

Система управления процессом регенерации кислорода станции в колонии N поддерживает постоянную концентрацию пригодного для дыхания воздуха с отклонениями не более 0,001. Регенерация кислорода осуществляется посредством электролиза воды, данные о котором поступают на пункт управления.

Здоровье поселенцев сильно зависит от исправной работы этой системы; в её истории есть пара трагических моментов. Так, однажды, в систему управления станцией приходили ошибочные данные об отсутствии напряжения на электродах центральной ванны, - это привело к тому, один из инженеров получил электроожоги такой степени, что остался инвалидом. Последний случай сбоя в системе управления был зафиксирован сравнительно не давно, и заключался в отказе подсистемы датчиков контроля качества воздуха (вражеский вирус блокировал передачу данных). Это привело к тому, что пострадали 42 мирных жителя, проживавших внутри колонии N, которую обслуживает данная станция. Специалисты по безопасности компании OpenOxygen, которая обслуживает станцию, утверждают, что все опасности, помимо блокировки передачи данных вражеским ВПО и передачи ошибочных данных на АСУ, для системы не актуальны! У нас нет повода не доверять им.

Выберите базовый необходимый набор мер ЗИ для данной системы.

**Формат флага:** номера необходимых ЗИ через запятую.

# Классификация ЧП

Из исторических данных и заверений «специалистов» мы можем определить максимальный вред, который могут повлечь аварии на данной **ключевой системе информационной инфраструктуры.**

В соответствии с **Постановлением N. 304 от 21.05.2007**

первую ЧП можно классифицировать как "ЧП локального характера" (ЧП не вышло за границы объекта, пострадало не более 10 человек),

а вторую – как "ЧП муниципального характера" (ЧП не вышло за границы одного поселения, пострадало не более 50 человек).



# Применение 31-Приказа ФСТЭК

В соответствии с **Приказом ФСТЭК N. 31 от 14.03.2014** наша АСУП обрабатывает два вида информации,

при этом для первой системы значимо только свойство целостности, а для второй -- доступности, если все угрозы, кроме перечисленных, не актуальны.

Получается, в обоих случаях определен низкий уровень ущерба (ЧП локального и муниципального характеров), следовательно в обоих случаях мы имеем низкий уровень критичности (УЗ 3).

Получаем требуемый класс защищенности АСУ: **КЗ**

# Выбор мер ЗИ

В соответствии с Приказом ФСТЭК Н. 31 от 14.03.2014 для КЗ:

- + 1. Идентификация и аутентификация пользователей, являющихся работниками оператора
- + 2. Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)
- 3. Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
- + 4. Ограничение неуспешных попыток входа в автоматизированную систему управления (доступа к системе)
- 5. Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения
- + 6. Учет машинных носителей информации
- + 7. Управление доступом к машинным носителям информации
- 8. Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации
- + 9. Контроль подключения машинных носителей информации
- + 10. Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них



# Выбор мер ЗИ (продолжение)

- 11. Генерирование временных меток и (или) синхронизация системного времени в автоматизированной системе управления
- 12. Обнаружение вторжений
- + 13. Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации
- 14. Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации
- 15. Контроль точности, полноты и правильности данных, вводимых в автоматизированную систему управления
- 16. Использование отказоустойчивых технических средств
- + 17. Регистрация событий безопасности в виртуальной инфраструктуре
- 18. Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных

**Таким образом получается флаг: 1,2,4,6,7,9,10,13,17**