INFOWATCH® ARMA

ЧТО И КАК ЗАЩИЩАТЬ В АСУ ТП?

Переосмысление концепции ИБ АСУ ТП в 2023 году

ИБ АСУ ТП — 2022. Влияние инцидентов ИБ на деятельность организаций

— **Наибольшее влияние** инцидентов ИБ на деятельность организаций отмечено в госсекторе и топливно-энергетическом комплексе

— **Умеренный и значительный** ущерб коснулся как минимум половины организаций во всех отраслях

— **Наиболее разрушительные** для деятельности инциденты ИБ вызвали полную остановку производства

Источник: The state of the industrial security in 2022

ИБ АСУ ТП — 2023. Факторы

1. Изменение ландшафтов ИТ и АСУ
2. Усиление нормативного регулирования ИБ
3. Рост активности компьютерных злоумышленников

ИБ на промышленном предприятии

- Эффективность организационных мер
- Необходимость документирования
- Ограниченность ресурсов
- Разрозненная информация
- Реагирование на простые и понятные инциденты
- Сотни данных с СОВ, требующих обработки
- Создание комплексных систем защиты на базе СрЗИ с простыми сценариями реагирования

Управление системой ИБ. Процессный подход

Жизненный цикл ИБ

Модель зрелости процессов в соответствии с требованиями ISO/IEC 21827
«Инжиниринг систем безопасности — модель зрелости возможностей»

Базовые практики выполнены

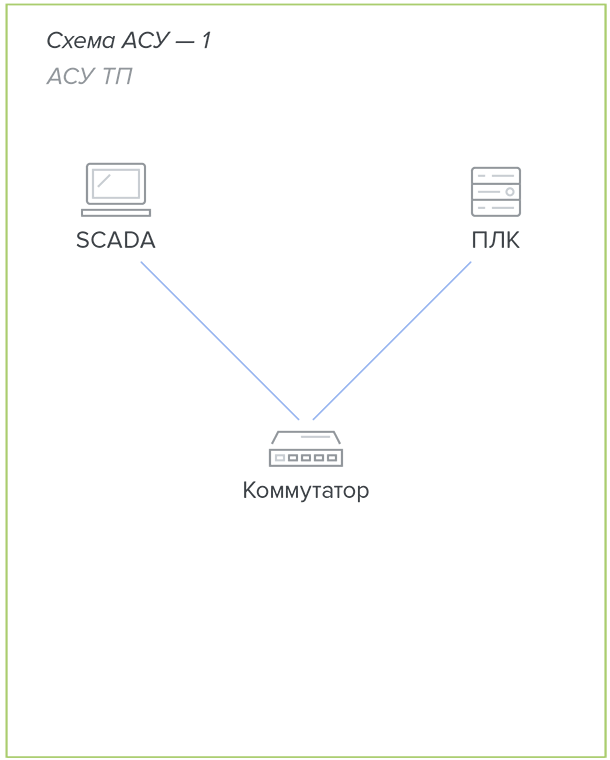
- **Поручение** выполнения
- **Планирование** выполнения
- **Дисциплинарное** выполнение
- **Прослеживание** выполнения
- **Верификация** выполнения

- **Определение** стандартного процесса
- **Адаптация** стандартного процесса
- **Использование** данных
- **Выполнение** определённого процесса

- **Установление** измеримых целей качества
- **Определение** возможности процесса для достижения целей
- **Объективное** руководство выполнением

- **Установление** количественных целей эффективности процесса
- **Улучшение** эффективности процесса

Современная картина ИБ предприятия ТЭК



Особенности

- Контролируемый физический доступ
- Плановое управление изменениями
- Ручной контроль и реагирование на нештатные ситуации

Вызовы

- Ограниченность ресурсов ИБ
- Отсутствие технической поддержки импортных систем АСУ
- Сложности обновления ПО и эксплуатации антивирусов

