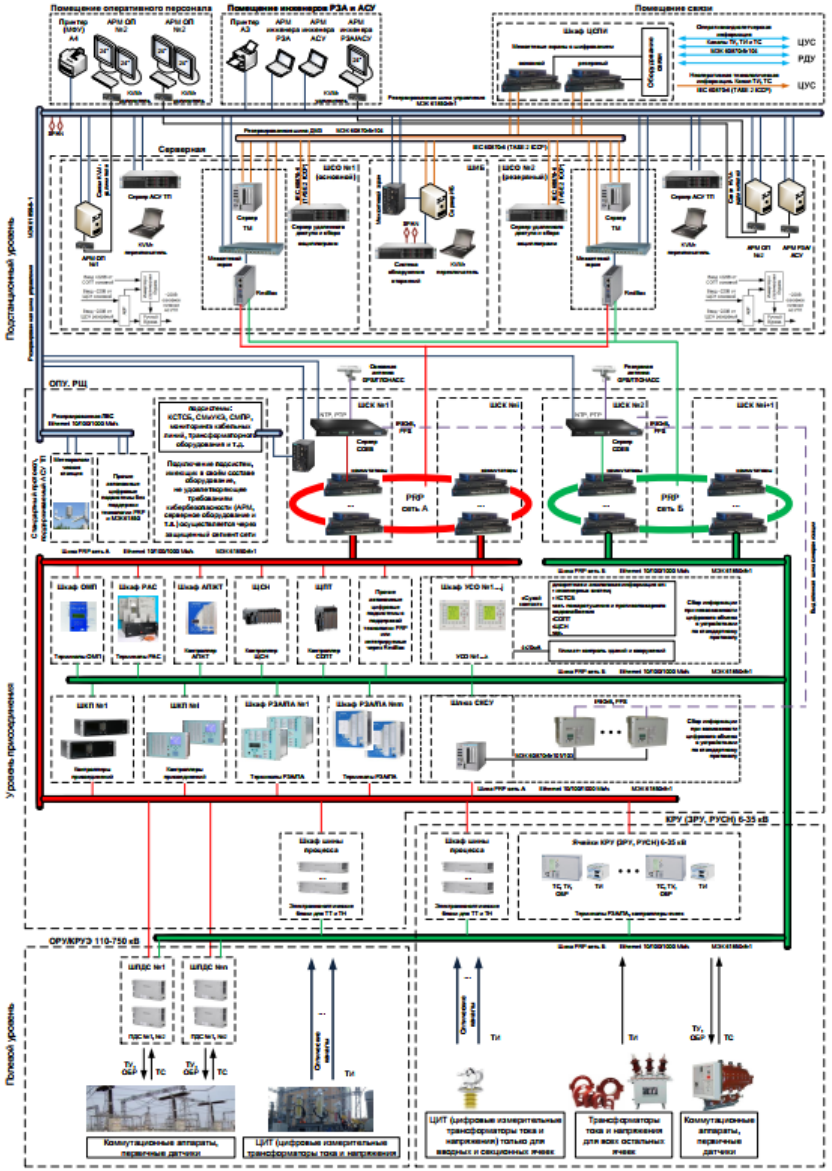
Методы и средства обеспечения информационной безопасности локально-вычислительных сетей цифровых подстанций

Максим Никандров
к.т.н., ООО «Интеллектуальные Сети»

Изменения ситуации

- **Тотальный переход на Ethernet и, как следствие, большие локальные сети**
- **Больше количество интеллектуальных устройств на один объект управления**
- **ЛВС стала критически важной подсистемой комплекса управления**

