**Пояснительная записка к техническому решению**

**1. Цель проекта**

Интеграция 16 объектов АСУ ТП (категории значимости 2 и 3) в корпоративный SOC компании, обеспечивая централизованный мониторинг, реагирование на кибер-инциденты и соответствие приказу ФСТЭК № 239.

**2. Архитектура решения**

* Лог-коллекторы на каждой площадке: поддержка Syslog/CEF, буферизация > 7 суток, передача логов по VPN-каналу.
* Сетевой периметр: разделение OT и IT через двухзонный DMZ (российские NGFW).
* Средства ИБ: EDR, RBAC + MFA, централизованный журнал событий.
* SOC-интеграция: единый формат логов, движок корреляции, SOAR-плейбуки.
* Надёжность: ежедневные off-site backup, ежеквартальное тестирование восстановления.
* Обучение: цикл тренингов для эксплуатационного и ИБ-персонала.

**3. Процедура реагирования на инцидент «Отказ системы ХВП»**

* Предиктивный мониторинг подачи реагентов (σ-контроль) - SLA < 1 мин
* Срабатывание датчиков качества воды (SCADA+SIEM) - SLA ≤ 5 с
* Запуск ПАЗ-байпаса ХВП - SLA ≤ 2 с
* Дистанционный стоп подачи пара - SLA ≤ 5 с
* Промывка и инспекция турбины - SLA ≤ 12 ч

**4. Риски и меры**

* Техническая несовместимость контроллеров - разработка адаптеров, пилоты.
* Отсутствие актуальной документации - опрос, инвентаризация.
* Низкая цифровая зрелость персонала - обучение, методички.
* Регуляторное несоответствие - Waterfall-документация, аудит.

**5. Вывод**

Предложенное решение минимизирует риски, повышает кибер-устойчивость ОКИИ  
и укладывается в сроки **01.05.2025 – 01.11.2026** благодаря гибридной методологии (Waterfall + Agile).