Защита рабочих станций и серверов

Организационные меры

— Доступ пользователей и авторизация

— Проверка съёмных носителей информации

— Проверка подключаемых устройств

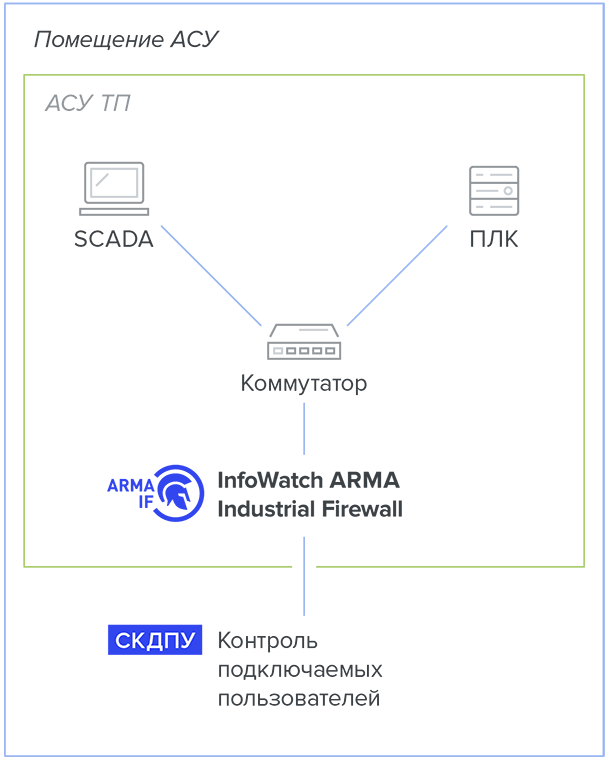
СрЗИ

— Контроль подключаемых устройств

— Белые списки приложений

— Логирование действий и событий

Защита сети



СрЗИ

— Сегментирование сети

— Авторизация подключаемых по сети пользователей

— DoS-проверка

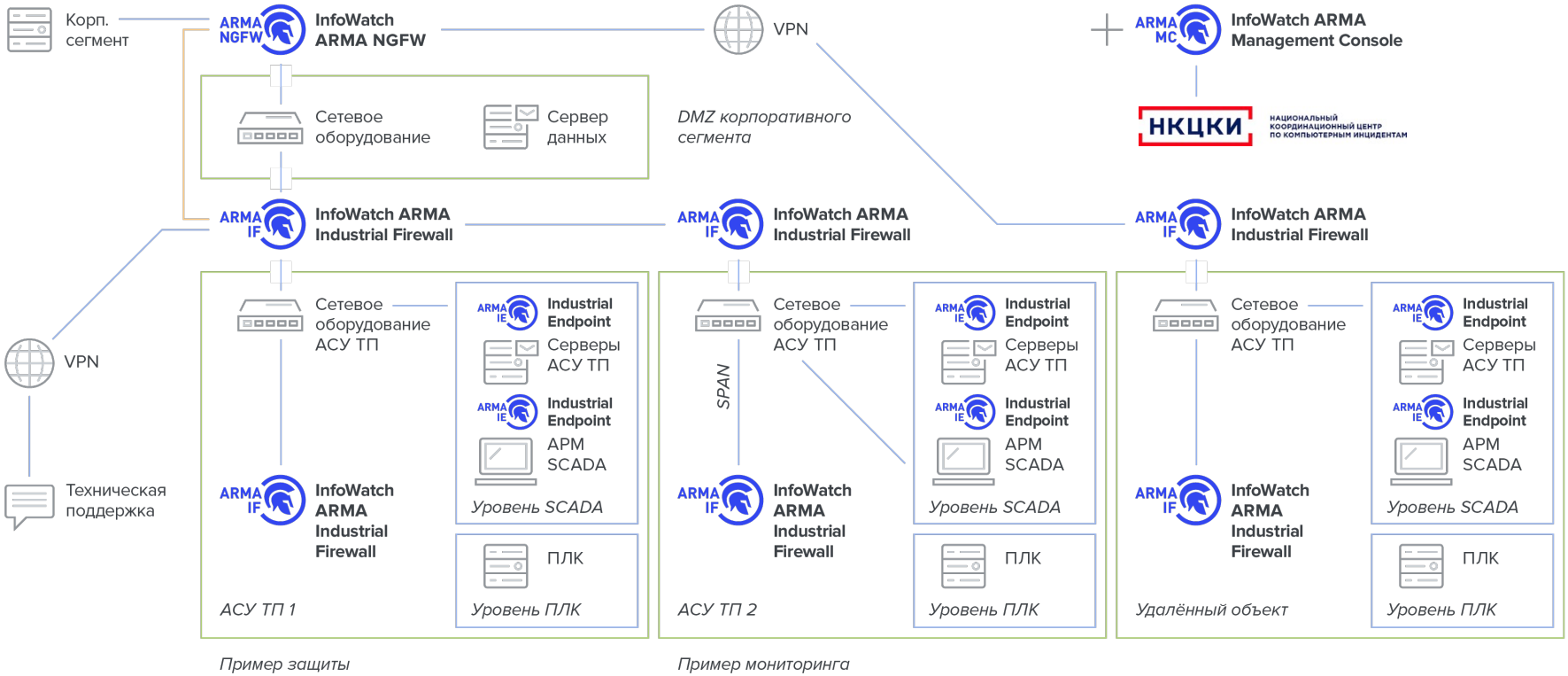
— Запрет всех подключений, кроме разрешённых связей с другими системами автоматизации и управления производством

