kaspersky

Kaspersky Industrial Cybersecurity Conference 2021

Алексей Иванов

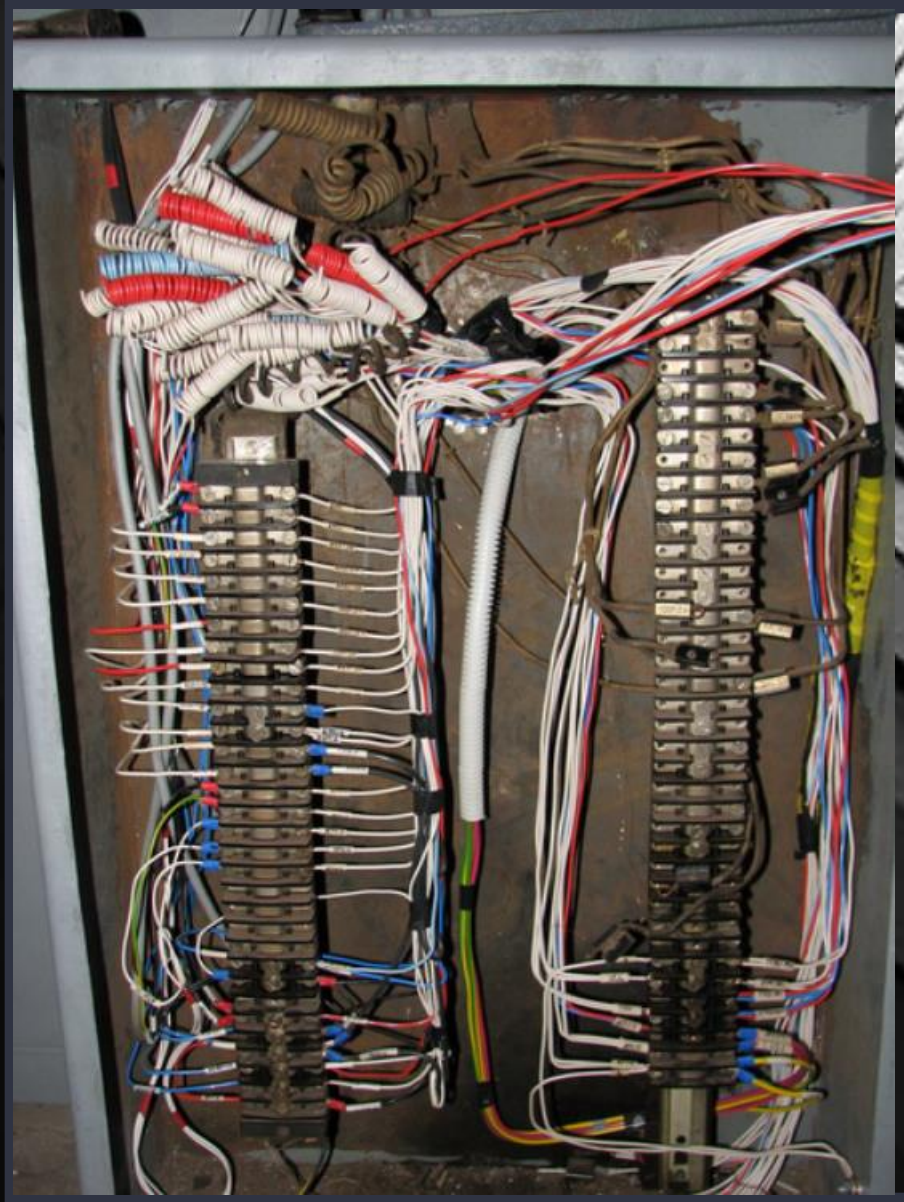
Независимый эксперт, Россия

#KasperskyICS

Чат конференции: https://kas.pr/kicscon

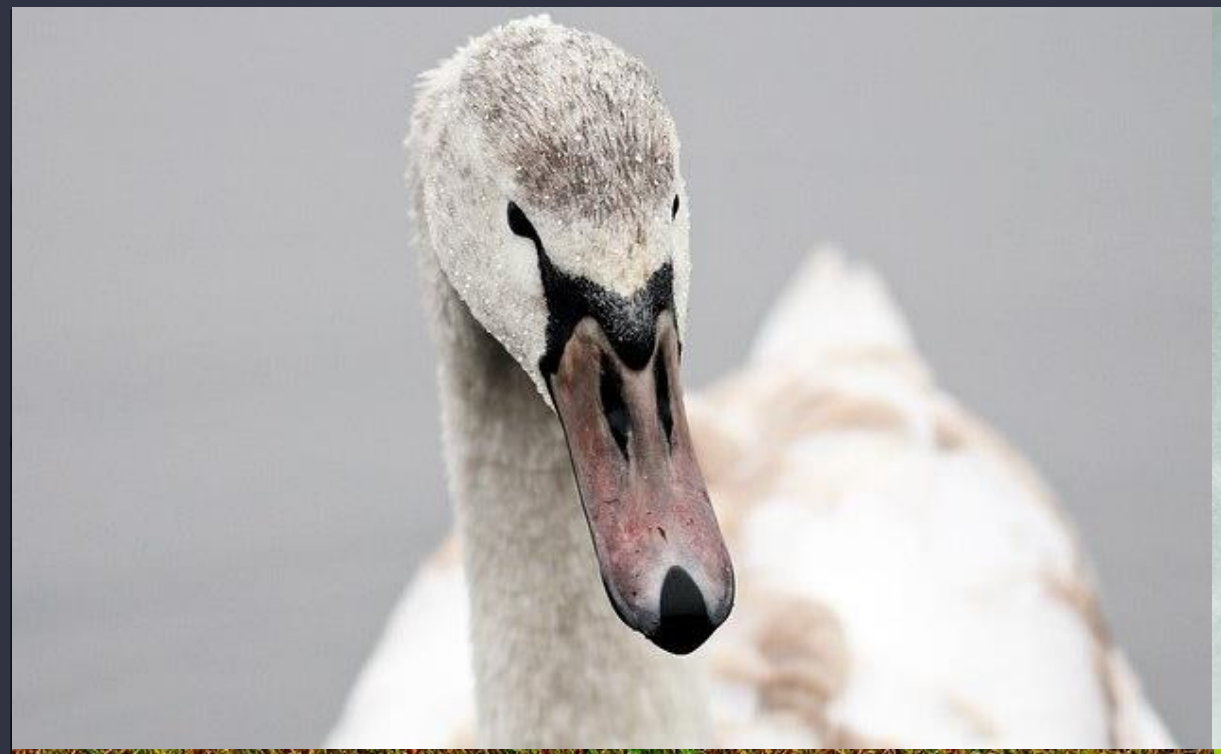
АСУ ТП ПОДСТАНЦИЙ

Реализация проектов в соответствии с ФЗ-187



Проекты

- Модернизация действующих ПС по одной из типовых архитектур
- Создание новых ПС



Текущая ситуация

Отсутствует согласованность по вопросам ИБ между

- Заказчиком
- Проектировщиком
- Вендором АСУ ТП
- Интегратором
- Службой ИБ

Новое (ТЗ) – это хорошо забытое старое (ТЗ)

Обилие бюрократии приводит к тому, что очень часто на скорую руку адаптируют старое техническое задание

