Аудит ИБ АСУ ТП

Роман Попов

e·on

Антон Ёркин

УЦСБ
Интегратор Сильных Решений

Информация о докладчиках

Роман Попов

Начальник ОИБ

20 лет в ИТ

10 лет в ИБ

1 год в ИБ АСУ ТП

Антон Ёркин

CISA

11 лет в ИБ

8 лет Аудитов ИБ

5 лет Аудитов ИБ АСУ ТП

e·on

УЦСБ

Интегратор Сильных Решений

Совместный проект по аудиту ИБ АСУ ТП

Заказчик – Э.ОН Россия, г. Москва

Аудитор – УЦСБ, г. Екатеринбург

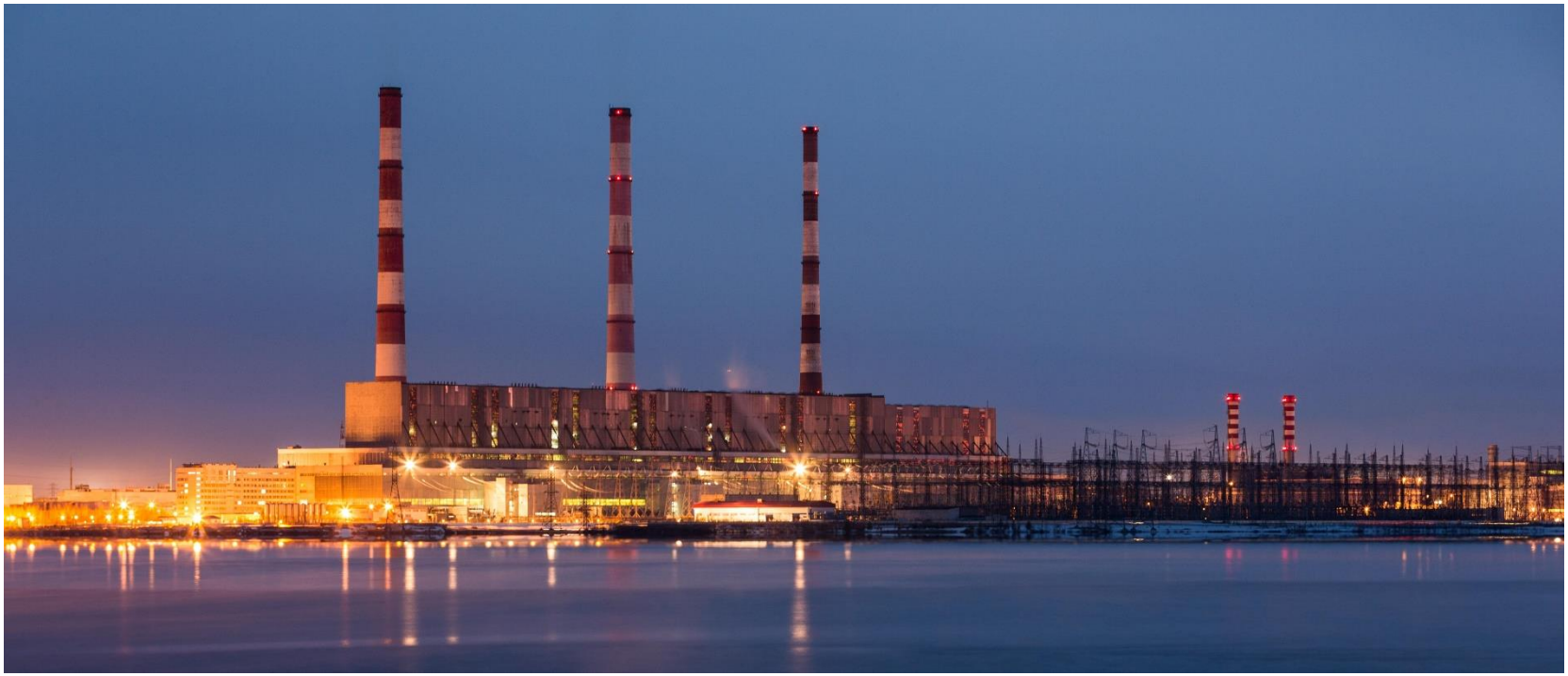
Область работ – АСУ ТП ГРЭС

Длительность основного этапа – 3 месяца

Длительность инструментального аудита – 1 год

Область аудита

- Самая крупная электростанция России по выработке электроэнергии
- Вторая по мощности тепловая электростанция в мире
- Установленная мощность станции составляет 5597,1 МВт



АСУ ТП ГРЭС

- ПИК Прогресс
- Emerson Process Management
- General Electric
- Siemens
- НТЦ Комплексные системы

Обрабатывается более 100 000 параметров работы технологического оборудования

Старт проекта

- Получаем поддержку снизу
  - Аудит – это не проверка, а квалифицированный доп. ресурс для решения накопившихся вопросов
- Получаем поддержку сверху
  - Информационный шум
  - Очень недорого за уверенность в завтрашнем дне
  - «Требования» регуляторов
  - «Принятие рисков»

= Инициатор - производственники

Зачем ИБ в АСУ ТП / Общие вызовы

В 2015 г. в России средний ущерб от инцидента ИБ увеличился с $3,6 млн до $5,3 млн (на 47% по сравнению с 2014 г.).[1]

PricewaterhouseCoopers

В тоже время ущерб от хакерских атак на системы интернет-банкинга в России упал в 3,7 раза до 2,6 млрд руб. по сравнению с 9,8 млрд руб. в 2014 году. Хакеры уходят в другие отрасли.

