Защита критической информационной инфраструктуры на объектах электроэнергетики.

«Знание — сила: Экспертиза производителя в борьбе с угрозами»

ИТОГИ 2023 ИБ

12 объектов — **7,1 ГВт**

Внедрены системы обеспечения информационной безопасности объекта «под ключ»

47 объектов — **33,4 ГВт**

Приведены в «эталонное» состояние по всему объему установленных автоматизированных систем

> 50 объектов — **35,6 ГВт**

электрогенерации обеспечивается эксплуатационная готовность и реагирование на инциденты в режиме 24/7

> 300 средств защиты информации

и комплексных ИБ-решений собственной разработки установлено на ЗО КИИ

Целевая атака

Время, Сложность, Величина ущерба, Уровень компетенций

Проникновение

Получение НСД

Закрепление

Расширение НСД на критические узлы

Разведка

Архитектура, технология, алгоритмы

Подготовка

Подготовка технологической последовательности атаки

Атака

- Воздействие на критический узел

Атака

- Подмена параметров контроля
- Загрузка измененных алгоритмов
- Ложная команда или блокировка управления

Останов

- Быстрая атака;
- Средние компетенции нарушителя;
- Небольшой ущерб.

Разрушение

- Долгая атака;
- Неограниченные компетенции нарушителя;
- Неприемлемый ущерб.

Особенности ПТК АСУТП

- ПТК АСУТП это **набор разнородных компонент** определенных версий, которые собраны воедино и функционально протестированы на совместимость и взаимную работоспособность
- Система работает **в «реальном времени»** с парированием любого единичного отказа
- ПТК АСУТП – это условно **детерминированная система** на протяжении всего жизненного цикла
- ПТК АСУТП – чаще **самодостаточная** (независящая от внешних систем) **система** для управления технологическим процессом
- Жизненный цикл ПТК АСУТП **от 15 лет**

Меры защиты

Время, Сложность, Величина ущерба, Уровень компетенций

Проникновение

Получение НСД

Закрепление

Расширение НСД на критические узлы

Разведка

Архитектура, технология, алгоритмы

Подготовка

Подготовка технологической последовательности атаки

Атака

Изоляция

Эталон

Мониторинг

Эталонное состояние

Безопасность создается на каждом этапе жизненного цикла системы, на всех уровнях иерархии системы по всем доступным интерфейсам, учитывая все субъекты взаимодействия.

- Субъекты доступа к системе (люди, системы)
- Интерфейс взаимодействия с системой (физический, сетевой, прикладной, программный, HMI)
- Функциональная архитектура ПТК АСУТП (уровень оператора, уровень системного администрирования, уровень прикладной конфигурации, уровень автоматизации, уровень цифрового обмена)
- Жизненный цикл ПТК АСУТП (создание, внедрение, эксплуатация, обслуживание)

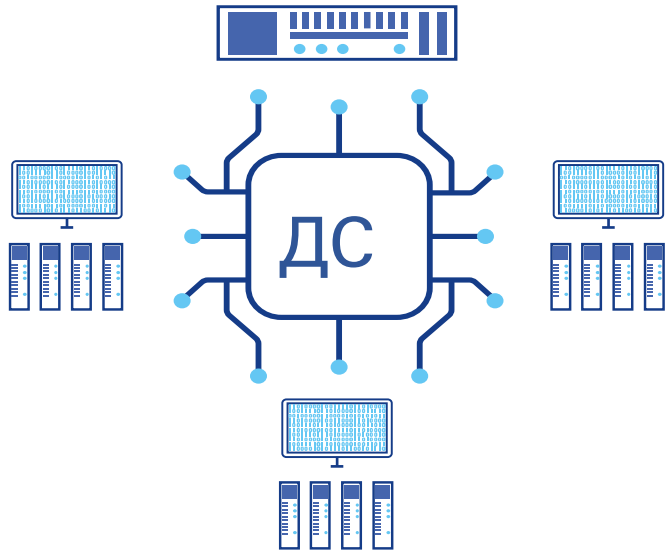
Эталонное – состояние, отклонение от которого является инцидентом!