ЦПС критично зависит от ЛВС



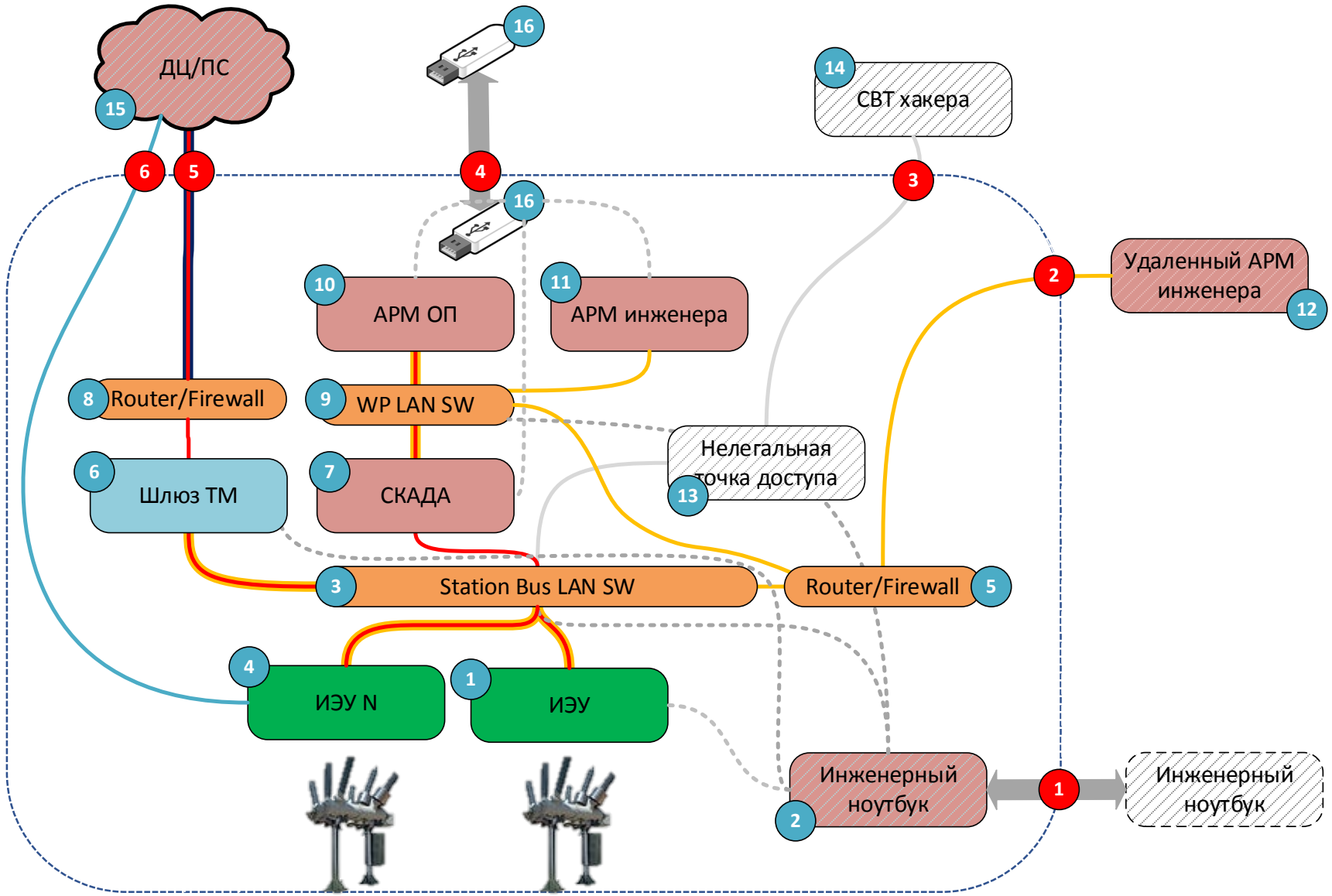
Цифровая подстанция
III архитектура типовых решений

Особенности:

- для новых и реконструируемых подстанций;
- применение протокола PRP (MMS, GOOSE);
- объединение MMS-, GOOSE- и SV-потоков в мультишине;
- применение ШПДС;
- применение цифровых измерительных ТТ и ТН;
- применение электронно-оптических блоков для ТТ и ТН;
- учет требований в части ИБ.

iGrids интеллектуальные сети

Уязвимости периметра ПС



Из презентации Дорофеева Ивана

iGrids интеллектуальные сети

Что можно сделать чтобы улучшить ситуацию?