Group-IB

Кибератаки 2015 направлены на все сферы, особую распространенность получили т. н. разрушительные атаки (destructive attacks).[2] 2014 - серия эффективных DDoS-атак на ЦБ и МИД России, 2015 - в открытый доступ выложены сотни тысяч SMS-сообщений россиян, атак на промышленные предприятия.

Александр Бодрик. CISA, эксперт ЦИБ

В 2014 году 94% исследованных систем содержали уязвимости, позволяющие получить полный контроль над критически важными ресурсами. В 67% систем получение контроля возможно из сети Интернет. Для 44% возможно получение полного контроля над всей информационной инфраструктурой.

Positive Technologies

Санкции по Украине; Россия вступила в конфликт на Ближнем Востоке; конфликт с Турцией; блэкаут на Украине из-за кибератаки (СБУ обвинила Россию в причастности к инциденту).
Стоит ожидать ответных хакерских атак.

Зачем ИБ в АСУ ТП / Предпосылки

Резкое увеличение количества инцидентов ИБ в области АСУ ТП в мире

- Апрель 2000. Перехват из Интернета управления сетью крупнейшего в мире газопровода ОАО «ГАЗПРОМ»[1]
- Март 2008. Внештатное аварийное выключение блока 2 ядерной станции "Hatch" (США) - обновление ПО.
- Апрель 2009. Зафиксировано проникновение в электроэнергетическую сеть США и размещения в ней программных «закладок», направленных на внештатную остановку её функциональных элементов и нарушение корректной работы.
- Апрель 2010 г. Специалистами энергетической компании LCRA, обслуживающей более 1 миллиона людей в штате Техас, зафиксировано свыше 4800 попыток получения доступа к их компьютерной системе.
- Июль 2010 г. Вирусом Stuxnet заражены 43 операторских станции одной крупной госкомпания США. Через месяц была полностью потеряна информация всей ИС.
- Ноябрь 2011 г. Взломана SCADA-система одной из американских ГЭС. Из строя выведен насос, который использовался для водоснабжения.
- С 2010 года в 20 раз выросло число обнаруженных уязвимостей[2].

1 – брифинг МВД РФ , и.о. начальника управления "Р" МВД полковник Константин Мачабели

2 - Безопасность промышленных систем в цифрах. Positive Techologies 2012

Зачем ИБ в АСУ ТП / Предпосылки

Появление в свободном доступе инструментов эксплуатации уязвимостей

- PLCScan, WinCC Harvester, S7 password offline bruteforce tool, etc. 15 минут – время потраченное на поиск в Интернете уязвимой системы АСУ ТП и получения к ней доступа[1].
- 50% уязвимостей позволяют хакеру запустить выполнение кода. Для 35% уязвимостей есть эксплойты[2].

ФЗ РФ N 256 "О безопасности объектов ТЭК"

- Статья 11. Обеспечение безопасности информационных систем объектов ТЭК

  В целях обеспечения безопасности объектов ТЭК, субъекты ТЭК создают на этих объектах **системы защиты информации и информационно-телекоммуникационных сетей от неправомерных доступа, уничтожения, модифицирования, блокирования информации и иных неправомерных действий** и обеспечивают функционирование таких систем.

Приказ № 31 ФСТЭК РФ

- «Об утверждении требований к обеспечению защиты информации в АСУ ТП …»

1 – Роман Попов, семинар РТ по безопасности АСУ ТП.

2 – Безопасность промышленных систем в цифрах. Positive Techologies 2012

Зачем ИБ в АСУ ТП / А реально?

или

1. Инвентаризация
2. Оценка рисков

Понимание ситуации!

Цели аудита ИБ АСУ ТП

1. **Получение независимой экспертной оценки уровня текущей защищенности АСУ ТП**
2. **Оценка соответствия требованиям законодательства РФ**
3. **Оценка соответствия внутренним требованиям**
4. **Получение экспертных рекомендаций по устранению обнаруженных недостатков**
5. Документирование текущего состояние (разработка паспортов объектов защиты)
6. Разработка модели угроз

Основные этапы аудита ИБ АСУ ТП

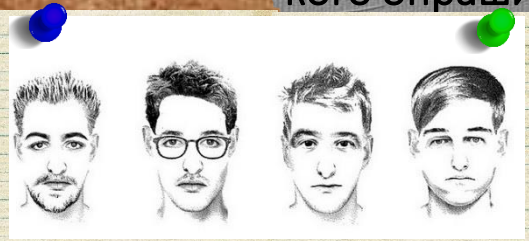
1. Обследование
2. Инструментальный аудит
3. Оценка соответствия требованиям
4. Классификация АСУ ТП
5. Анализ угроз ИБ АСУ ТП
6. Разработка рекомендаций

Обследование

задачи

Интервьюирование

кого опрашивать?



