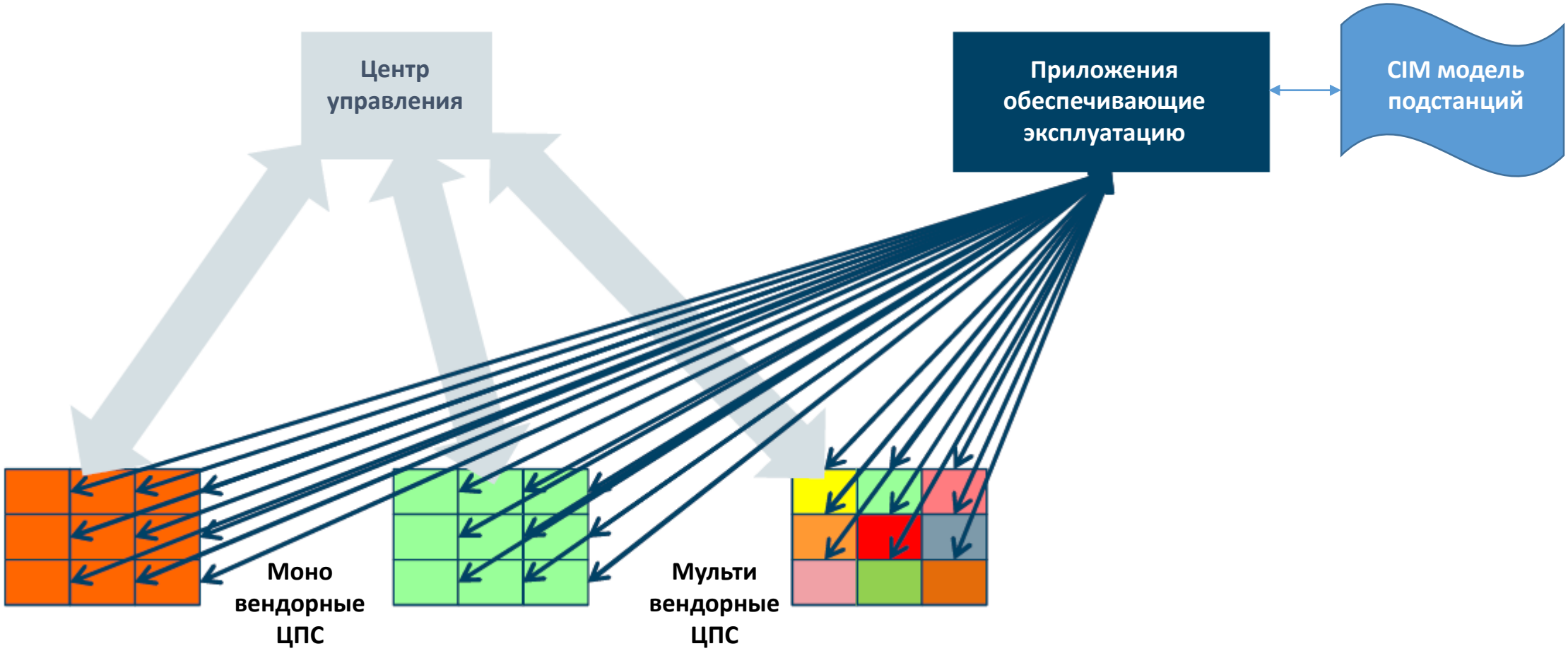
- Потому что это крутая, хайповая и модная технология
- Потому что рынок рано или поздно заставит меня это сделать
- Поскольку я оценил общие затраты эксплуатации объекта в долгосрочной перспективе и считаю более выгодным для компании, переход на МЭК 61850
- Другое

Попробуйте ответить, прежде всего себе, на вопрос по какой из вышеперечисленных причин сейчас переходят на ЦПС?