iGrids
интеллектуальные сети

Предложения по защите ЛВС

1. **Повышение наблюдаемости ЛВС**

2. **Сегментирование ЛВС – с помощью программных или физических межсетевых экранов.**

3. **Организация демилитаризованной зоны – для обеспечения информационного обмена с вышестоящими уровнями управления.**

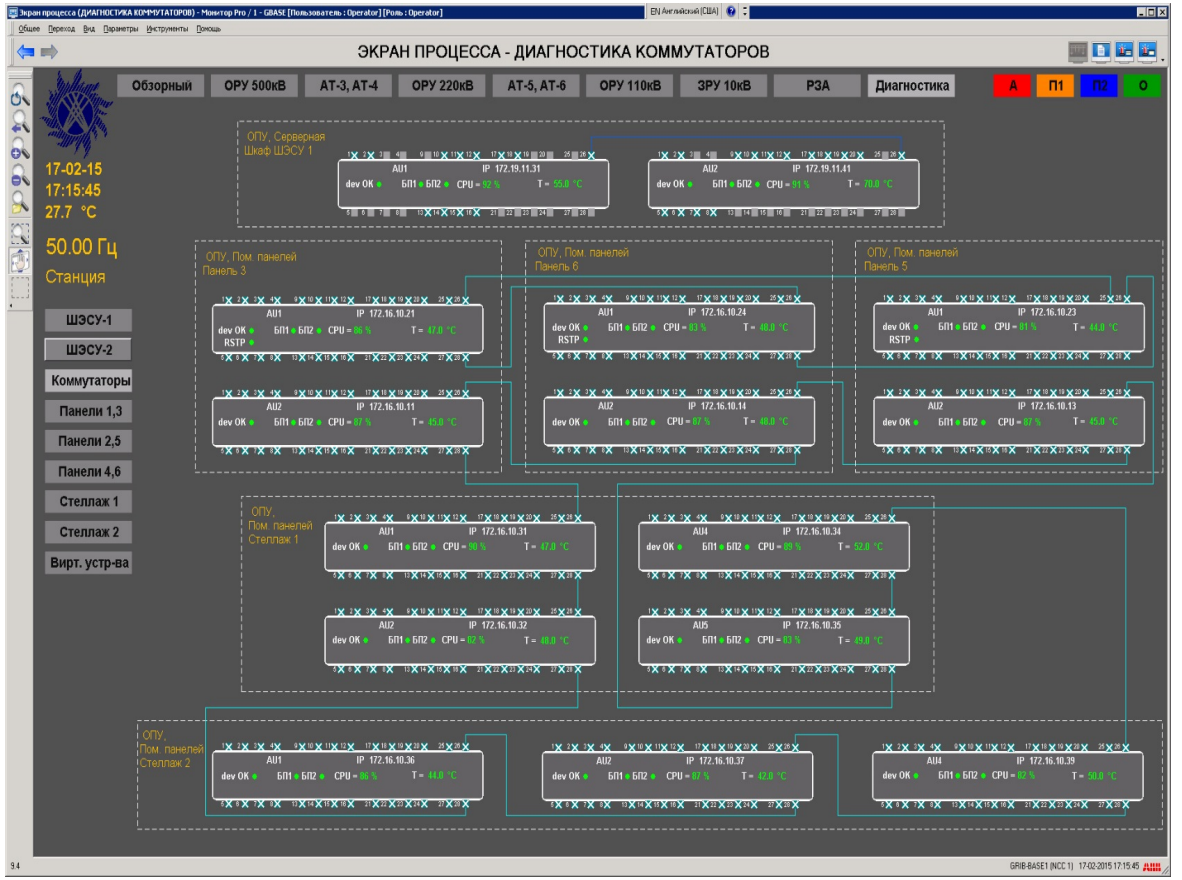
4. **Система обнаружения вторжений – для контроля трафика в ключевых точках ЛВС.**

5. **Антивирусное обеспечение – для безопасности данных на серверах и АРМ АСУ ТП.**

6. **Центр управления ИБ (сервер ИБ) – для удаленного централизованного управления защитой**

Повышение наблюдаемости сети

- готовность устройства к работе (успешное завершение самодиагностики);
- получение диагностической информации с модулей или плат устройства;
- отсутствие питания (неисправность) основного или резервного блока питания;
- статус сетевого взаимодействия по всем портам;
- температура внутри корпуса устройства;
- информация о загрузке CPU;
- признак перестроения дерева (технология RSPT или аналогичная).