Составитель ТЗ

Не проконсультировался со службой ИБ собственной организации

Упустил из виду, что строится ОКИИ (ЗОКИИ?)

Плохо общался с представителями Интегратора, Проектанта и Вендора АСУ ТП

Проектант

Не консультируется с Вендором АСУ ТП
Не учитывает требования по ИБ (ведь их практически нет!)

Вендор АСУ ТП

Не верит, что нужны ВСЗИ, типовые решения, документация по ИБ, сертификаты, ПМИ в части ИБ для Интегратора и Заказчика

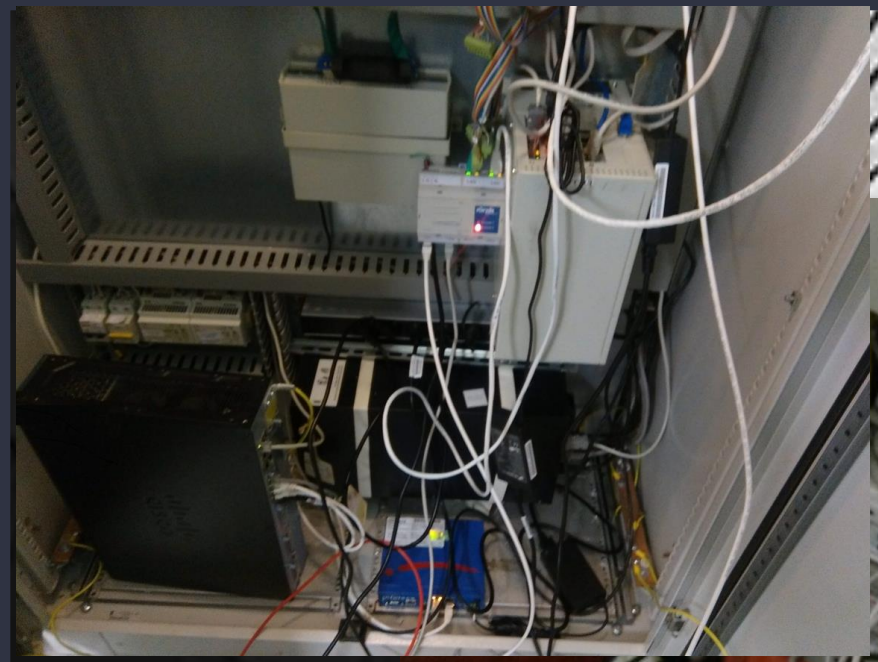
Де факто оставляет задействованным небезопасный функционал, подстраховываясь в документации рекомендациями его не использовать