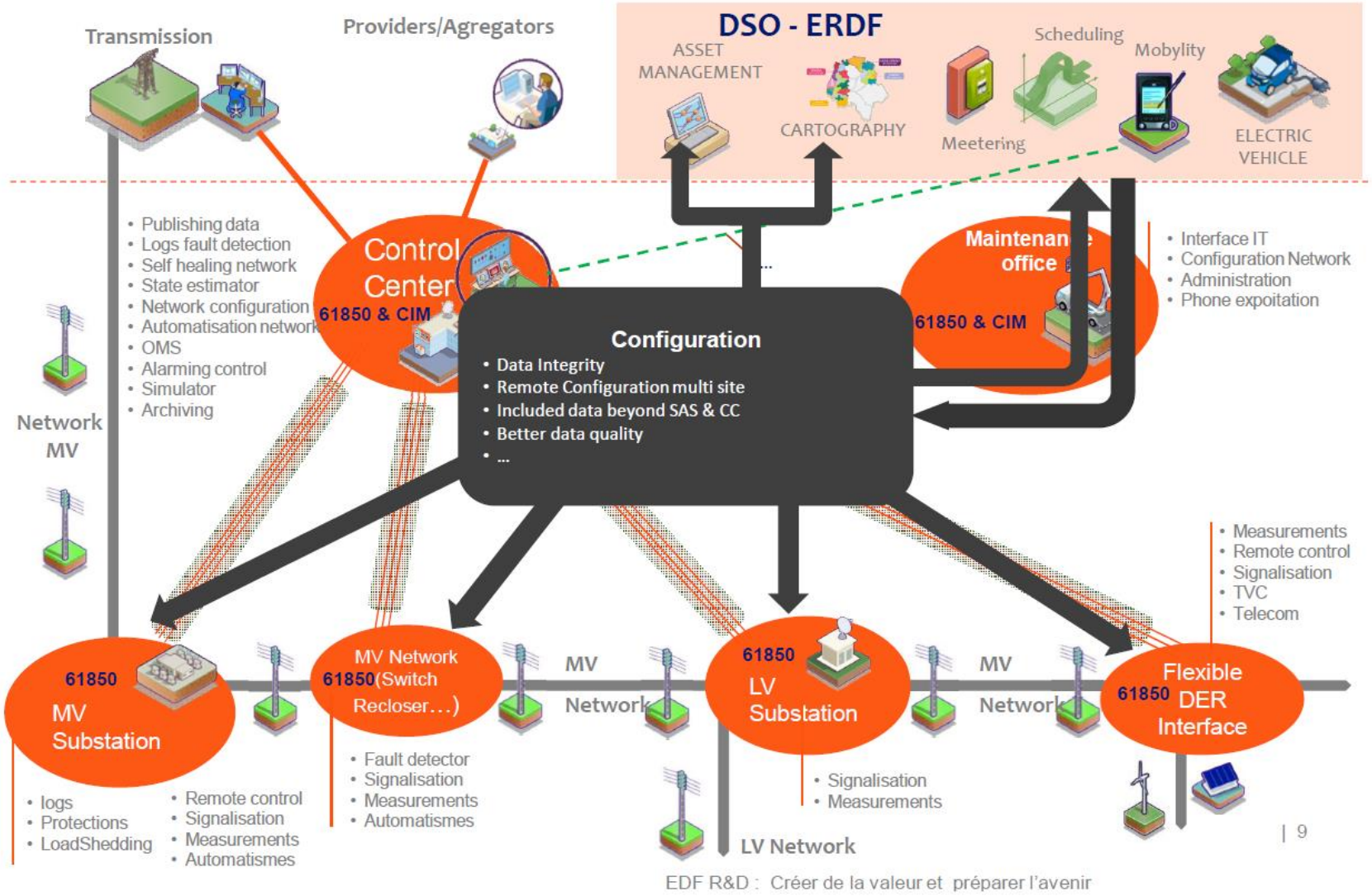
Тренды

- Переход на автоматическое удаленное управление подстанциями.
- РЗА цифровой подстанции станет одним из элементов удаленной системы управления, с постепенным выносом алгоритмов на более высокие уровни управления.
- Возврат инвестиций будет сильно зависеть от того, насколько эффективно будут использоваться растущий объем первичной информации с объекта
- Оптимизация управления инфраструктурой, а не работа каждой подстанции в отдельности, является реальным драйвером для развития ЦПС на базе МЭК 61850.

Структура информационных потоков



Пример интегрированной информационной инфраструктуры (EDF)



Актуальные вопросы

- Новые технологии и идеи требуют выстраивания новых процессов или наоборот?
- Методологии тестирования и проверки (против чего?).
- Значимое влияние на управление активами:
  - Требует появление новых навыков, ресурсов и обучения
  - Изменение подходов к обслуживанию и ресурсам.
- Контроль «аппетита к риску» - сбалансировать преимуществ и последствий:
  - Информационная безопасность
  - Увеличение уровня автоматизации и целостности сети.

Что необходимо определить на этапе внедрения ЦПС

- Соответствие требованиям ТЗ
- Обоснование надежности работы
- Информационная безопасность (соответствие Модели угроз)
- Безопасность управляющих взаимодействий
- Управление доступом третьих сторон
- Взаимодействие с устаревшими системами
- Методология эксплуатации

Уязвимость сетевой информационной инфраструктуры в электроэнергетике (международная статистика)

Более **60%** организаций рассматривают уровень существующих киберугроз для своих АСУ/АСУТП (ICS) как критический.

В более **70%** организаций, за прошедший год, произошел хотя бы один кибер инцидент.

Менее **25%** организаций полностью задокументировали информационную инфраструктуру АСУ и АСУТП

SANS 2016 State of ICS Security Survey

Вектора атак на критическую инфраструктуру

Удаленный сервисный (вендор) доступ

- Эксплуатация цифровых релейных терминалов требует доступа для удаленного сервисного обслуживания в случае текущих работ или аварий, точка внешнего доступа, часто находится не только за пределами корпоративной сети компании.

Через контроллеры, установленные на объектах

- Используют маршрутизируемые протоколы типа МЭК 60870-5-104, МЭК 61850 и т п.