Цели достигаемые эталонным состоянием системы:

1. **Снижение затрат на наложенные средства**
2. **Реальное повышение эффективности защиты**

Мониторинг эталонного состояния

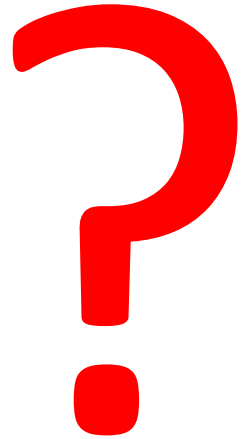
Однажды настроенное «Эталонное» состояние системы может быть изменено в процессе эксплуатации. Для подтверждения неизменности защищенного состояния системы должен проводиться постоянный автоматизированный мониторинг настроек.



Диагностическая станция

Наложенные средства защиты

А нужны ли они?



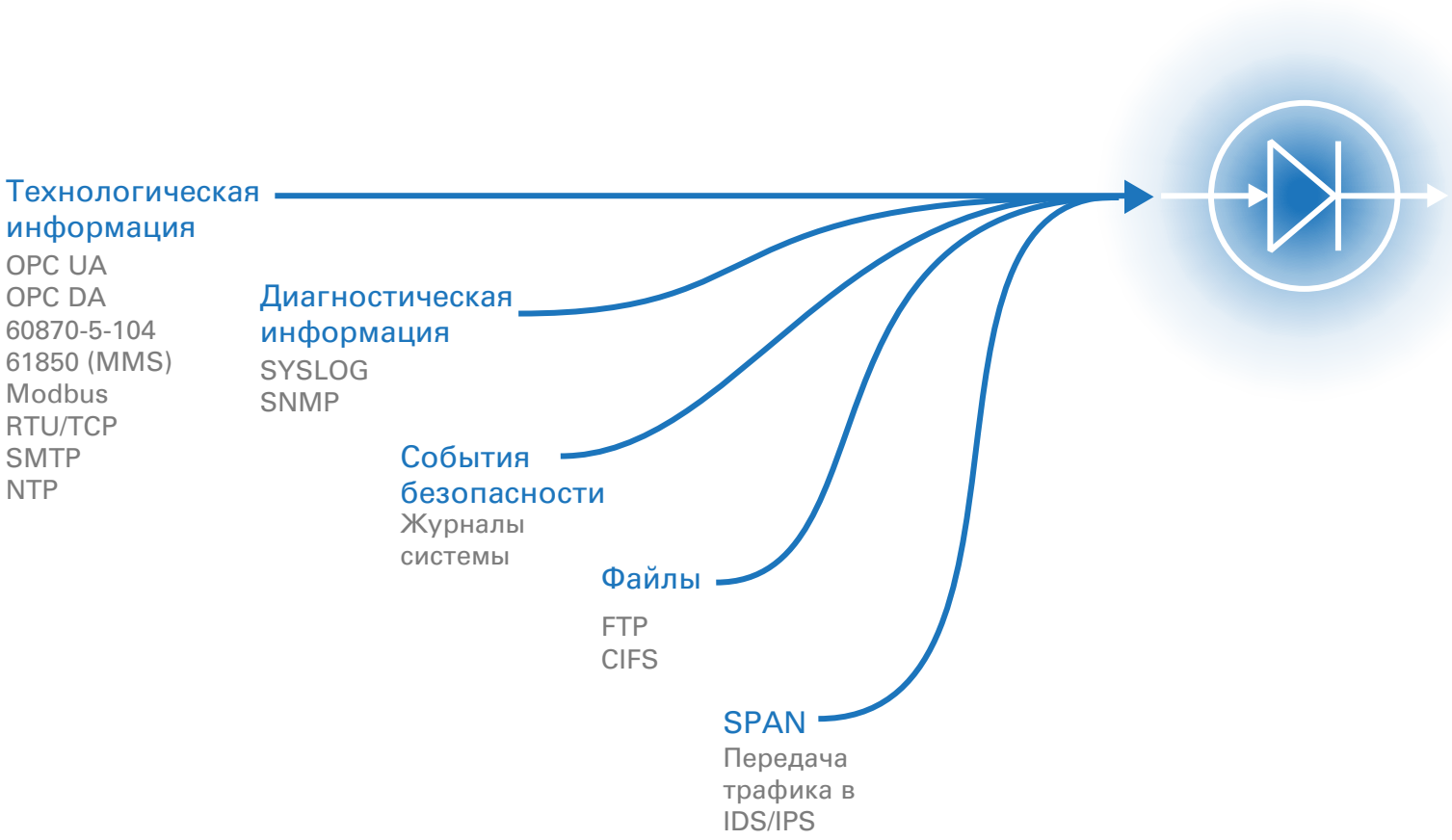
Для того чтобы ответить на этот вопрос, мы должны понять, а что осталось незащищенным?