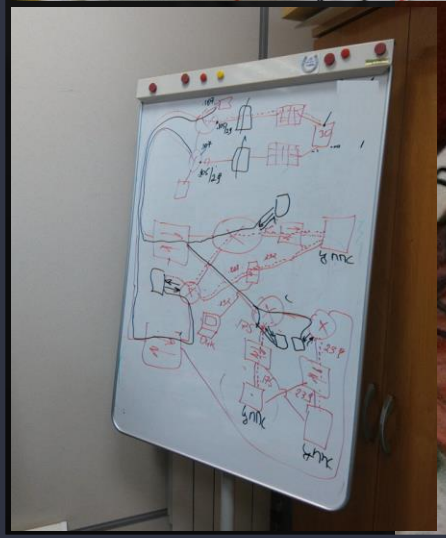
Интегратор

Пытается из зоопарка собрать работающую АСУ ТП
Вносит изменения (иногда) в документацию
Сроки горят

Приёмная комиссия

Может не принимать – и не принимает
Активизируется служба ИБ
«Вы сдаёте объект КИИ, не соответствующий требованиям ФЗ-187»
Надо принимать по ТЗ – а в ТЗ в части ИБ пусто
Кто заплатит за средства защиты, их установку, наладку?





Как «впихнуть невпихуемое»

В результате приходится устанавливать оборудование, для которого нет:

- Мощностей по питанию
- Места в стойке

Также может потребоваться изменить топологию

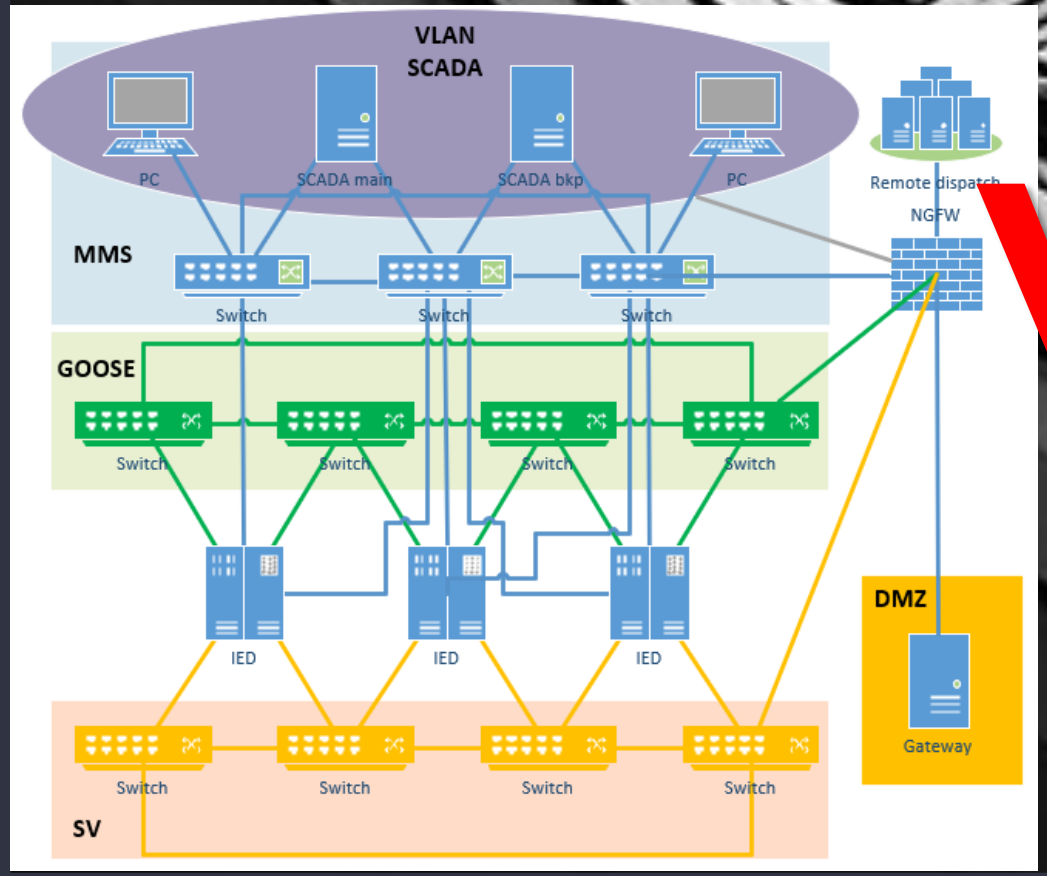
VS

Power ~x2, варистор, резервирование!