Инженеры АСУ ТП

Специалисты ИБ, ИТ, СБ, ГОиЧС

Разработчик

Анализ документации

Проект

ЭД

- Технологический регламент
- Инструкции персонала
- Внутренние документы

Инструментальное обследование

Программа обследования

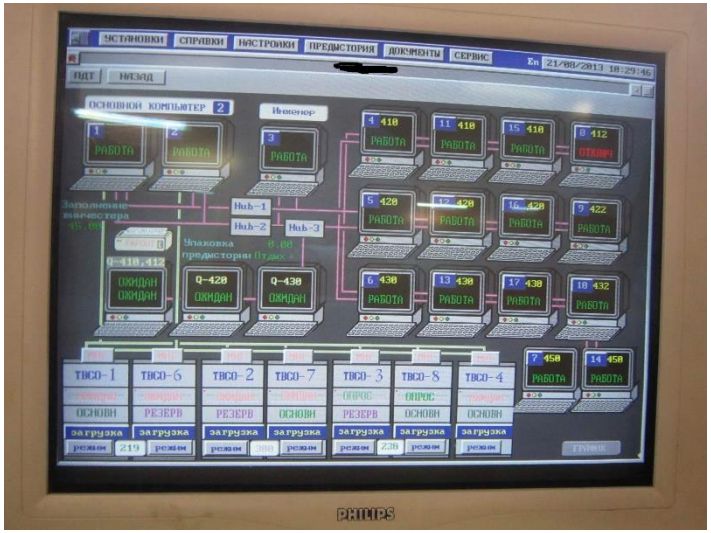
нельзя использовать стороннее ПО

- Встроенные средства системного и прикладного ПО
- Фотографирование

Что взять с собой аудитору?

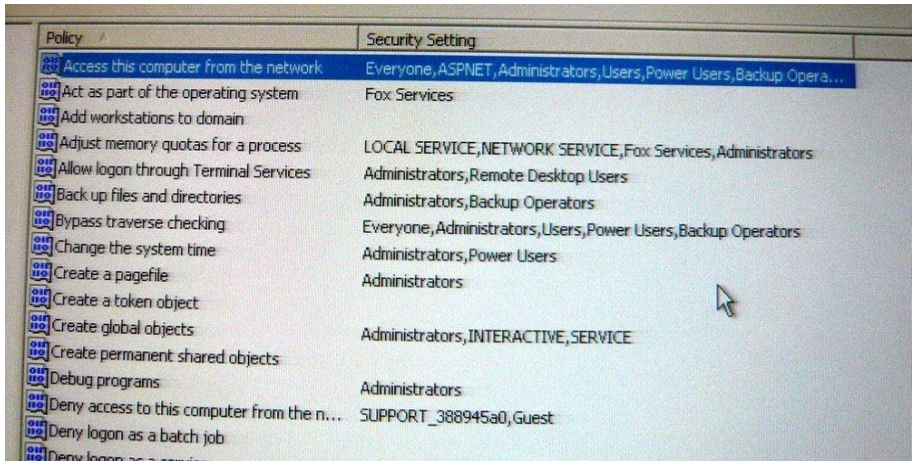
Возможные ограничения

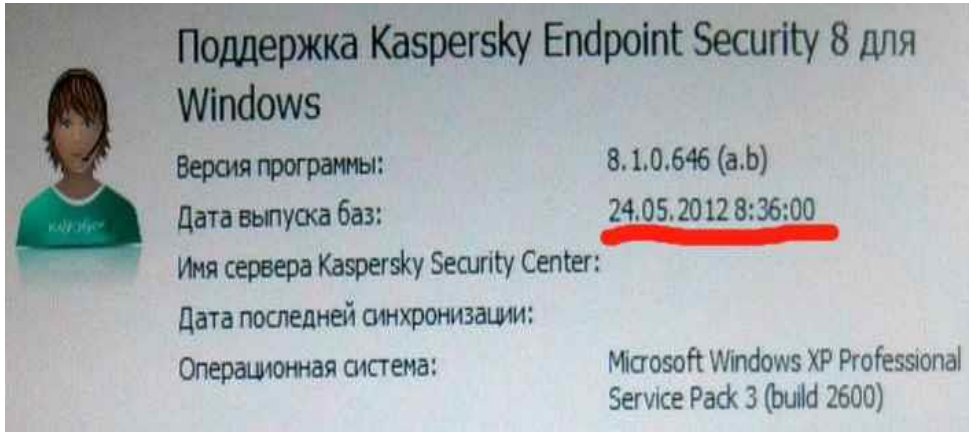
- Нет исходных данных
- Проекты только на бумаге и устарели
- Нужно искать оборудование АСУ ТП



Возможные ограничения (2)

- Доверяй, но проверяй





Первые результаты

Industrial != Commercial

- Исполнительность на местах
- Никакой самодеятельности
- Жесткие вертикали
- Высокое доверие к вендору
- Оперативные изменения невозможны!

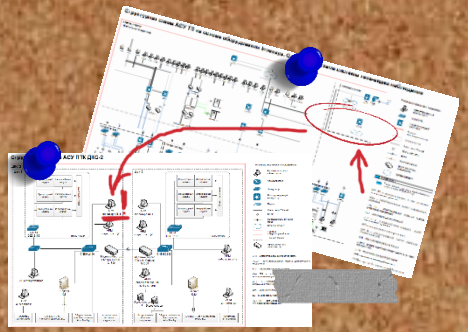
Инструментальный аудит нужен!

