**Отчёт по проекту интеграции АСУ ТП значимых объектов ОКИИ в корпоративный SOC**

**1. Проектное решение и структурная схема**

**1.1 Формат и стандарты разработки схем**

* **Стандарты:** ГОСТ 21.408‑2013 - условные графические обозначения.
* **Цветовая дифференциация компонентов:**  
  • **Серый** - физические объекты (заводы, площадки)  
  • **Синий** - защищаемые ИТ‑системы (АСУ ТП)  
  • **Красный** - компоненты кибербезопасности (СЗИ, Лог‑коллекторы, DMZ, SOC)  
  • **Зелёный** - смежные системы (ПАЗ, диспетчеризация, инженерные системы)

**1.2 Состав элементов структурной схемы**

|  |  |
| --- | --- |
| Категория | Элементы |
| Физические объекты | 4 предприятия (2 региона), производственные и энергетические площадки |
| Защищаемые системы | 16 АСУ ТП (по 4 на объект), САУ, SCADA, система управления химводо‑подготовкой |
| Компоненты ИБ | лог‑коллекторы, DMZ, SOC, СЗИ, EDR/MDR, криптошлюзы с VPN, межсетевые экраны, контроль доступа |
| Смежные системы | ПАЗ, диспетчеризация, фидеры, инженерные коммуникации |

**1.3 Краткое текстовое описание взаимодействий**

1. АСУ ТП объектов подключены к локальной OT‑сети; журналы отправляются на локальный Лог‑коллектор.
2. Через OT/IT‑DMZ логи передаются в центральную SIEM SOC по VPN + TLS.
3. Компоненты СЗИ (EDR/MDR, NGFW, криптошлюзы) размещены в зонах риска и шлют события в лог‑коллектор.
4. ПАЗ и диспетчеризация интегрированы через защищённые шлюзы.

**1.4 Минимальная обзорная структурная схема (логическая)**



**2. Назначения и распределение ролей**

|  |  |  |
| --- | --- | --- |
| Имя | Роль | Основные обязанности |
| Новиков В.С. | Руководитель проекта | Координация, контроль сроков, взаимодействие с заказчиком, отчётность |
| Орлов И.Н. | Главный инженер | Техническое руководство, контроль качества инженерных решений |
| Садриев Б.А. | Архитектор проекта | Проектирование архитектуры, разработка схем, формат логов, DMZ дизайн |
| Белов С.В. | Инженер | Реализация прототипов, тестирование систем сбора данных |
| Москвин В.Д. | Инженер | Настройка оборудования, установка лог‑коллекторов |
| Фролов В.Д. | Инженер | Интеграция агентов, полевые тесты, поддержка |

**3. Пояснительная записка к техническому решению**

**3.1 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.

**3.2 Обзор архитектуры решения**

* **Лог‑коллекторы** на каждой площадке: поддержка Syslog/CEF, буферизация > 7 суток, передача логов по VPN‑каналу.
* **Сетевой периметр**: строгое разделение OT и IT через двухзонный DMZ; импортозамещение оборудования (российские NGFW, криптошлюзы, коммутаторы).
* **Средства ИБ**: АВЗ / EDR/MDR, RBAC + MFA, сегментированный доступ, централизованный журнал событий.
* **SOC‑интеграция**: единый формат логов, движок корреляции, SOAR‑плейбуки (низко‑уровневое реагирование), орг‑процедуры.
* **Надёжность**: ежедневные off‑site backup, ежеквартальное тестирование восстановления конфигураций и журналов.
* **Обучение персонала**: цикл тренингов (основы кибербезопасности, работа с SIEM, реагирование на инциденты).

**3.3 Предотвращение и реагирование на недопустимое событие «Отказ системы ХВП»**

|  |  |  |  |
| --- | --- | --- | --- |
| Этап | Контроль | Средство | SLA |
| Предиктивный | Мониторинг подачи реагентов | Алгоритм корреляции «отклонение > 3 σ» | < 1 мин до события |
| Обнаружение | Датчики качества воды | SCADA + SIEM триггер | ≤ 5 с |
| Сдерживание | Аварийный ПАЗ‑запуск байпаса ХВП | ПАЗ‑контроллер | ≤ 2 с |
| Ликвидация | Дистанционный стоп подачи пара | Система управления турбиной | ≤ 5 с |
| Восстановление | Промывка системы, инспекция турбины | РД по аварийному ремонту | ≤ 12 ч |

**4. Оценка и управление рисками**

**4.1 Матрица рисков**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Риск | Вероятность | Влияние | Стратегия | Ответственный |
| 1 | Техническая несовместимость старых контроллеров | Высокая | Среднее | Разработка адаптеров, пилоты | Садриев Б.А. |
| 2 | Отсутствие актуальной документации | Средняя | Среднее | Опрос на месте, инвентаризация | Орлов И.Н. |
| 3 | Низкая цифровая зрелость персонала | Средняя | Низкое | Обучение, методички | Белов С.В. |
| 4 | Регуляторное несоответствие | Низкая | Высокое | Waterfall‑документы, аудит | Новиков В.С. |

**4.2 Планы реагирования на критические инциденты**

* **Отказ ХВП** - см. § 3.3.
* **Failure OT/IT DMZ** - автоматическое переключение на резервный канал VPN L2; оповещение SOC.

**5. Методология управления проектом**

**5.1 Обоснование выбора гибридной методологии**

* **Waterfall** - формализованные этапы с регуляторной отчётностью (ТЗ, макеты схем, финальный отчёт).
* **Agile** - пилотное внедрение, спринты по 2 недели, быстрая обратная связь, корректировка backlog.

**5.2 Этапы реализации и контрольные точки**

|  |  |  |  |
| --- | --- | --- | --- |
| Этап | Период | Методология | Основной результат |
| 1 | 01.05–31.08.2025 | Waterfall | Согласованное ТЗ, план проекта |
| 2 | 01.09–31.12.2025 | Agile | Аудит АСУ ТП, backlog пилота |
| 3 | 01.01–30.06.2026 | Agile | Пилот на площадке № 1, доработка |
| 4 | 01.07–31.10.2026 | Agile | Тиражирование решения на 3 площадки |
| 5 | 01.11.2026 | Waterfall | Итоговое тестирование, приёмка |

**Приложение А. Текстовое описание структурной схемы**

1. **Транспортный уровень** - MPLS‑каналы операторов, резерв - спутниковый Ku‑band, все через криптошлюзы.
2. **DMZ‑зона** - два NGFW в режиме Active/Active, проверка OT → IT только после DPI SCADA.
3. **SIEM** - кластер N+1, корреляционные правила согласно матрице MITRE ATT&CK for ICS.

**Приложение Б. Глоссарий терминов**

* **АСУ ТП** - автоматизированная система управления технологическим процессом.
* **СЗИ** - средство защиты информации.
* **ХВП** - химводо‑подготовка.
* **ПАЗ** - противоаварийная защита.
* **DMZ** - демилитаризованная зона.