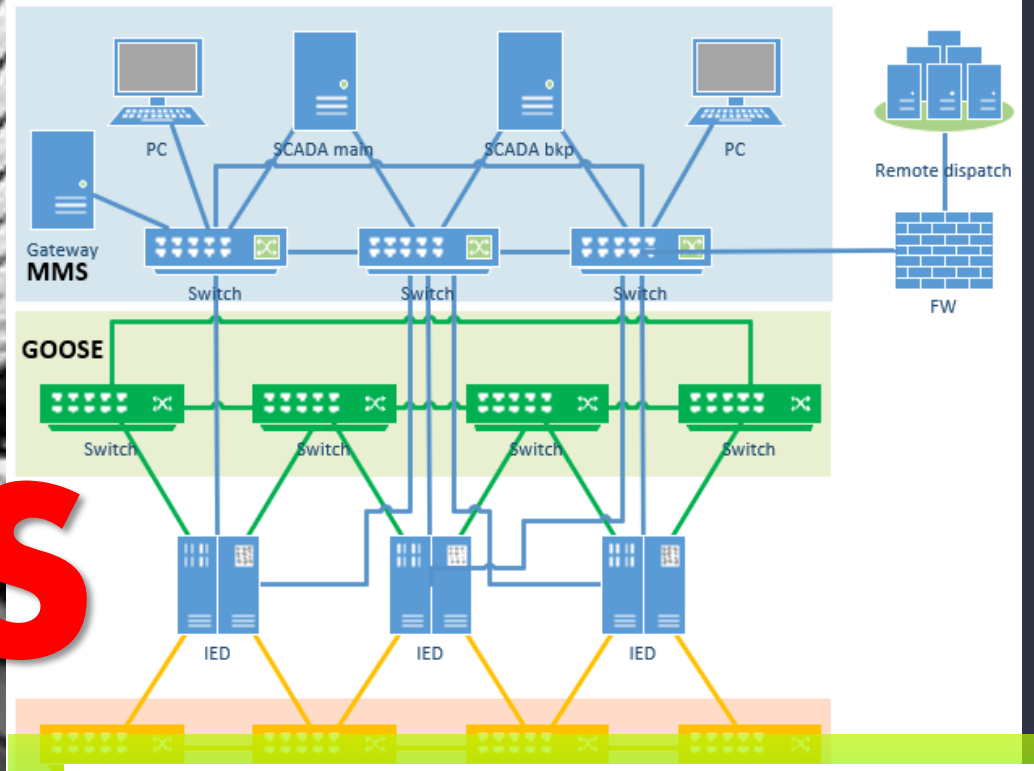
$$$$$$$$$$$$$$$$$$$$$$$$

Требования к оборудованию

IEC 61850-3
Резервируемое питание
Промышленные СЗИ часто под длинный заказ

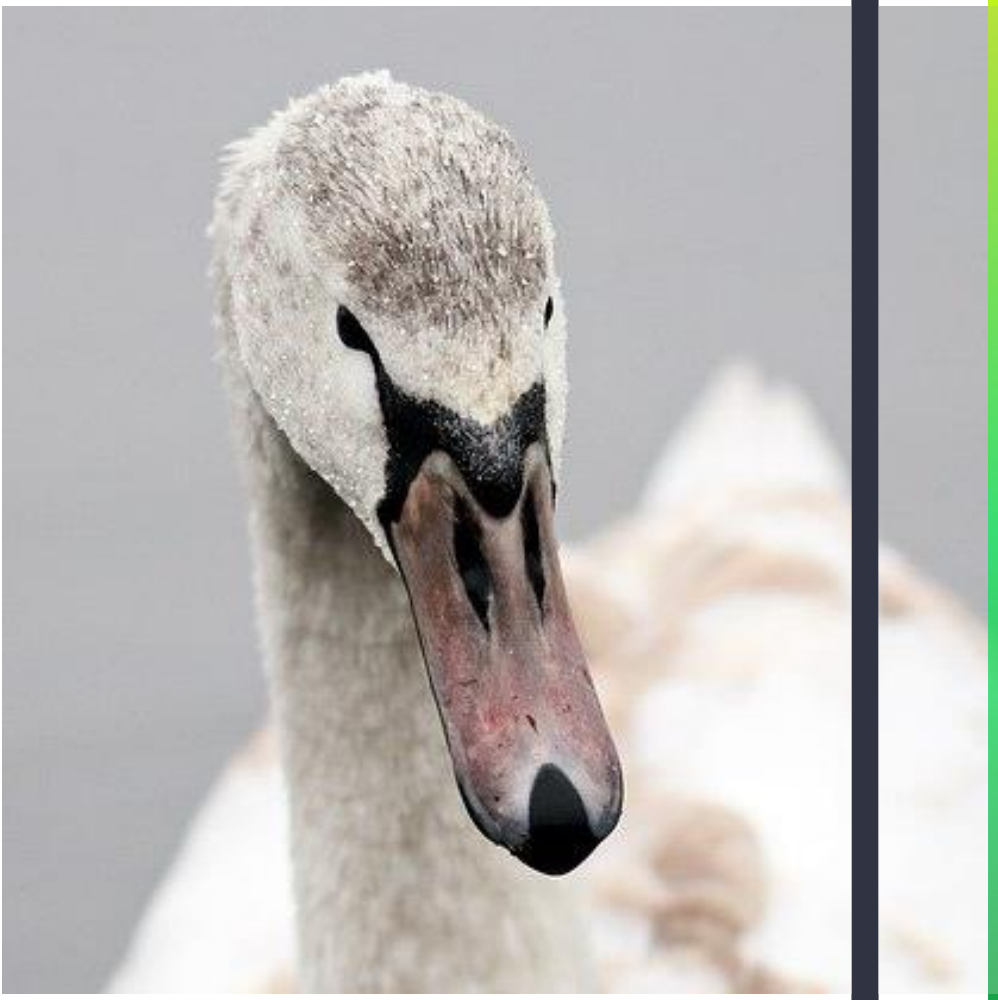


VS



«Плоская топология»

Сложно собирать трафик
Подключения IDS во многих точках
Отсутствует мониторинг некоторых сегментов
Возможен непосредственный доступ к трафику технологических протоколов



ВЫВОДЫ

Для авторов ТЗ

Консультироваться со службой ИБ

Привлечь комиссию по категорированию

Задать категорию объекта (может быть пересмотрена)

Консультироваться с потенциальными поставщиками АСУ ТП, проектной организацией, интеграторами

Определить, интеграция с какими существующими решениями потребуется

Прописать требования к наличию лицензии на ТЗКИ

ВЫВОДЫ

Для проектантов

Если не указана категория, нет МУ или иных требований – запросить

Консультироваться со службой ИБ Заказчика

Консультироваться с вендором АСУ ТП

Консультироваться с Интегратором

Не стесняться спрашивать или просить помощи

ВЫВОДЫ

Для разработчиков

Заранее (сильно заранее) ориентироваться на требования и меры законодательства

ГОСТ 56939 и оформление документации

Типовые конфигурации и тестирование на совместимость с вендорами СЗИ

Наборы рекомендаций по построению АСУ ТП, использованию ВСЗИ

Учитывать особенности заказчиков

ВЫВОДЫ

Для интеграторов

Встретиться с представителями службы ИБ заказчика не на приёмке

Своевременно информировать об изменениях в документации

Консультироваться с Вендорами

Выстроить взаимодействие как можно раньше

Проводить испытания

ВЫВОДЫ

Для службы ИБ Заказчика

Выстраивать отношения с другими службами

Обновлять методики испытаний средств защиты

Принимать участие в проектах ещё на стадии написания ТЗ

Исключать спорные ситуации путем внесения изменений в нормативные акты

Изучать типовые решения от Вендоров заранее

Фиксировать полученный опыт и переиспользовать его

THANK YOU

linkedin.com/in/alexey-ivanov-540bb34