- Проверка данных обследования
- Без него никто не поверит
- Без него ты сам не разберешься
- Дает переход от перечня недостатков к плану действий по их устранению

Инструментальный аудит

задачи

1. **Разработка Программы и выбор инструментов**



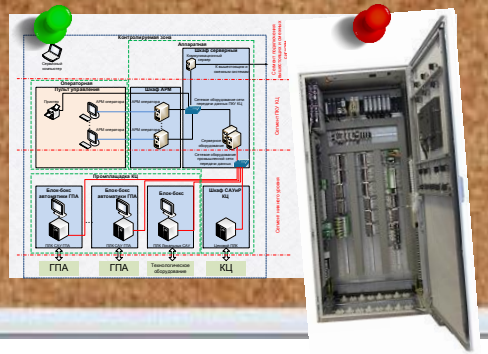
2. **Проникновение в защищаемый сегмент**

только **до границы** сегмента АСУ ТП

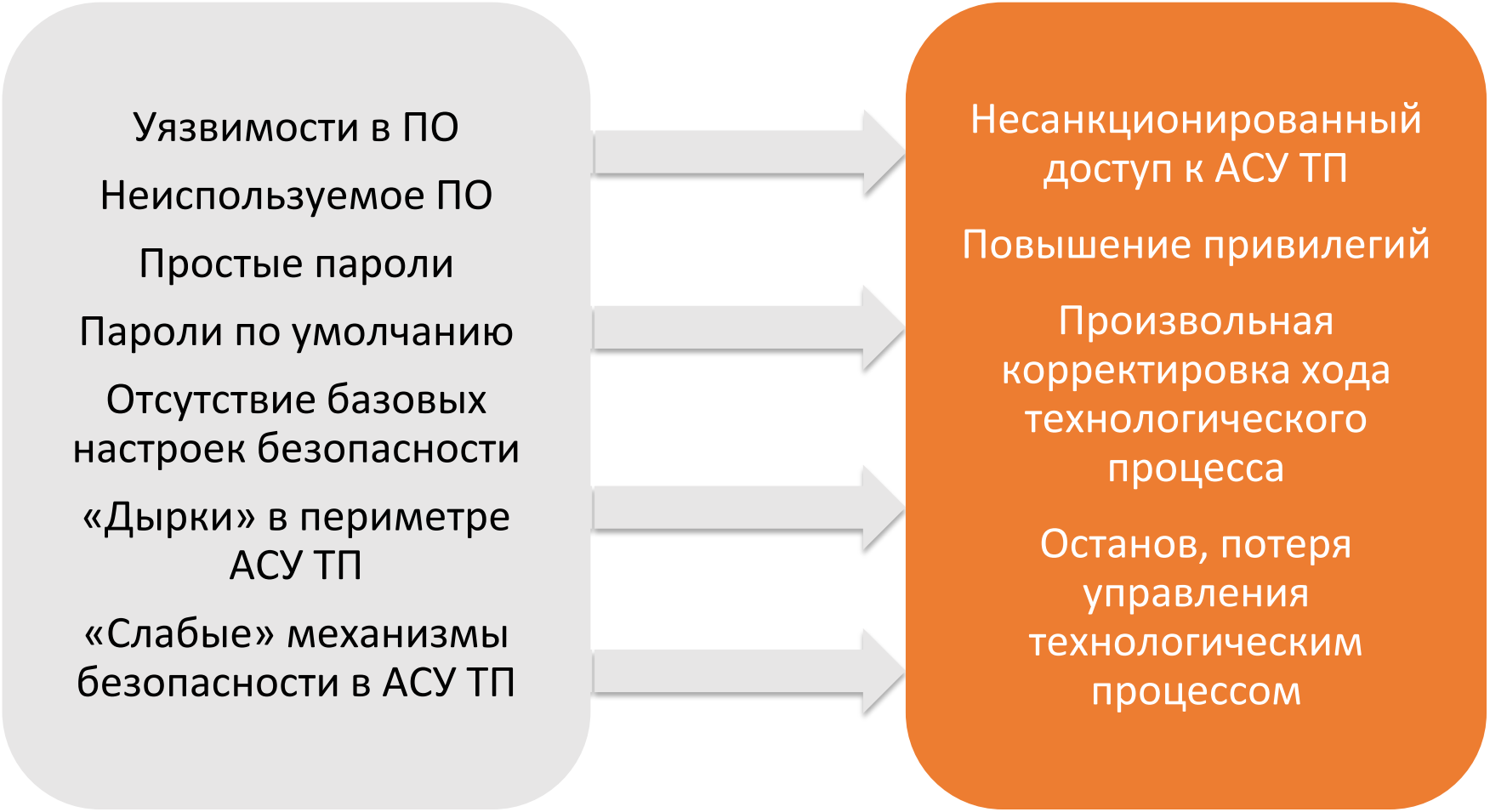
Разработчик

3. **Демонстрация атак**

- **на стенде**
- в ходе **ТО**

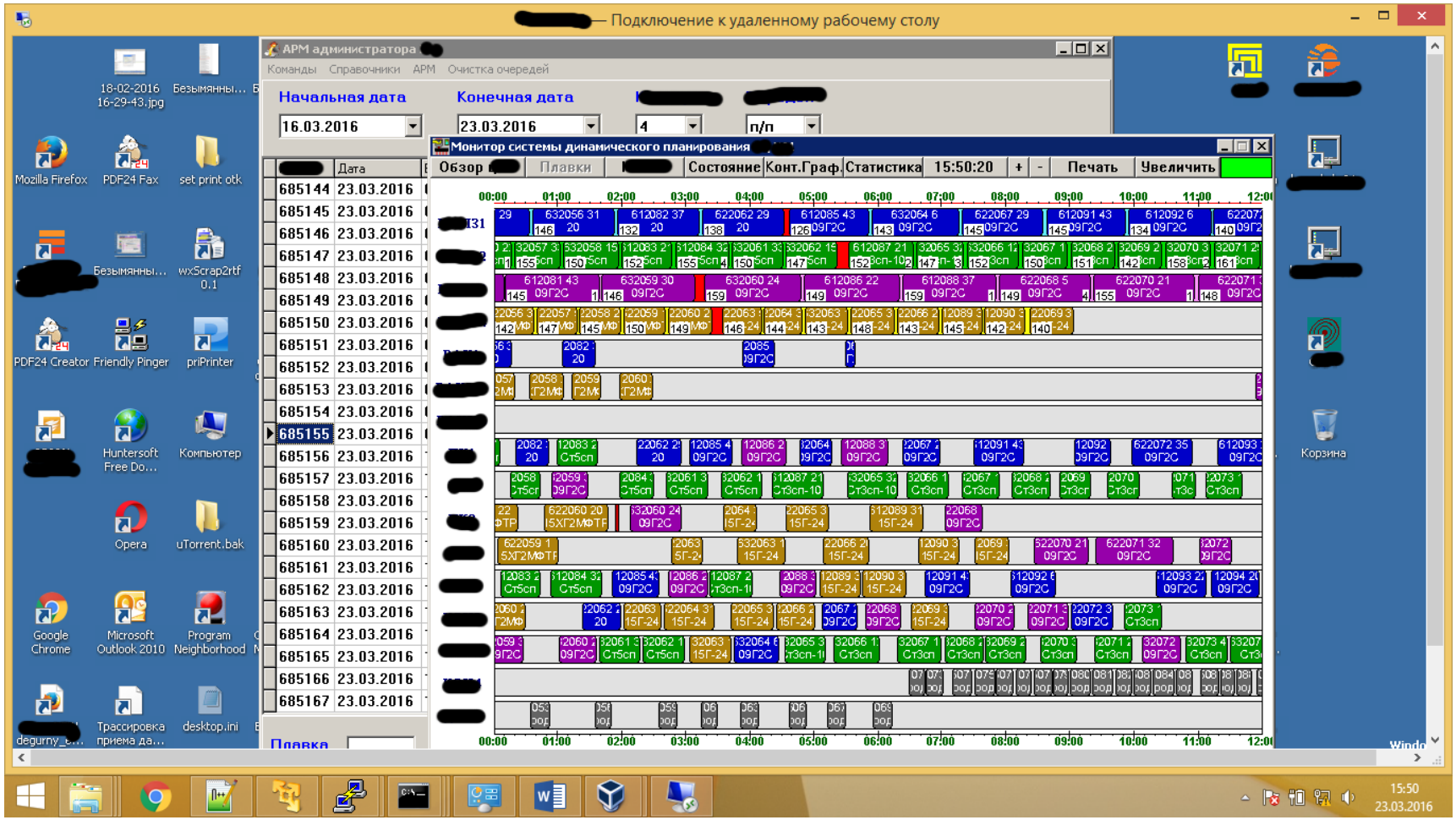


Типовые уязвимости



Доступ в АСУ ТП из корпоративной сети

Удаленный доступ в АСУ ТП с АРМ наладчика