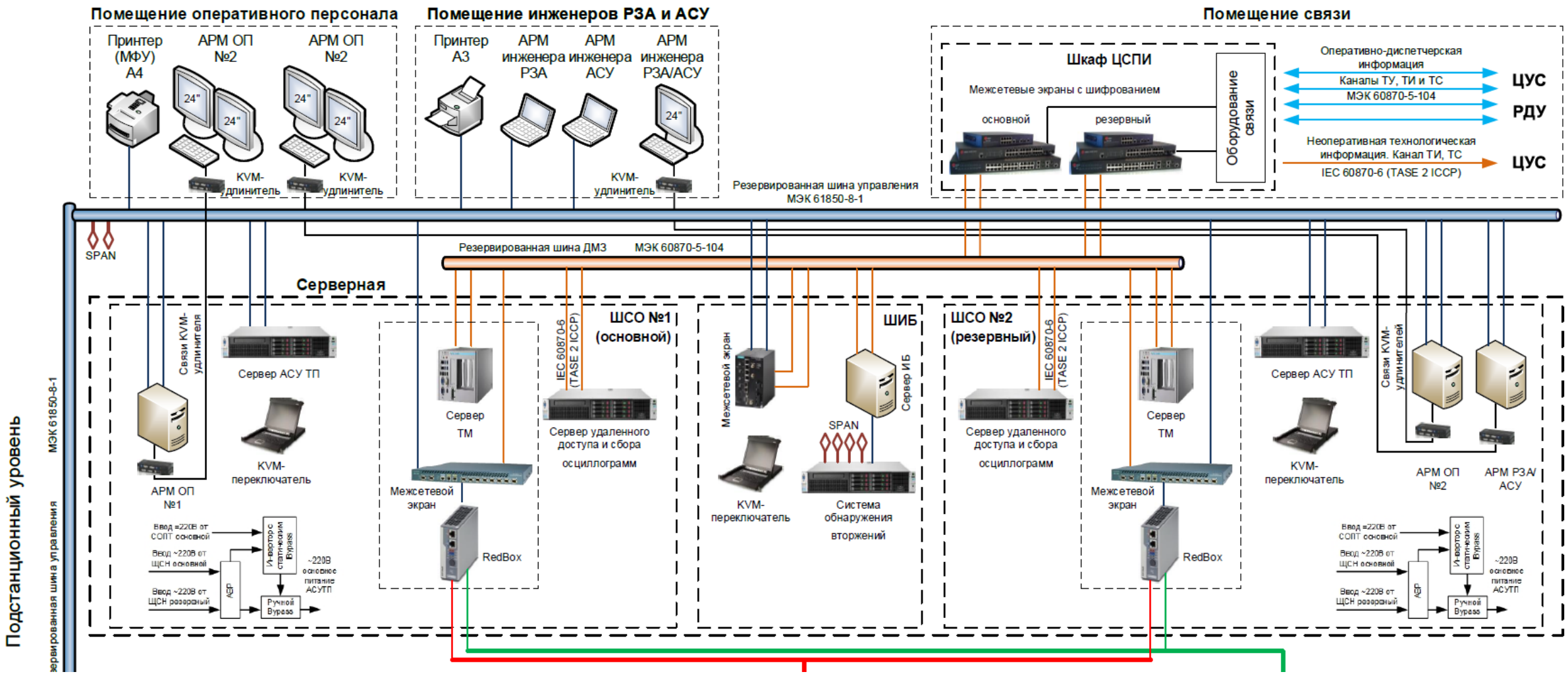


SNMP v3 – добавления криптографической защиты

Эта диагностика уже есть