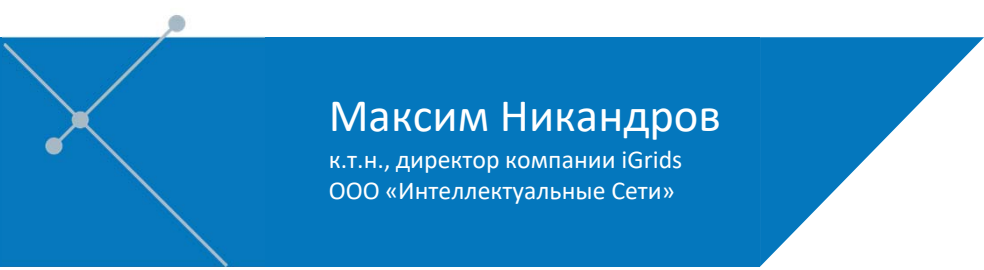


Опыт построения комплекса информационной безопасности ПТК АСДУ ЦУС и ТМ филиалов «Сетевая компания» Татарстана



Максим Никандров

к.т.н., директор компании iGrids
ООО «Интеллектуальные Сети»

«Сетевая компания», Республика Татарстан



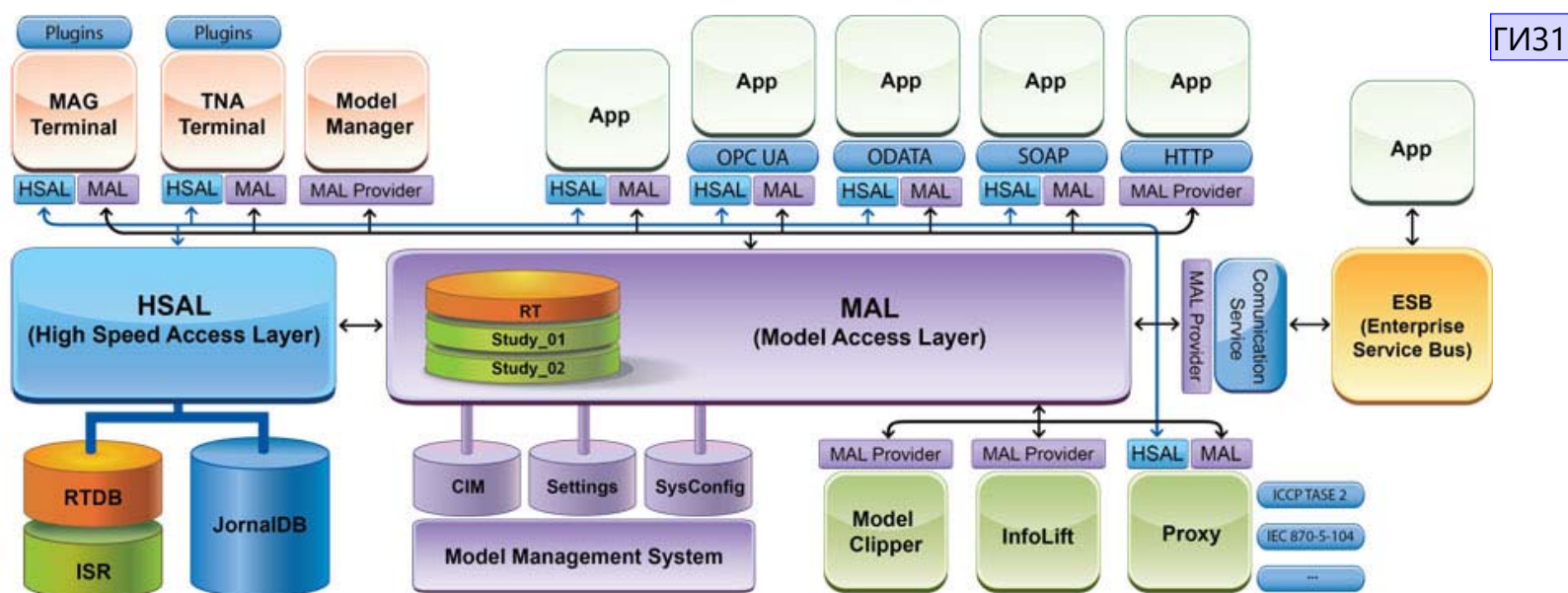
- установленной мощностью **18,6 ГВт**
- **9** предприятий электрических сетей
- **374** подстанции 35-500 кВ
- **19152** ТП и РП-6(10) кВ

Техническое перевооружение систем ПТК АСДУ ЦУС и ТМ



В 2019 г начат проект реконструкции действующей системы АСДУ без перерыва электроснабжения потребителей