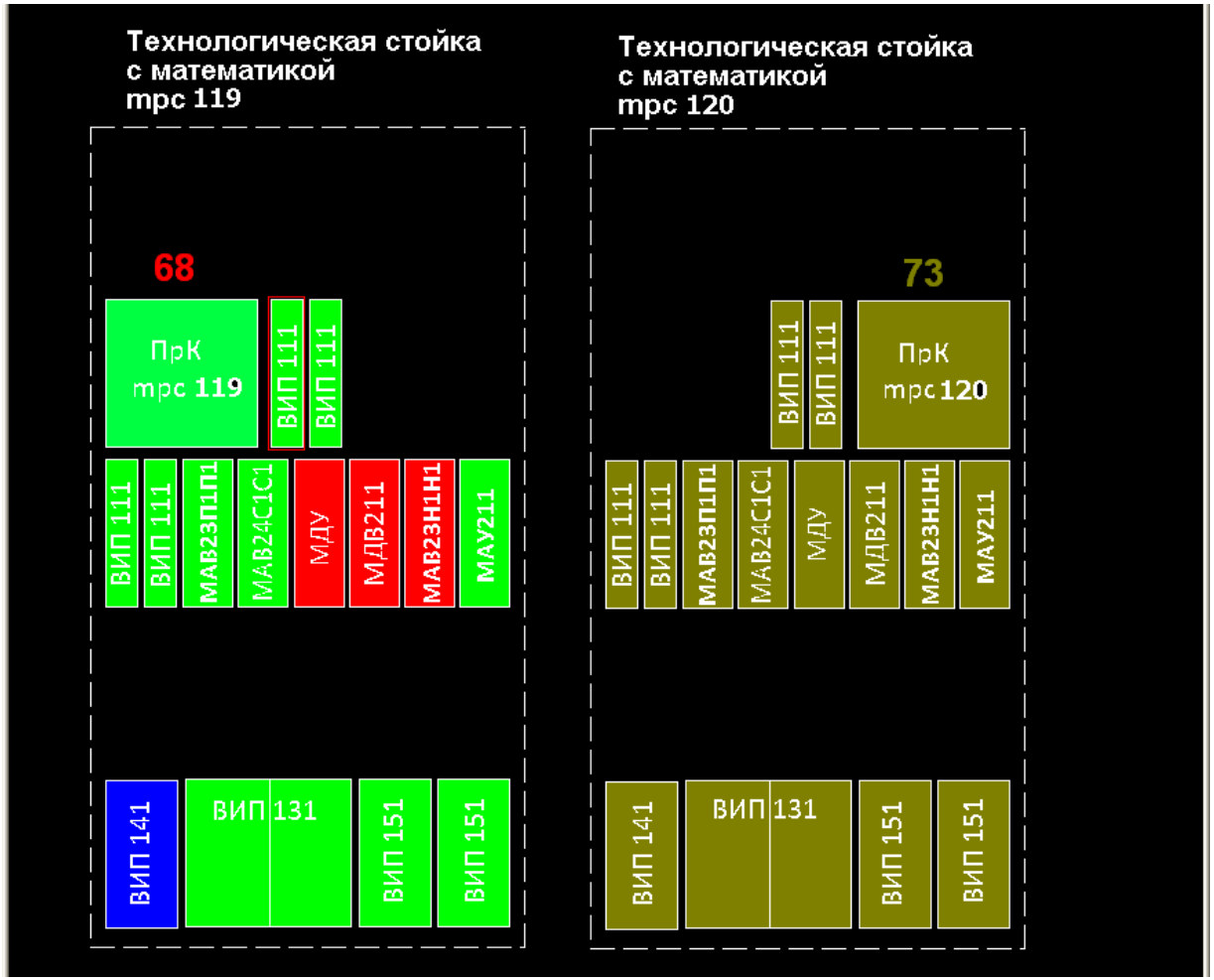


Отказ в обслуживании ПЛК

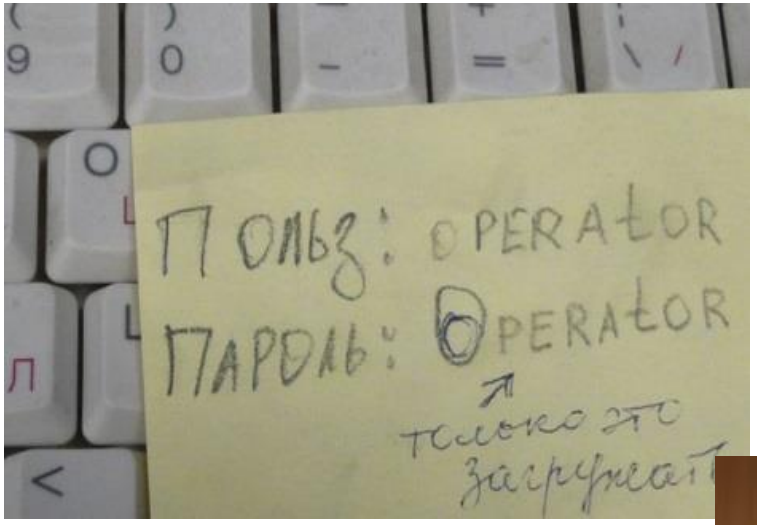
Зависание ПЛК вследствие некорректной обработки запросов на TCP-соединения

Отказ в обслуживании ПЛК

Уязвимость в реализации сетевого протокола FLEET (QNX) приводит к аварийной перезагрузке



