# Устав проекта

**Название проекта**: «Интеграция значимых ОКИИ АСУ ТП в корпоративный SOC»

**Инициатор проекта**: компания «Страна Плюс»

**Дата начала проекта**: 01.05.2025

**Планируемая дата завершения**: 01.11.2026 (18 месяцев)

# 1. Цели проекта

Обеспечить мониторинг событий и управление инцидентами информационной безопасности (ИБ) на значимых объектах критической информационной инфраструктуры (ОКИИ) категорий 2 и 3 в соответствии с Федеральным законом № 187-ФЗ и Приказом ФСТЭК № 239. Цель достигается путем подключения всех технически совместимых АСУ ТП (около 16 объектов) к корпоративному центру кибербезопасности (SOC).

# 2. Область проекта

**География:** 4 предприятия в двух регионах РФ.

**Объекты:** значимые ОКИИ (АСУ ТП на платформах Siemens и Schneider Electric, около 4 объекта на предприятие).

**Задачи:**

* Проведение аудита АСУ ТП для оценки возможности логирования.
* Внедрение средств логирования, сбора и передачи событий безопасности.
* Интеграция событий с корпоративным SOC.
* Проведение пилотного внедрения на одном предприятии.
* Масштабирование решения на остальные предприятия.
* Обучение персонала заказчика основам мониторинга и реагирования.

**Результат:** Полностью функционирующая система мониторинга событий ИБ, интегрированная с SOC, с подготовленным персоналом.

# 3. Ограничения проекта

* Устаревшее оборудование (ввод в эксплуатацию ~15 лет назад, Siemens и Schneider Electric).
* Отсутствие встроенных решений для логирования событий.
* Низкая квалификация персонала заказчика в области ИБ.
* Географическая распределенность (два региона).
* Необходимость уточнения бюджета на основе аудита систем.

# 4. Предполагаемые риски

|  |  |  |
| --- | --- | --- |
| **Риск** | **Описание** | **Меры минимизации** |
| Невозможность логирования | Устаревшие платформы могут не поддерживать сбор событий. | Проведение аудита систем, консультации с вендорами (Siemens, Schneider Electric). |
| Задержки в настройке | Сложности с конфигурацией Log коллекторов. | Пилотное внедрение для тестирования решений. |
| Недостаточная квалификация персонала | Персонал заказчика не имеет опыта работы с SOC. | Итеративное обучение в рамках Agile-этапов. |
| Зависимость от вендоров | Ограниченная поддержка из-за зарубежных поставщиков. | Закупка совместимых решений, поиск альтернативных поставщиков. |
| Логистические сложности | Распределенность предприятий усложняет развертывание. | Поэтапное масштабирование, координация через Jira. |

# 5. Методика и подход

**Методика**: Гибридная (Waterfall + Agile).

**Подход**: Поэтапный, с пилотным внедрением на одном предприятии и последующим тиражированием.

**Этапы**:

* + Месяцы 1–3 (05.2025–07.2025): Категорирование и документация (Waterfall).
  + Месяцы 4–6 (08.2025–10.2025): Аудит и прототипирование (Agile).
  + Месяцы 7–12 (11.2025–04.2026): Пилотное внедрение (Agile).
  + Месяцы 13–17 (05.2026–09.2026): Масштабирование (Agile).
  + Месяц 18 (10.2026–11.2026): Отчетность и сдача (Waterfall).

# 6. Команда проекта

| **Имя** | **Роль** |
| --- | --- |
| Новиков В.С. | Руководитель проекта (координация, отчетность) |
| Орлов И.Н. | Главный инженер (техническое руководство) |
| Садриев Б.А. | Архитектор проекта (проектирование решения) |
| Белов С.В. | Инженер (техническая реализация) |
| Москвин В.Д. | Инженер (техническая реализация) |
| Фролов В.Д. | Инженер (техническая реализация) |

# 7. Бюджет

**Статус** - предварительная смета должна быть подготовлена и утверждена до 31.05.2025. На май 2025 предполагается, что бюджет находится в стадии финального согласования.

**Ориентировочные статьи расходов**:

* + Аудит АСУ ТП.
  + Закупка и установка Log коллекторов.
  + Лицензии для интеграции с SOC.
  + Обучение персонала.
  + Координация и логистика между регионами.

Следующие шаги предусматривают уточнение бюджета после аудита систем (месяцы 4–6, 08.2025–10.2025).

# 8. Критерии успешности

* Подключение к SOC всех технически совместимых АСУ ТП (стремление к 100% охвату значимых ОКИИ).
* Полная интеграция событий в корпоративный SOC.
* Соответствие системы требованиям Приказа ФСТЭК № 239.
* Обученный персонал, способный выполнять базовые функции мониторинга и реагирования.

# 9. Нормативная база

* Федеральный закон № 187-ФЗ «О безопасности КИИ».
* Приказ ФСТЭК № 239.
* ГОСТ Р 54869-2011 (управление проектами).