Корпоративная сеть – критическая инфраструктура

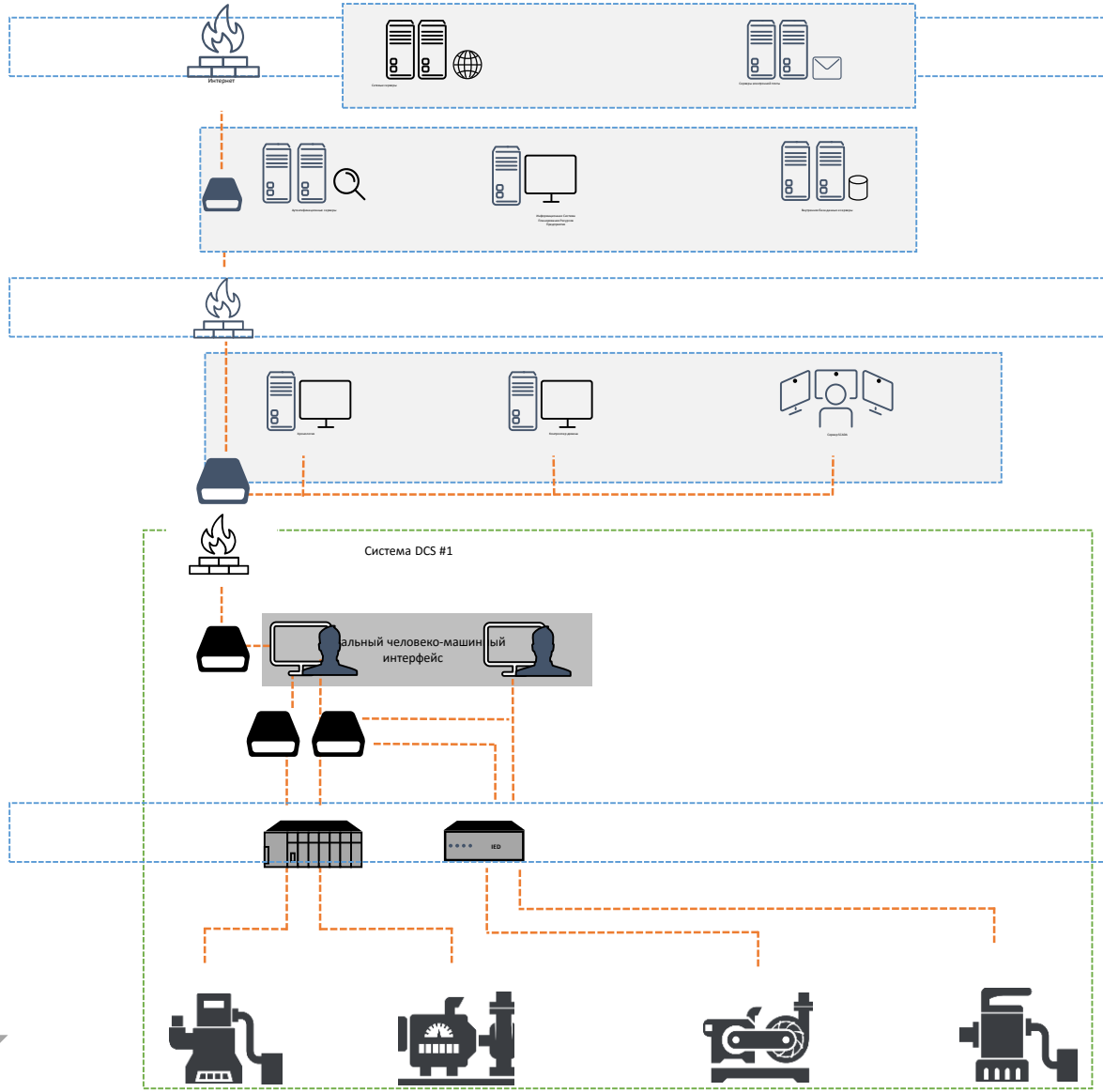
- Корпоративная сеть является более динамичной и чаще подвергается изменениям, в отличии от ICS / SCADA сетей, корпоративные сети являются более уязвимыми.

Комплексный многоуровневый набор угроз, сочетающий вектора атак на ИТ, АСУ и АСУТП

Целевая атака
предназначенная для использования офисной сети, с целью проникновения в промышленную сеть

MalOT
программное обеспечение, предназначенное для использования компонентов АСУ для доступа к АСУТП

M2M
использование сети АСУТП для атаки, путем скрытого подключения несанкционированных устройств, подмены прошивок, подмены данных



Корпоративная сеть компании

Офисные информационные технологии (ИТ)

Промышленная сеть (уровень АСУ)

Автоматизированные системы управления производством (АСУ)

Промышленная сеть (объект)

Автоматизированные системы управления технологическим процессом (АСУТП)