Другие уязвимости



Оценка соответствия требованиям

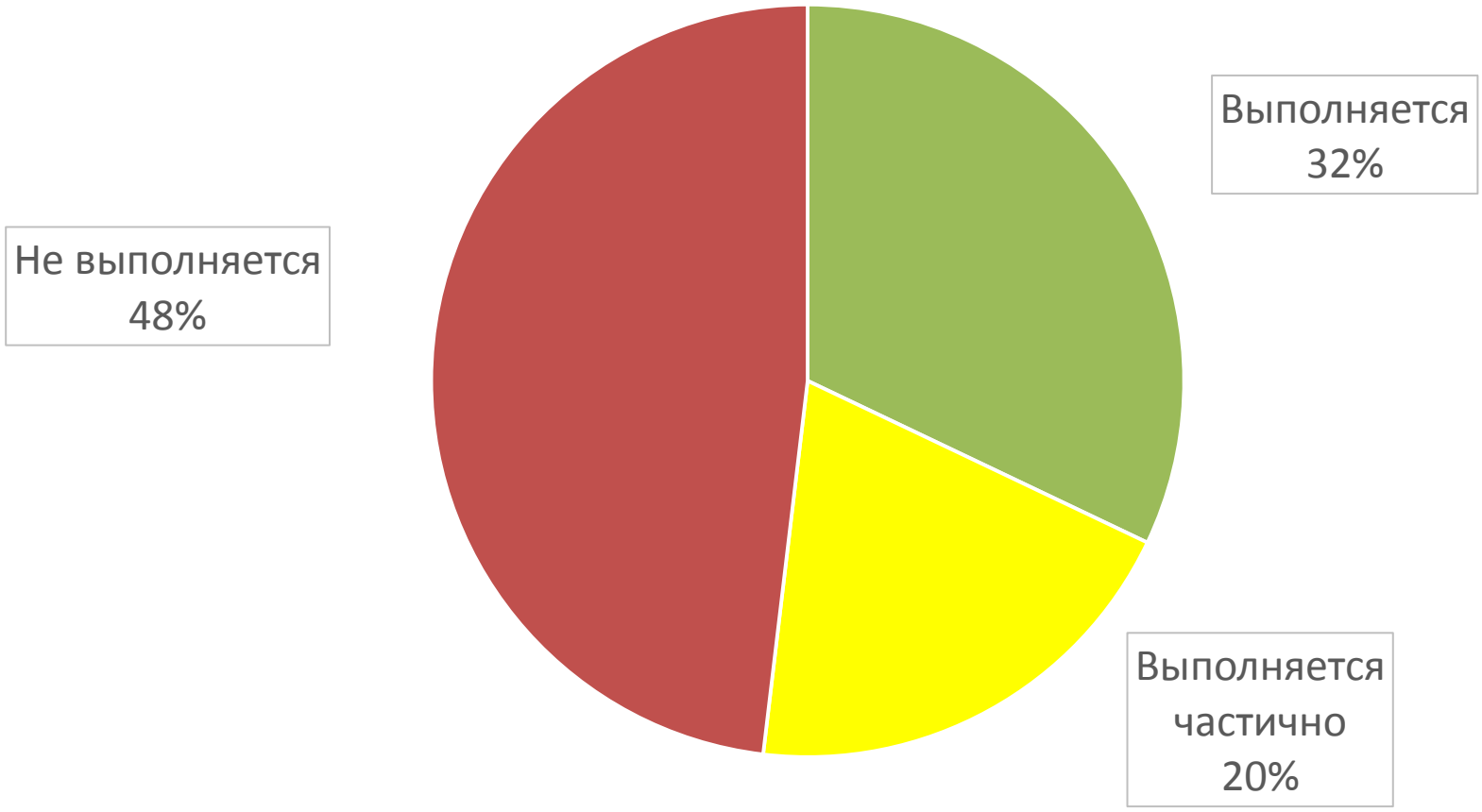
Обязательно:

- Приказ №31 ФСТЭК России
- Отраслевые требования
- Внутренние требования

Дополнительно:

- Международные документы
- Документы ФСТЭК России по КСИИ
- Рекомендации разработчиков АСУ ТП

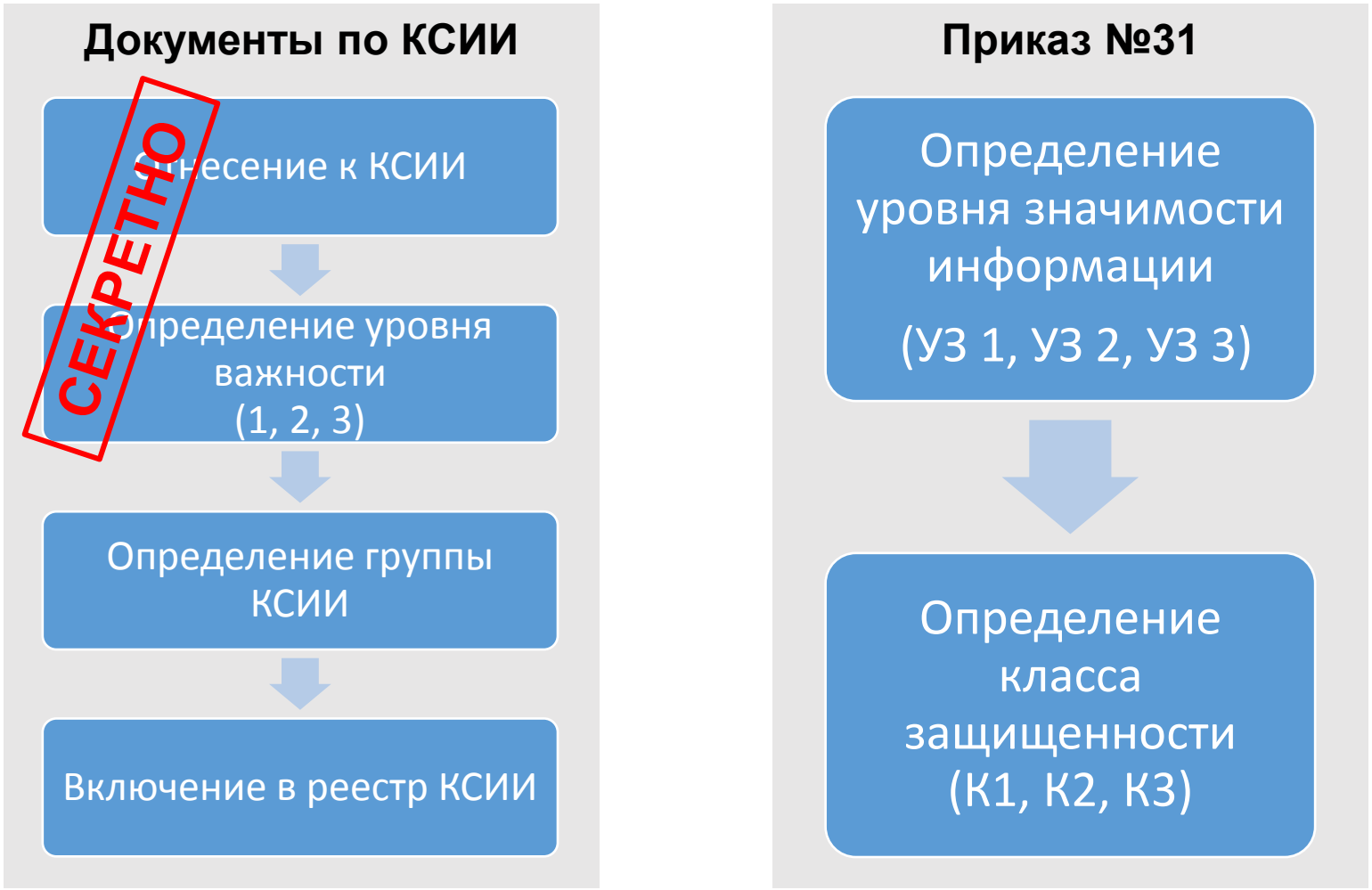
Соответствие требованиям Приказа ФСТЭК №31