Межсистемное взаимодействие

- **ПТК и Информационные системы**
- ПТК и ПТК
- ПТК и Диспетчерское управление

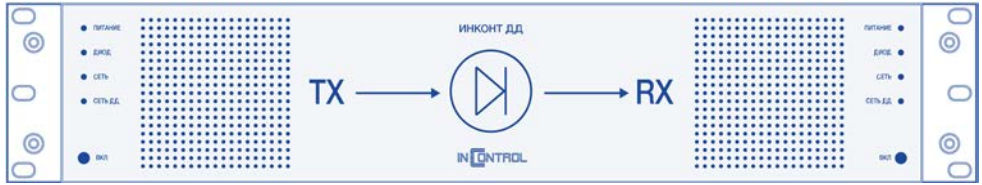
Межсистемное взаимодействие

ПТК и Информационные системы



Межсистемное взаимодействие

ПТК и Информационные системы



Устройство однонаправленной передачи данных

- Физическое отсутствие обратного канала связи;
- Бесшовное встраивание в существующую цифровую связь;
- Основные промышленные протоколы связи;
- Производительность до 200 000 тегов в секунду;
- Возможность работы с историческими данными;
- Кластерное исполнение.

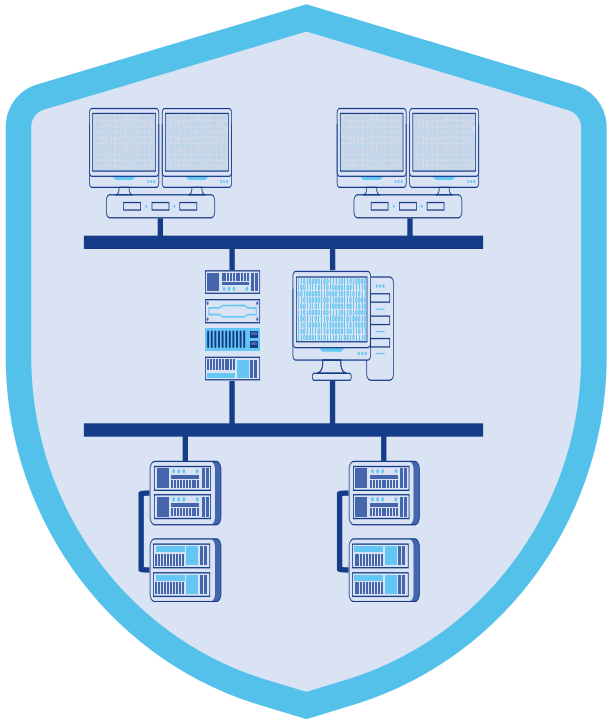
СОВМЕСТИМО С ПТК АСУТП

Межсистемное взаимодействие

- ПТК и Информационные системы
- **ПТК и ПТК**
- ПТК и Диспетчерское управление

Межсистемное взаимодействие

ПТК и Информационные системы



- Коммуникационные серверы
- Межсетевые экраны
- NGFW ?