Техническое перевооружение систем ПТК АСДУ ЦУС и ТМ



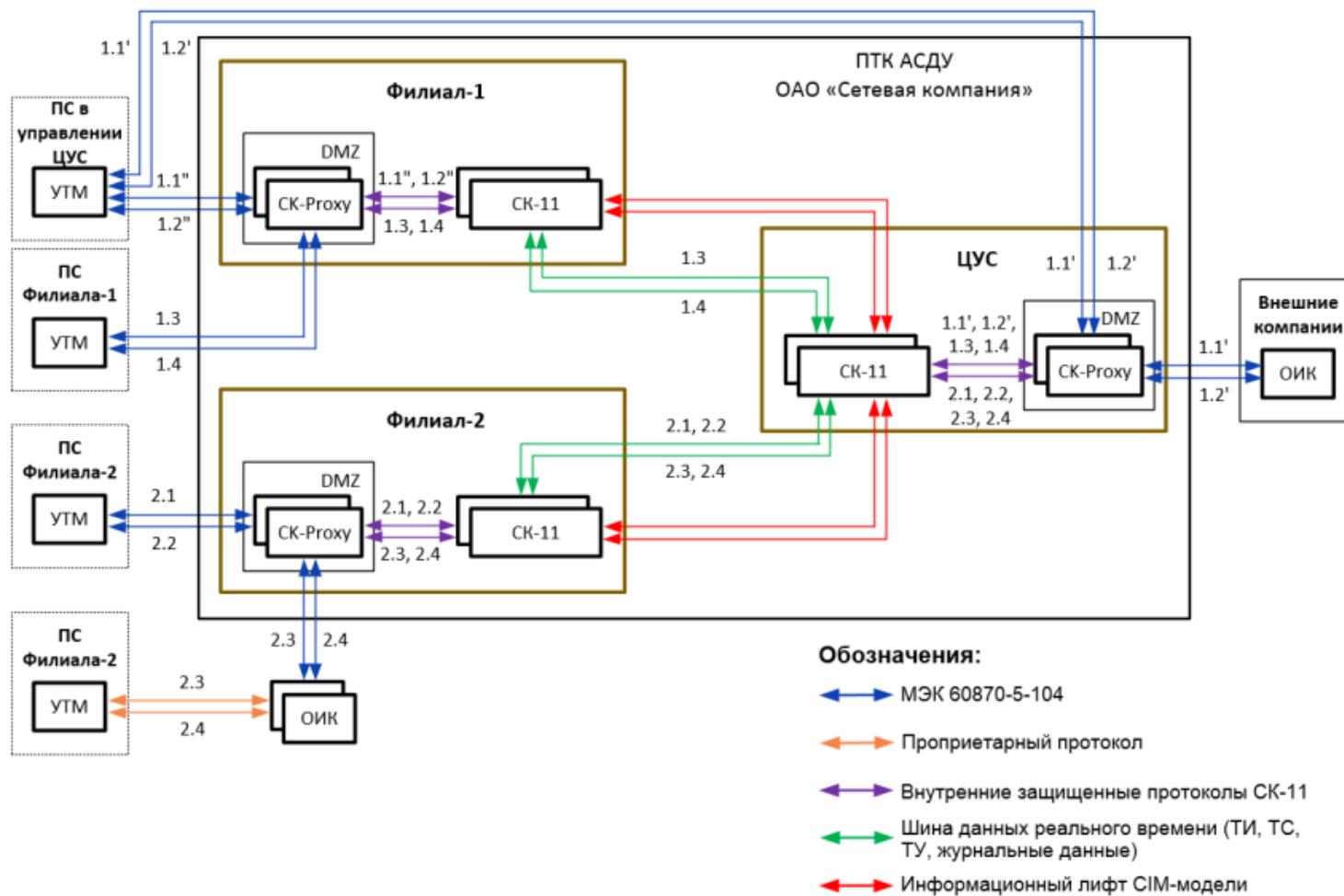
Основная система управления – «СК-11», Монитор электрик

ГИЗ1

не слишком ли сложная схема? может взять сруктурку из проекта фабрики ?