Криптография

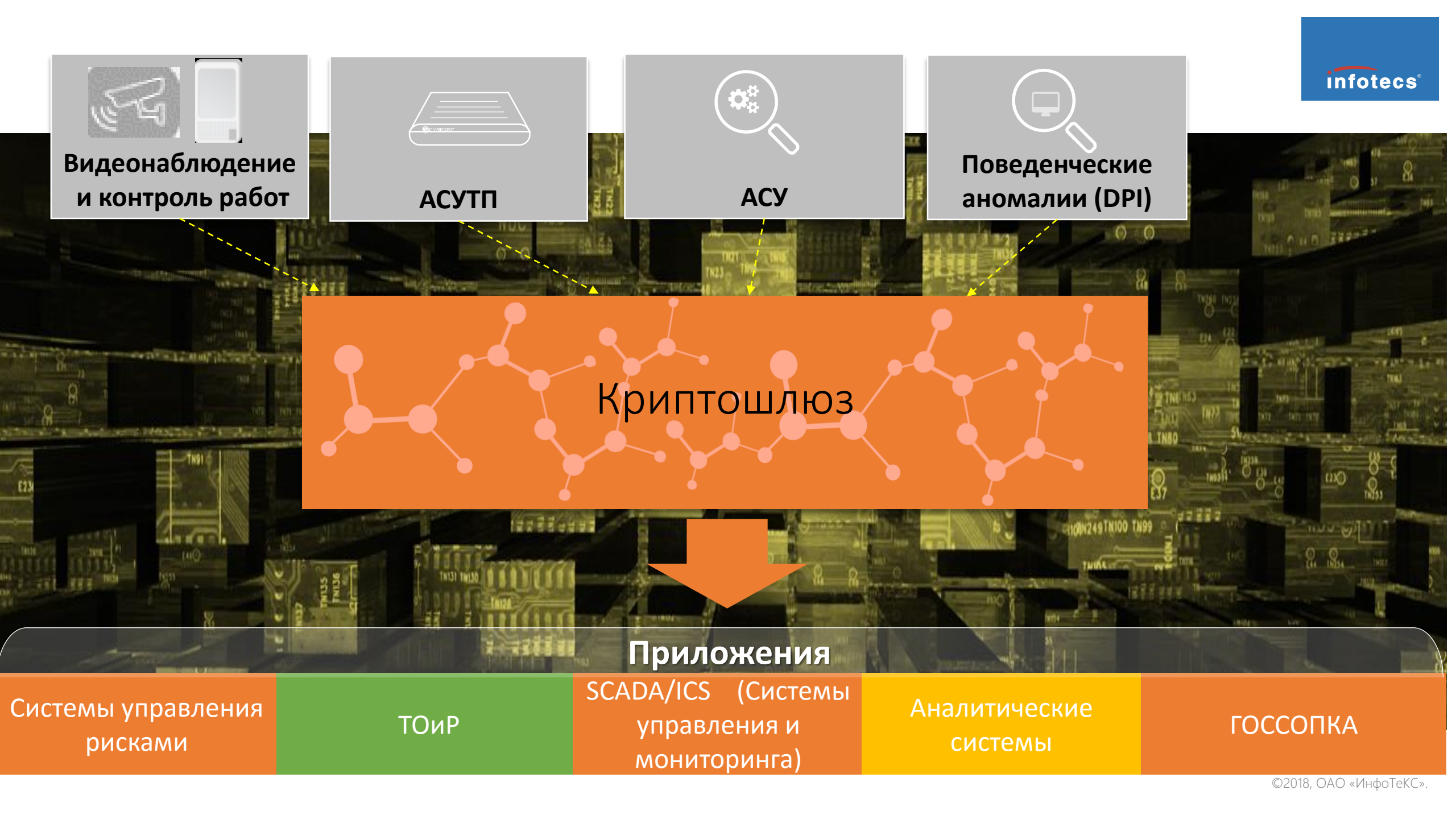
- Обеспечение связности по защищенному каналу распределенных локальных сетей, компьютеров и промышленного оборудования, в том числе и через публичные сети и другие не доверенные каналы связи.

Преимущества:

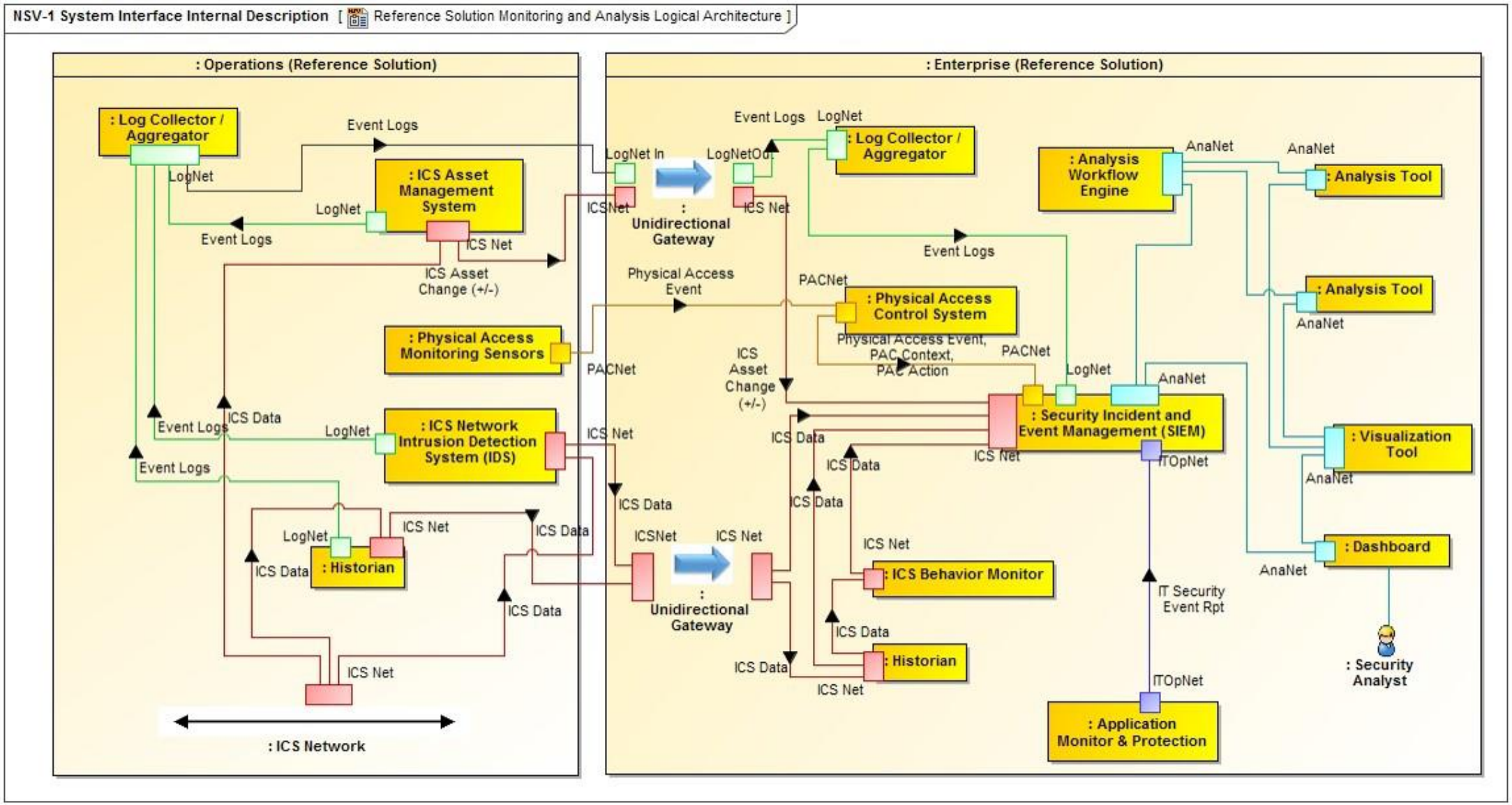
  - Связность узлов сети автоматически поддерживается в сетевом окружении с динамически изменяемой IP-адресацией.
  - Объединение локальных сетей как на сетевом (L3 OSI), так и на канальном уровне (L2 OSI).