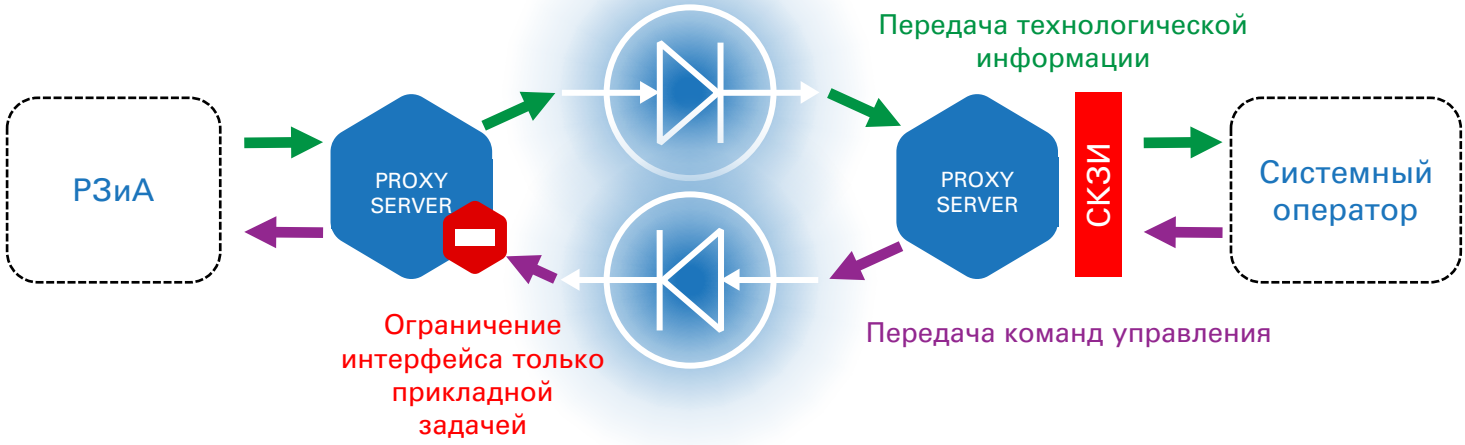
Межсистемное взаимодействие

- ПТК и Информационные системы
- ПТК и ПТК
- **ПТК и Диспетчерское управление**

Межсистемное взаимодействие

ПТК и Диспетчерское управление

ПТК ОПДУ – организация безопасного дистанционного управления



- Два юридических лица управляют одним технологическим процессом
- Две системы географически разнесены
- Не определена ответственность

Взаимодействие человека и машины

- **Физический доступ**
- Работа с HMI
- Удаленная работа с HMI
- Носители информации

Взаимодействие человека и машины

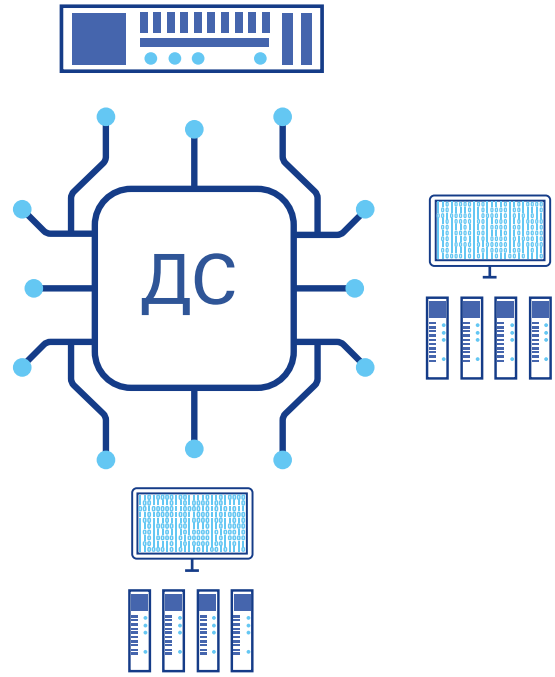
- Физический доступ
- **Работа с HMI**
- Удаленная работа с HMI
- Носители информации

