# Процесс реагирования на инцидент ИБ: Нарушение химводоподготовки

## Недопустимое событие

Нарушение работы системы химводоподготовки, в результате которого загрязнённый пар оседает на лопатках турбины, приводя к их разрушению. Авария затрагивает критически важные объекты КИИ.

## Цели реагирования

- минимизировать время между обнаружением и локализацией инцидента;  
- предотвратить физические повреждения оборудования;  
- сохранить доказательную базу;  
- соблюсти требования 187-ФЗ и Приказа ФСТЭК № 239.

## Последовательность реагирования

### 1. Выявление и регистрация

* срабатывание корреляции в SIEM (SOC 1 линия);
* регистрация события в ITSM / SOAR;
* присвоение категории High и ID инцидента.

### 2. Первичный анализ и классификация

* проверка события SOC 1 линия;
* анализ SCADA и ПАЗ логов (SOC 2 линия);
* эскалация до уровня Инцидент ИБ К1 (КИИ).

### 3. Эскалация и уведомление

* уведомление дежурного инженера ЦТАИ и начальника смены;
* информирование ИБ-службы, ПАЗ;
* уведомление ФСТЭК (в течение 1 часа при подтверждении), ГосСОПКА.

### 4. Локализация

* перевод на резервную линию водоподготовки;
* перевод узлов в безопасный режим (ПАЗ);
* изоляция сегмента (ICS администратор).

### 5. Ликвидация последствий

* Нормализация состава воды (Химцех);
* Очистка турбины (Турбинный цех);
* Восстановление SCADA (OT-инженеры).

### 6. Восстановление

* подтверждение качества воды лабораторией;
* постепенный запуск турбины;
* проверка конфигураций САУ / АСУ ТП.

### 7. Анализ причин и меры

* RCA (Root Cause Analysis) комиссией;
* модернизация настроек СЗИ и ПАЗ;
* план учений.

### 8. Закрытие инцидента

* закрытие инцидента SOC;
* отчет в ФСТЭК (форма 1), ГосСОПКА;
* обновление базы знаний.

## Матрица ответственности (RACI)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Этап | Ответственный (R) | Утверждающий (A) | Консультируемый (C) | Информируемый (I) |
| Выявление | Сменный инженер SOC (1 линия) | Руководитель SOC | Инженеры ПАЗ | Начальник смены станции |
| Анализ | Сменный инженер SOC (2 линия) | Руководитель департамента ИБ | ICS-администраторы | Главный инженер |
| Локализация | Начальник смены станции | Директор ТЭЦ | Инженер ПАЗ | SOC, химический цех |
| Ликвидация | Инженер ПАЗ | Главный инженер | Химический цех | SOC, турбинный цех |
| Восстановление | Начальник смены станции | Главный инженер | Лаборатория | SOC |
| Анализ причин | Руководитель службы аудита, аналитик угроз (3 линия) | Зам. гендиректора по ИТ | Команда проекта | ФСТЭК ГосСОПКА |
| Закрытие инцидента | Руководитель департамента ИБ | Зам. гендиректора по ИТ | SOC | Все службы |

## Привязка к MITRE ATT&CK for ICS

|  |  |  |
| --- | --- | --- |
| Этап атаки | Техника | Код |
| Манипуляция управлением | Manipulation of Control | T0810 |
| Подмена телеметрии | Spoof Reporting | T0811 |
| Остановка критических служб | Service Stop | T0831 |
| Использование удаленных средств | Remote Services | T0851 |

## Применяемые средства

- SIEM: MaxPatrol SIEM (любой MDR)

- SOAR: R-Vision

- СЗИ: МЭ (UserGate), СОВ (UserGate), РДП-шлюзы (Indeed PAM), АВЗ (KES) на конечных точках

- ПАЗ: Siemens PCS 7, Schneider Electric Triconex

## Нормативная база

- 187-ФЗ: О безопасности КИИ  
- Приказ ФСТЭК № 239: Требования к СИБ КИИ  
- ГОСТ Р 57580.2–2018: Управление инцидентами ИБ  
- ГОСТ Р 54869–2011: Управление проектами