сейчас во многих коммутаторах

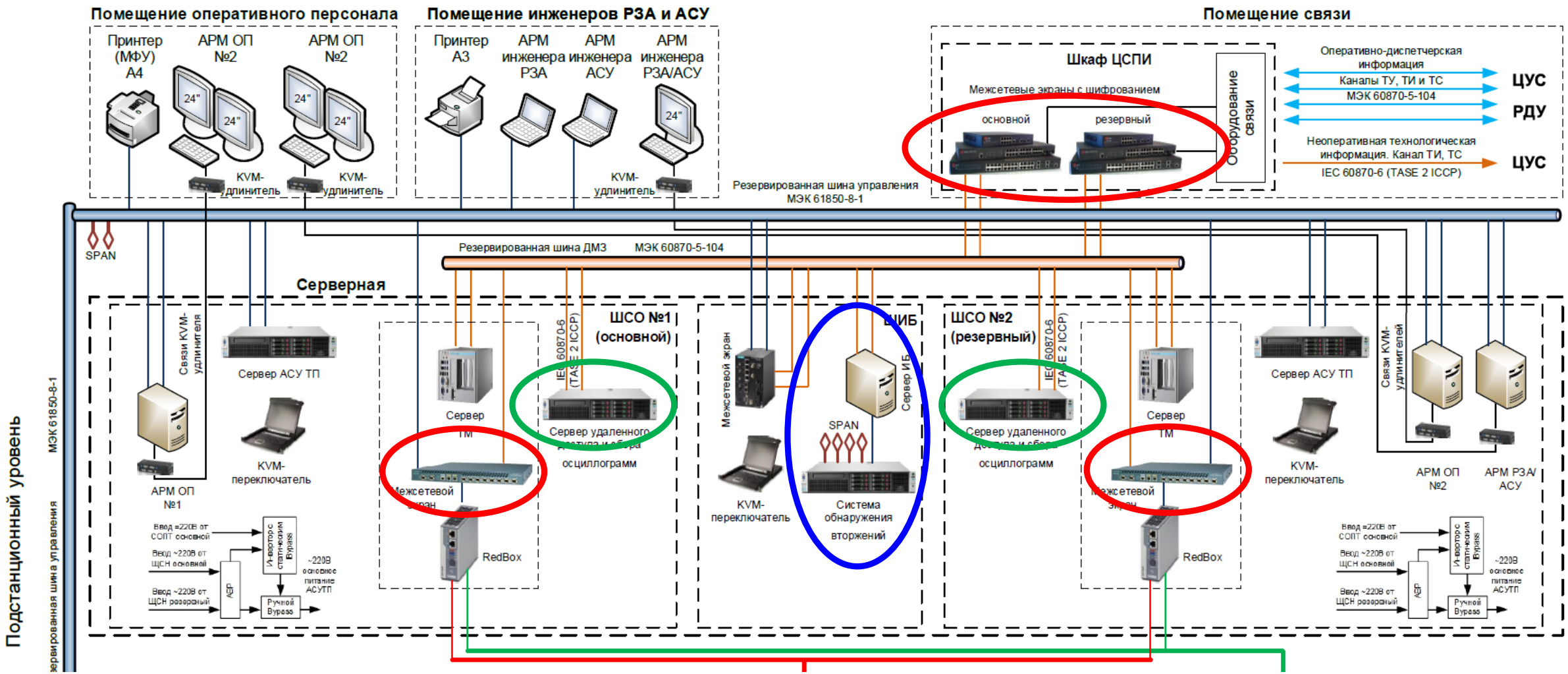
Организация ДМЗ, установка СОВ и сервера ИБ