Георгий Иванович Здобнов; 08.02.2021

Структурная схема обмена телеметрической информацией



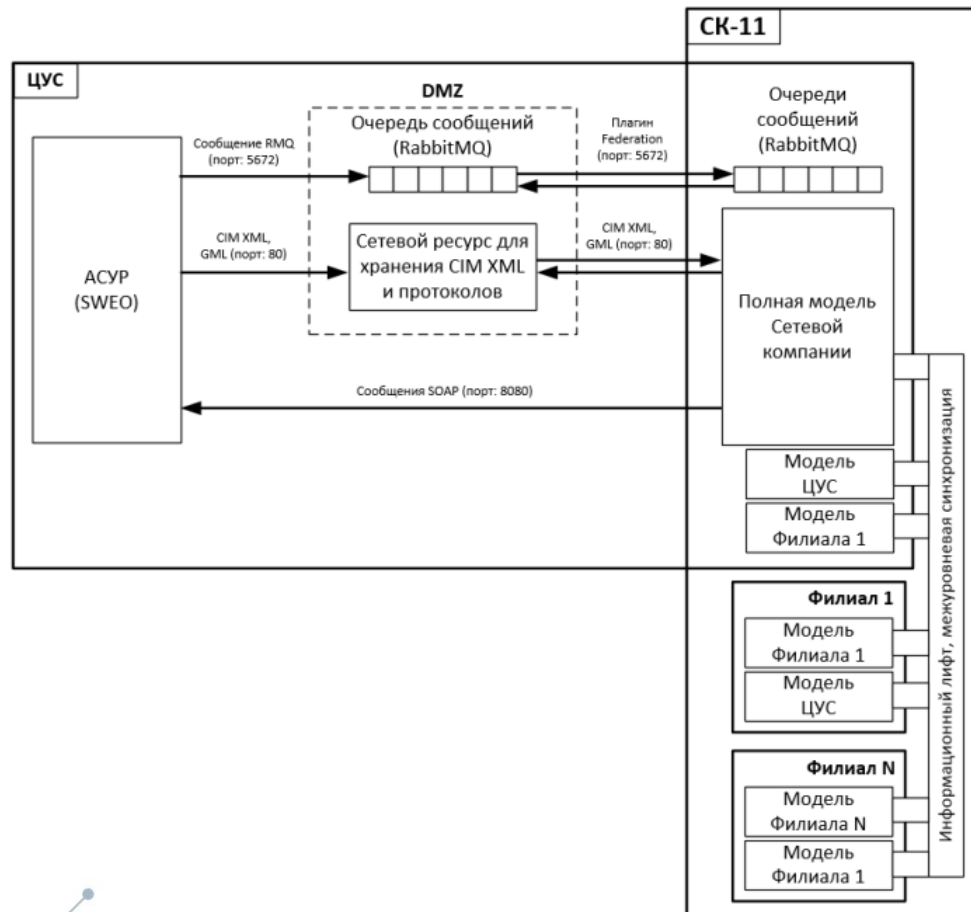


Апробация технических решений ИБ

- Основные программно-технические средства Информационной безопасности прошли апробацию на специально созданном стенде
- Предпочтение отдавалось отечественным решениям
- Тестировалась совместимость с существующим оборудованием



Проектирование подсистемы Информационной безопасности



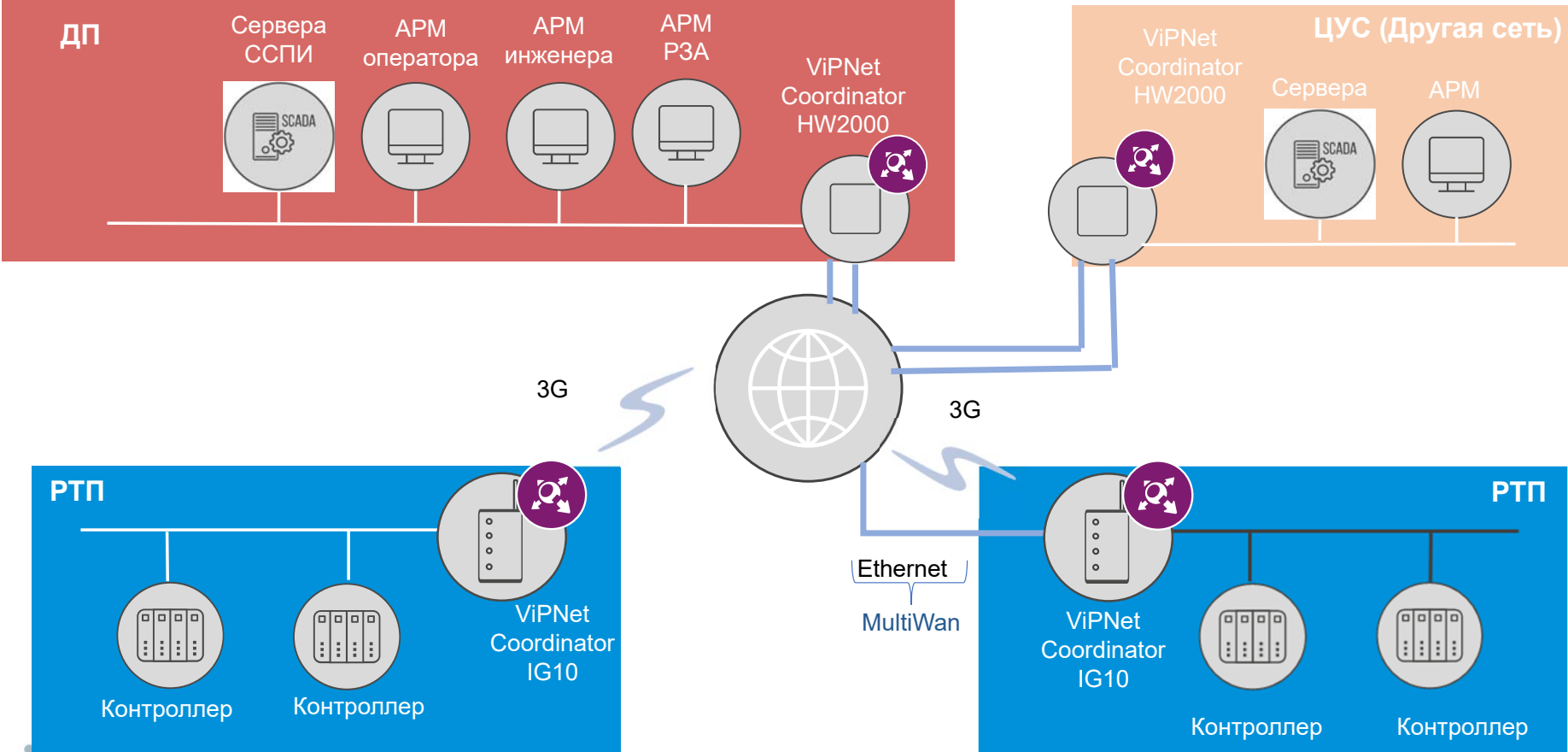
Особенности проектирования:

- назначение ответственных за проектные решения
- параллельная работа с основным проектом «Техническое перевооружение систем ПТК АСДУ ЦУС и систем телемеханики филиалов ОАО «Сетевая компания»
- до категорирования было принято решение работать по 2 категории значимости, на перспективу
- работа с параллельными титулами «SMART GRID»
- сжатые сроки проектирования

Ключевые технические решения подсистемы ИБ

Мера защиты	Применение решение
Защита каналов связи и сегментирование сети АСДУ	СКЗИ серии VipNet
Антивирусная защита	KICS for Nodes, KES
Система обнаружения вторжения	KICS for Network
Система резервного копирования и восстановления основных компонентов ПТК	Acronis
Выявление компьютерных инцидентов	MaxPatrol SIEM
Контроль защищенности	MaxPatrol
Средства диагностики оборудования	Zabbix
Переход на отечественное ПО	Astra linux

Защита каналов связи криптошлюзами



Пусконаладочные работы в условиях пандемии



Применение криптографических шлюзов позволило быстро и эффективно организовать удаленные пусконаладочные работы

Пусконаладочные работы

Особенности:

- Пусконаладка в условиях функционирующего объекта
- Настройка сети СКЗИ учётом технологических особенностей филиалов
- Тотальная антивирусная защита, в том числе установка АРМ с Astra Linux
- Контроль и обнаружение подозрительной сетевой активности в технологической сети
- Настройка политик безопасности ОС с учётом технологических особенностей ПТК
- Выдача рекомендаций по дополнительной настройке аппаратной части компонентов ПТК (BIOS, iDRAC)
- Выдача рекомендаций по физической защищённости компонентов ПТК



Эксплуатация подсистемы Информационной безопасности



- Создание отделов по информационной безопасности в соответствии с приказом ФСТЭК №235
- Опыта и компетенций не хватает
- Отправка на обучение персонала отделов Информационной безопасности
- Активной участи в процессе пусконаладочных работ
- Поиск и анализ уязвимостей компонентов ПТК и контроль их устранения

Планы на будущее

- Дальнейшая интеграция объектов в новую АСДУ и подсистему ИБ
- Разработка полного комплекта организационно распорядительной документации
- Внедрение системы контроля привилегированных пользователей
- Автоматизированная система актуализации документации



Выводы



- Создание комплексной и эффективной системы Информационной безопасности для крупных АСДУ **реально!**
- Программно-технические средства уже есть на рынке, есть из чего выбрать
- Отсутствие достаточного опыта в эксплуатации средств ИБ
- Есть проблемы организационного характера, но они решаемы.





Спасибо за внимание!



Директор ООО «Интеллектуальные Сети»,
к.т.н., Максим Никандров
nikandrov@igrids.ru