Недостатки:

  - Обеспечивается защита логического соединения, а не физического.



Информационная безопасность, архитектура



NIST Special Publication 1800-7 «SITUATIONAL AWARENES for Electric Utilities». Draft. 2017

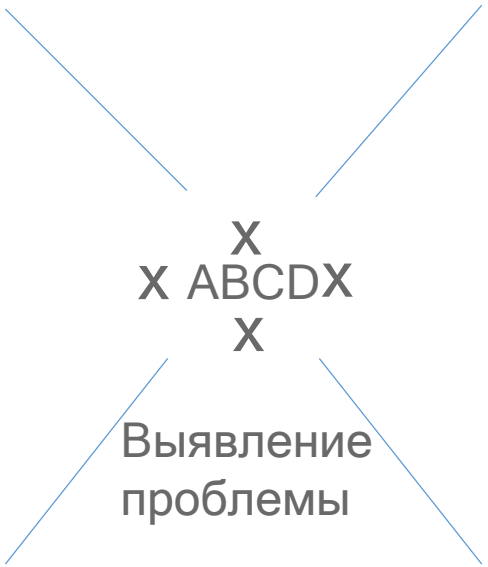
Контроль аномалий

ОМДП 1 контур: Источники данных - Компоненты ЦПС и сетевой инфраструктуры

$$\begin{matrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & & a_{2m} \\ \vdots & \vdots & \ddots & \\ a_{l1} & a_{l2} & & a_{lm} \end{matrix}$$

ОМДП 2 контур: Источники данных - Персонал

$$\begin{matrix} b_{11} & b_{12} & \cdots & b_{1p} \\ b_{21} & b_{22} & & b_{2p} \\ \vdots & \vdots & \ddots & \\ b_{n1} & b_{n2} & & b_{np} \end{matrix}$$



БРП 1: Источники данных - база знаний атак

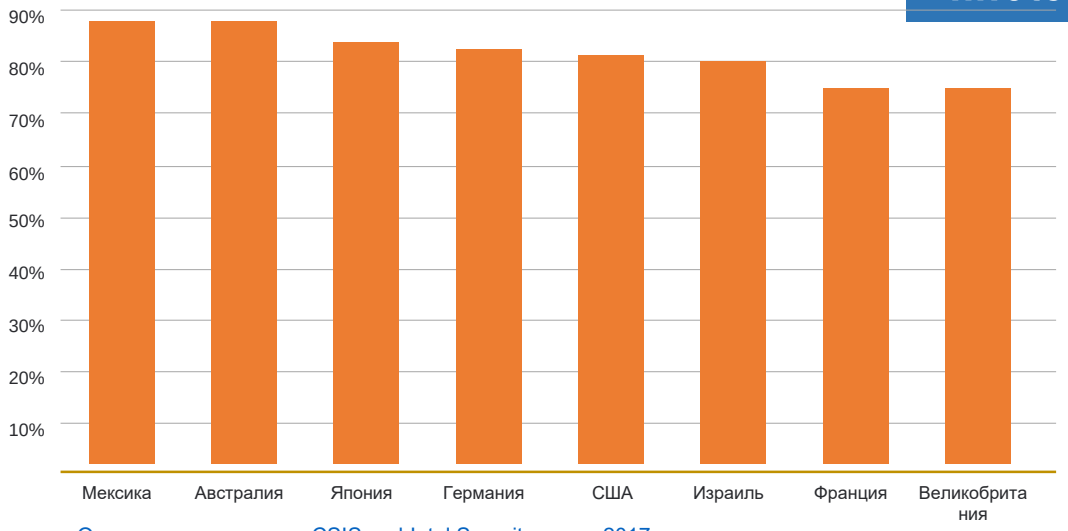
$$\begin{matrix} c_{11} & c_{12} & \cdots & c_{1a} \\ c_{21} & c_{22} & & c_{2a} \\ \vdots & \vdots & \ddots & \\ c_{k1} & c_{k2} & & c_{ka} \end{matrix}$$