Структурная схема типового ПТК АСУТП. Архитектура III с мультишиной

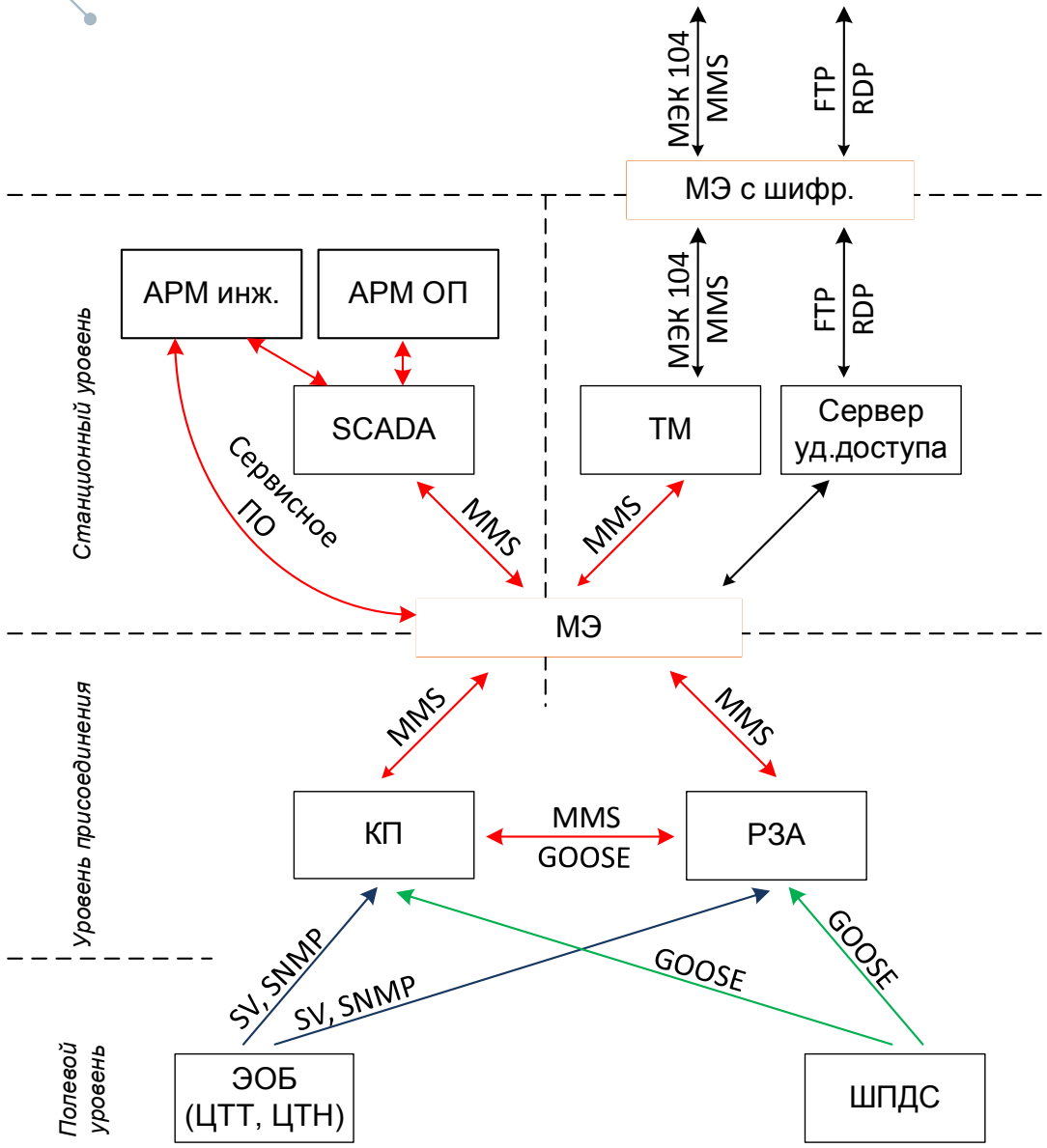


Организация ДМЗ, установка СОВ и сервера ИБ

Структурная схема типового ПТК АСУТП. Архитектура III с мультишиной



Сегментация ЛВС и контролируемая деградация



Управляемая деградация контура управления:

- потеря связи с удаленным ДП -> управление со скады;
- потеря связи со скадой -> управление с КП;
- потеря связи с КП -> управление с терминала РЗА.