— Фильтрация по типу протокола

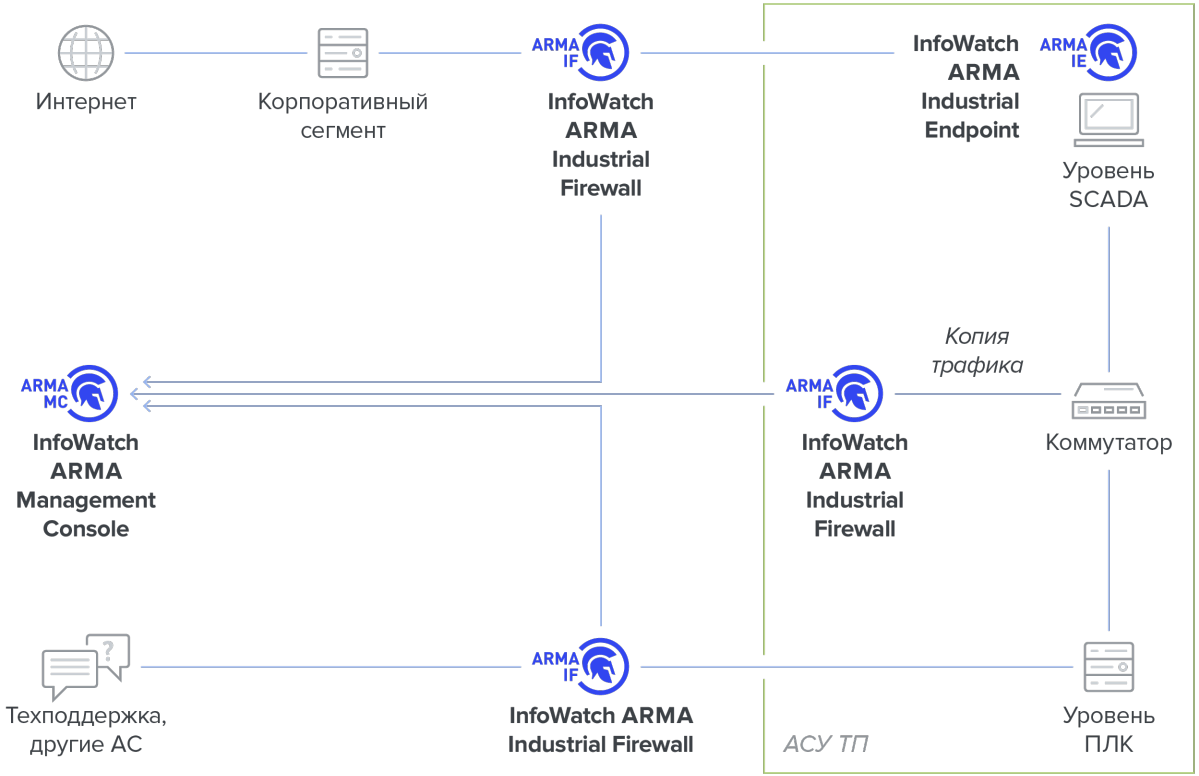
— Выявление новых устройств

— Защищённые соединения

Пример решения



Сценарии применения решений ИБ



- Удалённая наладка, эксплуатация и техническая поддержка продукта
- Защита рабочих станций и сети от угроз и уязвимостей для минимизации простоев, включая техническое обслуживание
- Дополнительный мониторинг состояния оборудования и сети
- Пограничное средство связи
- Автоматизация реагирования на инциденты, включая восстановление работоспособности системы

INFOWATCH® ARMA

ПРИГЛАШАЕМ К СОТРУДНИЧЕСТВУ

arma.infowatch.ru

/InfoWatchOut /InfoWatch