БРП 2: Источники данных - модели технологических и информационных процессов (отклонения)

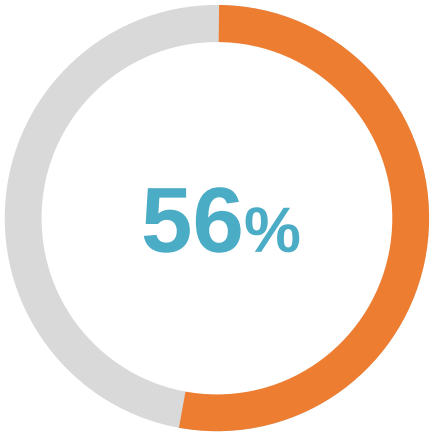
$$\begin{matrix} d_{11} & d_{12} & \cdots & d_{1r} \\ d_{21} & d_{22} & & d_{2r} \\ \vdots & \vdots & \ddots & \\ d_{j1} & d_{j2} & & d_{jr} \end{matrix}$$

Дефицит квалификации в области информационной безопасности КИИ является глобальной проблемой

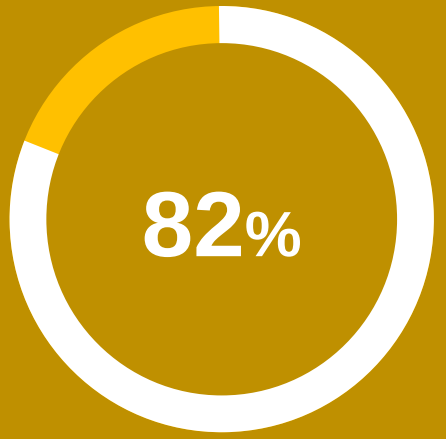
Процент опрошенных, которые сказали, что в их стране имеется дефицит специалистов в области обеспечения кибербезопасности



О недостатке навыков, CSIS and Intel Security, июль 2017



Указали нехватку квалифицированных ресурсов, проблемы с инвестициями в области информационной безопасности, и защиты ценностей организации



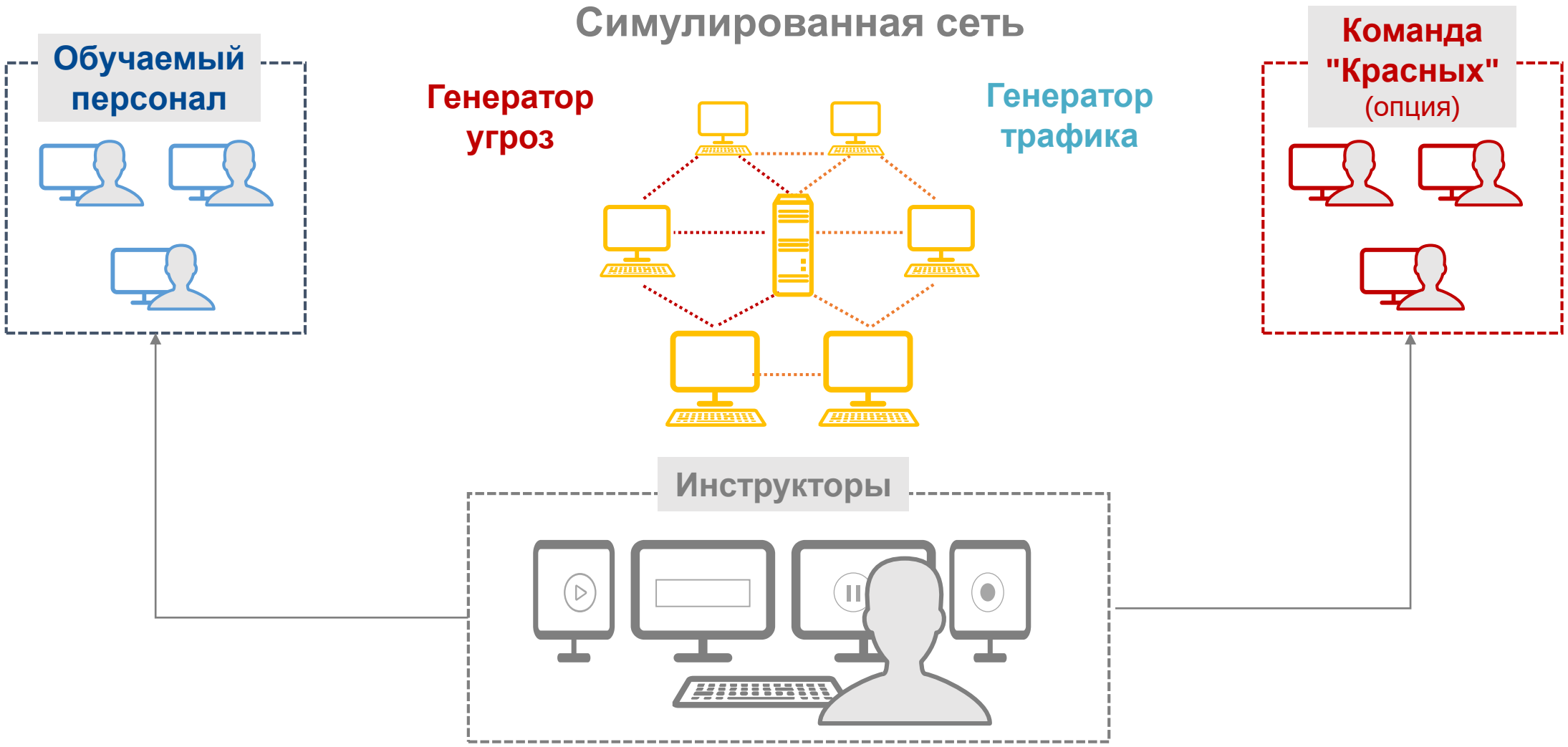
Отметили дефицит навыков в области кибербезопасности.