Концепция контролируемой деградации

«Нормальный режим» - контроль всех физических и логических подключений к информационной сети (не только внешний периметр, как классические Firewall) путем управления промышленными коммутаторами и контроля подключения по технологии IEEE 802.1x и MAD (MAC, IP) авторизации.

«Аварийный режим» - обеспечение автоматизированного перехода информационной сети системы управления на заранее подготовленные рубежи деградации в случае кибернетической атаки или другой активности нарушителей (как внутренних, так и внешних). Это должно значительно уменьшить поверхность атаки и в большинстве случаев купировать нападения, при сохранении работоспособности основных компонентов системы, хотя и с потерей второстепенных функций и части наблюдаемости технологического процесса.

«Режим восстановления» - обеспечение автоматизированного перехода информационной сети системы управления к первоначальному проектному состоянию.

iGrids интеллектуальные сети

Функции управления сетью

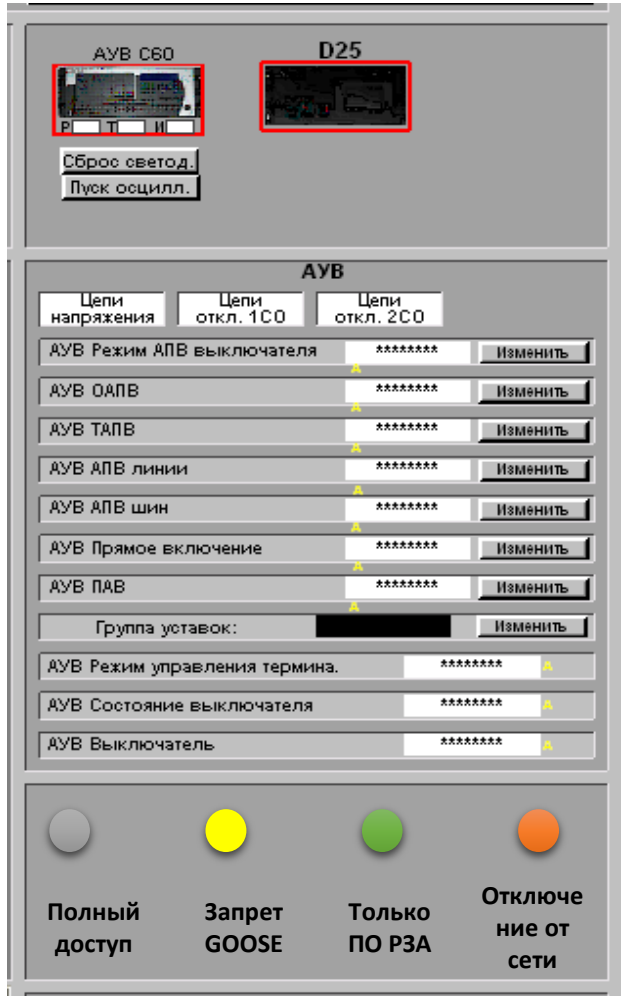
Перспектива дистанционное управление сетью и информационным обменом

Полный доступ в информационную сеть

Блокирование многоадресного трафика (GOOSE, SV)

Доступ к терминалу только сервисным ПО

Отключение устройства от информационной сети



Каждый терминал и группа терминалов одного присоединения должны получить новую функцию – уровень взаимодействия с информационной сетью

Выводы

1. **Необходимо учитывать что ЛВС критически важный элемент цифровой подстанции, который требует особого внимания**

2. **При проектировании необходимость применения методов и средств обеспечения безопасности:**
    - **Сегментирование ЛВС;**
    - **Организация ДМЗ;**
    - **Обязательное применения СОВ;**
    - **Централизованное управление ИБ объекта. – с помощью программных или физических межсетевых экранов.**
3. **Необходимо развитие проактивной защиты в дополнение к СОВ.**

13

Спасибо за внимание!

Максим Никандров
ООО «Интеллектуальные Сети»
nikandrov@igrids.ru