Взаимодействие человека и машины

Работа с HMI

Эталонное состояние

+



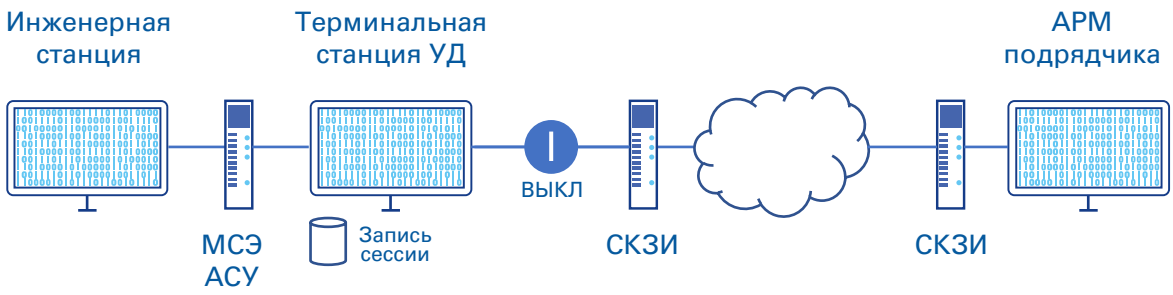
Диагностическая станция

Взаимодействие человека и машины

- Физический доступ
- Работа с HMI
- **Удаленная работа с HMI**
- Носители информации

Взаимодействие человека и машины

Удаленная работа с HMI



Защищенный удаленный доступ

Взаимодействие человека и машины

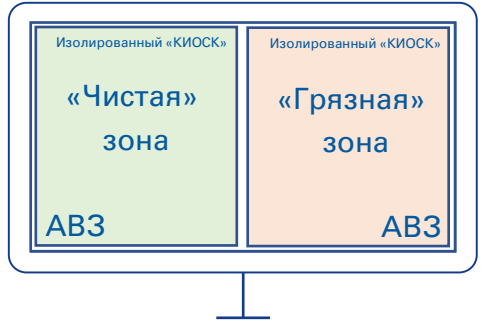
- Физический доступ
- Работа с HMI
- Удаленная работа с HMI
- **Носители информации**

Взаимодействие человека и машины

Внос\вынос файлов

- АРМ
- Сервер
- Контроллер

Специальный носитель



Любой внешний носитель

- Корпоративная сеть
- Подрядчик

Шлюз обмена файлами

Тестирование на совместимость

ПТК АСУТП - это набор разнородных компонент определенных версий, которые собраны воедино и функционально протестированы на совместимость и взаимную работоспособность.

- Резервное копирование и аварийное восстановление
- Средство антивирусной защиты
- Модули контроля целостности
- Системы мониторинга информационной безопасности
- Межсетевые экраны
- Встроенные средства защиты

Заключение

- Требуется **повышать зрелость ПТК АСУТП** с точки зрения информационной безопасности на этапе создания;
- Применяемые **сторонние средства защиты** рекомендуется **тестировать** разработчику также на этапе создания системы;
- **Без** привлечения специалистов **АСУТП построить работающую систему** обеспечения информационной безопасности **невозможно**;
- Применение **СЗИ без четко поставленной цели**, задачи и полного понимания объемов затрат на внедрение и эксплуатацию, скорее всего **приведет к неработоспособности** этого СЗИ.


ОКИИ
ЦОД
импортозамещение
ХВО
ЭТО
ГОСТ
ПТК АСУТП
SCADA
modbus
аудит
РЗиА
ИК.ДИОД
MMS
безопасность
законы
АВЗ
Мониторинг
спецификации
СКЗИ
Анализ угроз
контроллеры
Диагностическая станция
Тестирование на совместимость
меры
SIEM
Прикладное ПО
резервирование
приказы
60870-5-104
производство
защиты
ТМО
АВР
тестирование
дистанционное управление
технологии
187 ФЗ
шлюзы
ИК.ШОФ
Проектирование
Эталонное состояние
Шлюз обмена файлами
наладка
монтаж
КИИ
Уровень доверия
электропитание
ФСБ
ОРС DA
СОВ
функциональная безопасность
управление
МСЭ
САУ
61850
Удаленный доступ
Изоляция
ГОССОПКА
ОКИИ
Внедрение
сети
Математическое обеспечение
КСПД
ППР
ПТК ОПДУ
Реагирование
ФСТЭК
регламенты
goose
модернизация
Встроенные СЗИ
Обслуживание
ИК.УД
Защищенное исполнение
указы
ОРС UA
Оценка рисков
серверы
АРМ
события
утечки
нарушители
повреждение
ответственность
угрозы
взлом
ущерб
остановы
подмена
риски
уязвимости
потеря контроля
аварии
инциденты
Несанкционированный доступ
разрушение