Глобальное исследование в области информационной безопасности, EU, 2015

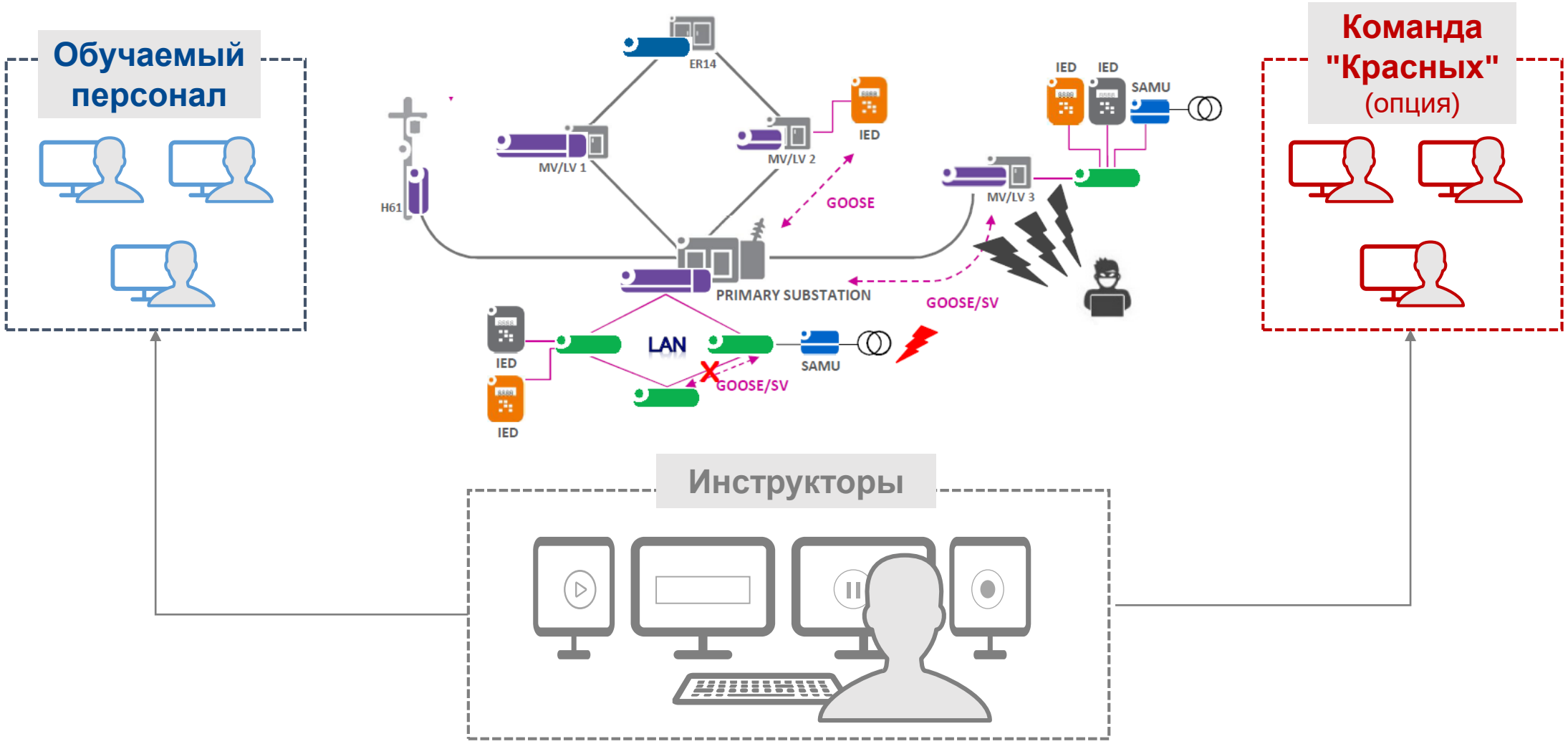
Кроме того, специалистам в области безопасности КИИ не хватает тестовой среды, приближенной к реальным условиям эксплуаатации, достаточной для испытания и оценки их методик по обеспечению ИБ

- Оценка достаточности архитектуры безопасности КИИ
- Проверка корректности и оценка ИБ
- Оценка уязвимостей
- Подтверждение работоспособности решения (POC) и испытания средств обеспечения ИБ

Настраиваемая сеть, трафик и угрозы



Пример симулятора для обучения ИБ (МЭК 61850 по IP/MPLS сети)

