**Часть 2. Текст выступления (пример ~7 минут)**

**Слайд 1 — Вступление**  
Добрый день, уважаемые члены комиссии. Наша команда представляет проект «Интеграция значимых объектов КИИ в корпоративный SOC». Проект длится 18 месяцев — с мая 2025 до ноября 2026 года — и ориентирован на выполнение требований 187-ФЗ и Приказа ФСТЭК № 239.

**Слайд 2 — Команда**  
Позвольте представить участников: я, *Виталий*, руководитель проекта; мой коллега *Илья* — главный инженер; архитектор *Богдан*; инженеры: *Владислав*, *Сергей, Владимир.* Каждый несёт персональную ответственность за отдельное направление, что позволяет удерживать контроль над сроками и качеством.

**Слайд 3 — Методология**  
Мы выбрали гибрид Waterfall + Agile. Формализованные этапы согласования документации закрываются Waterfall-подходом, что критично для регулятора. А технически рисковые задачи — аудит, пилот и тиражирование — выполняются Agile-спринтами, что даёт гибкость и раннюю обратную связь.

**Слайд 4 — План-Гант**  
Диаграмма отражает пять фаз. Ключевые контрольные точки: завершение аудита — декабрь 2025; успешный пилот — июнь 2026; полное тиражирование — октябрь 2026; приёмка — ноябрь 2026 г.

**Слайд 5 — Ресурсы**  
Проект опирается на шесть основных FTE (каждый отвечает за свою часть работы, распределены зоны ответсвенности), а также экспертов вендоров. Аппаратная часть — лог-коллекторы, СЗИ: NGFW, криптошлюзы, НСД; программная — лицензии на ПО по сбору логов с АСУ ТП; плюс обучение персонала на четырёх площадках.

**Слайд 6 — Бюджет**  
Сейчас идёт детализация закупочных цен, поэтому все финансовые ячейки отмечены жёлтым. Финальную смету представим к 31 мая 2025 года после инвентаризации оборудования.

**Слайд 7 — Недопустимые события**  
Главное: отказ химводоподготовки, ведущий к разрушению турбины. Дополнительно: потеря управления SCADA и компрометация DMZ.

**Слайд 8 — Сценарий ХВП**  
Показаны четыре стадии атаки согласно MITRE ATT&CK for ICS. Критический момент — подмена телеметрии датчиков, из-за чего система не успевает остановить подачу пара.

**Слайд 9 — Ключевые системы**  
Основные контроллеры — Siemens PCS 7 и Schneider Triconex. Защиту обеспечивает стек российских NGFW, лог-коллекторы и MaxPatrol SIEM; автоматизацию реагирования — R-Vision SOAR.

**Слайд 10 – 11 — Критерии и Процедура реагирования**  
Мы определили пороговые значения технологических параметров и связали их с триггерами SIEM. Процедура реагирования охватывает семь шагов — от выявления до RCA — с обозначением времени SLA на каждом этапе.

**Слайд 12 — RACI**  
Ответственность распределена так, чтобы технические службы занимались локализацией, а департамент ИБ контролировал анализ причин и отчётность ФСТЭК.

**Слайд 13 — Структурная схема**  
Логическая схема показывает защищённый поток журналов от АСУ ТП через OT/IT DMZ в SOC с резервированным VPN-каналом.

OT (Operational Technology) — технологические сети и системы управления АСУ ТП;

IT (Information Technology) — корпоративная ИТ-инфраструктура (офисные ЛВС, серверные, облака, SOC)

**Слайд 14 — Документация**  
Все исходные документы доступны в общем репозитории. Это обеспечивает транспарентность и возможность аудита.

**Заключение**  
Реализация проекта повысит кибер-устойчивость критически важных объектов, сократит время реакции на инциденты и обеспечит полное соответствие нормативным требованиям. Готов ответить на ваши вопросы.