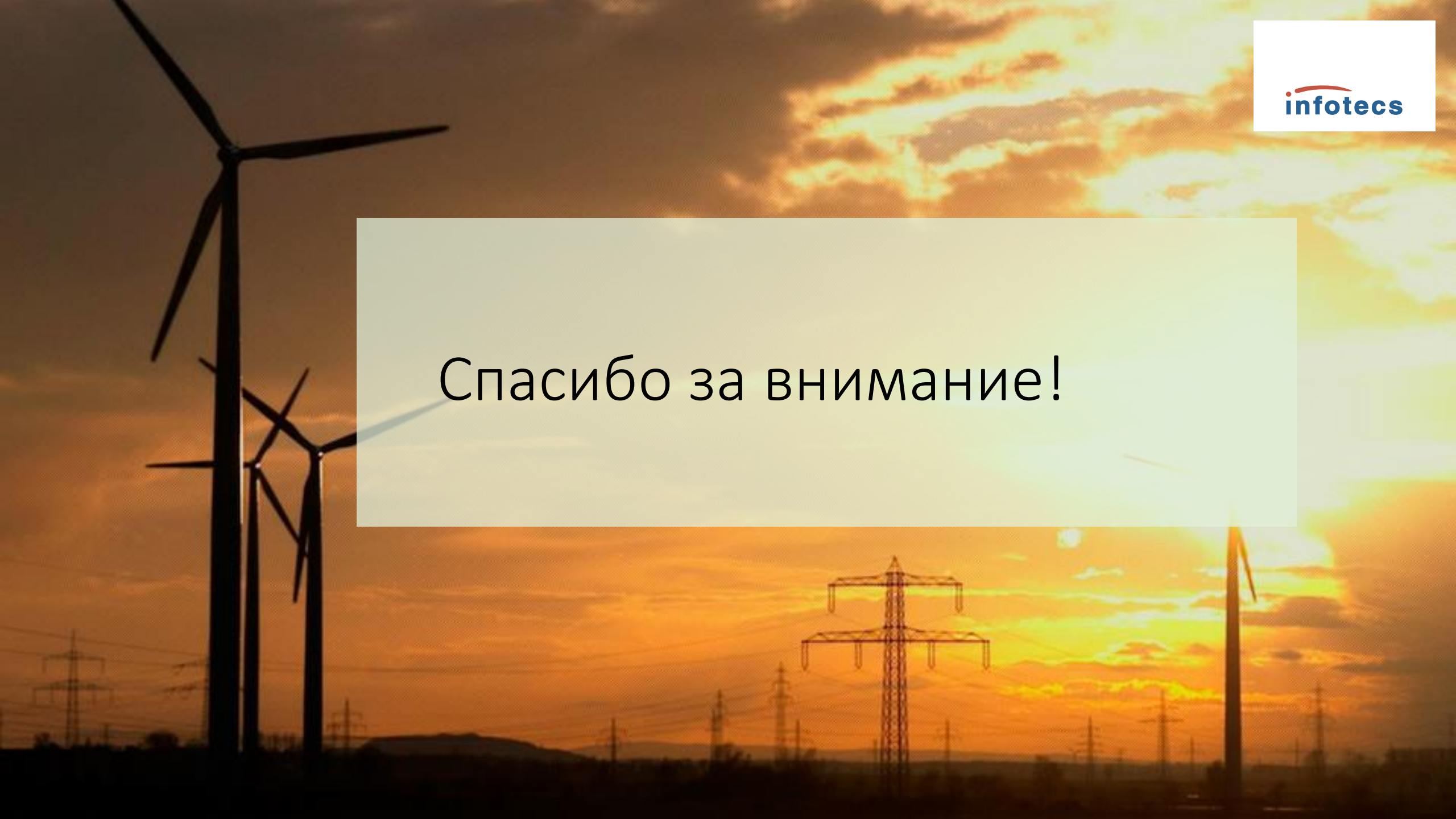


Выводы

- Развитие электроэнергетики по стандарту МЭК 61850 позволяет решить целый ряд технологических, эксплуатационных и экономических задач.
- В то же время растущий объем первичной информации требует пересмотра сложившихся бизнес-процессов управления в энергетике.
- Формируются новые вектора компьютерных атак, меняются требования к уровню подготовки обслуживающего персонала.
- В расчетах показателей надежности технологических процессов появляется существенная информационная составляющая.
- Процесс развития направления ЦПС нельзя ограничить рамками одной или нескольких подстанций, опыт показывает, что это должны быть системные комплексные решения.
- Обеспечение безопасности КИИ влечет за собой появление отдельных автоматизированных систем по аналогии с управлением эксплуатацией

О компании

- Компания ОАО «ИнфоТеКС» один из лидеров рынка информационной безопасности в России. Уже более 25 лет она успешно решает вопросы информационной безопасности и криптографической защиты данных для Заказчиков в государственном и корпоративном сегментах рынка.
- В портфолио компании входят сертифицированные линейки продуктов: **ViPNet; SIES; XFirewall; SafeBoot; IDS; TIAS, RANGE**.
- При активном участии Компании создан и функционирует Технический комитет по стандартизации «Криптографическая защита информации» (ТК 26), ведется активная работа с Техническими комитетами ISO/TC 307 «Технологии блокчейн и распределенных реестров» и ТК194 «Кибер-физические системы».


infotecs
Спасибо за внимание!