Общая характеристика соответствия требованиям

Идентификация и Аутентификация	Техническое обслуживание и сопровождение	Анализ угроз ИБ
Управление и контроль доступа	Анализ защищенности	Оценка рисков ИБ АСУ ТП
Целостность системы и информации	Защита при взаимодействии систем	Планирование
Антивирусная защита	Защита при передаче по открытым каналам связи	Информирование по вопросам ИБ
Выявление и реагирование на инциденты ИБ	Физическая защита	Управление непрерывностью бизнеса
Управление конфигурациями	Безопасность, связанная с персоналом	Защита информации на этапах жизненного цикла

Классификация АСУ ТП



Уровень значимости (УЗ) информации

Соответствует степени возможного ущерба:

- Возникновение ЧС (см. Постановление Правительства РФ № 304 «О классификации чрезвычайных ситуаций природного и техногенного характера»)

Декларация пром. безопасн.

План действий по предупр. и ликв. ЧС

- Иные негативные последствия в различных областях

Анализ угроз ИБ АСУ ТП

Документы по КСИИ

1. Процесс прописан в:
- Базовой модели угроз
- Методике определения актуальных угроз

2. Угроза признается актуальной на основании оценки:
- Коэффициента опасности
- Вероятности реализации

Приказ №31

1. Документы, описывающие процесс не разработаны

2. Проект методики определения угроз ожидается в 2016г

3. В настоящее время применяются документы по КСИИ

Методика определения актуальных угроз для КСИИ

- Универсальная
- Подробная
- Хорошо автоматизируется в Excel

- ДСП
- Универсальная
- Есть не проработанные места

<u>Вопросы для определения нарушителя:</u>

- Берут ли сотрудники работу на дом?
- Используется ли на объекте внешняя АТС?

<u>Определение вероятности угроз:</u>

Разработка моделей оценки вероятности длительный процесс => Вероятность угрозы НСД 1, если нет защитных мер
Вероятность угрозы 0, если угрозы нет

Угрозы ИБ АСУ ТП

BSI, Industrial Control System – Top 10 Threats	ФСТЭК России (более 100 угроз для КСИИ)
Несанкционированное использование технологий удаленного доступа	• Несанкционированное получение доступа к средствам удаленного администрирования • Несанкционированный удаленный доступ к контроллерам
Атаки через офисную (корпоративную) сеть	• …
Атаки на традиционные IT-компоненты	• …
(D)DoS атаки	• …
Человеческие ошибки и злонамеренные действия персонала	• …
Распространение вредоносного ПО с помощью съемных носителей и устройств, подкл. к сети	• …
Перехват, искажение и передача информации	• …
Неавторизованный доступ к компонентам	• …
Атаки на сеть передачи данных АСУ ТП	• …
Отказы оборудования, форс-мажор	• …

Разработка рекомендаций

Оперативные мероприятия

- Настройка компонентов АСУ ТП (установка паролей, отключение неиспользуемых служб и портов и т.п.)
- Регламентация фактически выполняемых мероприятий по обеспечению ИБ и закрепление ответственности

Тактические мероприятия

- Реализация периметральной защиты сети передачи данных АСУ ТП
- Устранение уязвимостей в рамках сервисного сопровождения (установка обновлений безопасности, настройка встроенных механизмов защиты)
- Контроль защищенности АСУ ТП (выявление уязвимостей, контроль выполнения мероприятий по обеспечению ИБ)

Стратегические мероприятия

- Адаптация СУИБ к АСУ ТП (формирование Стратегии обеспечения ИБ АСУ ТП, выстраивание процессов)
- Обеспечение ИБ АСУ ТП на всех этапах жизненного цикла (реализация Системы защиты информации в АСУ ТП)

Выбор средств защиты АСУ ТП

Специализированные решения

- Иностранные

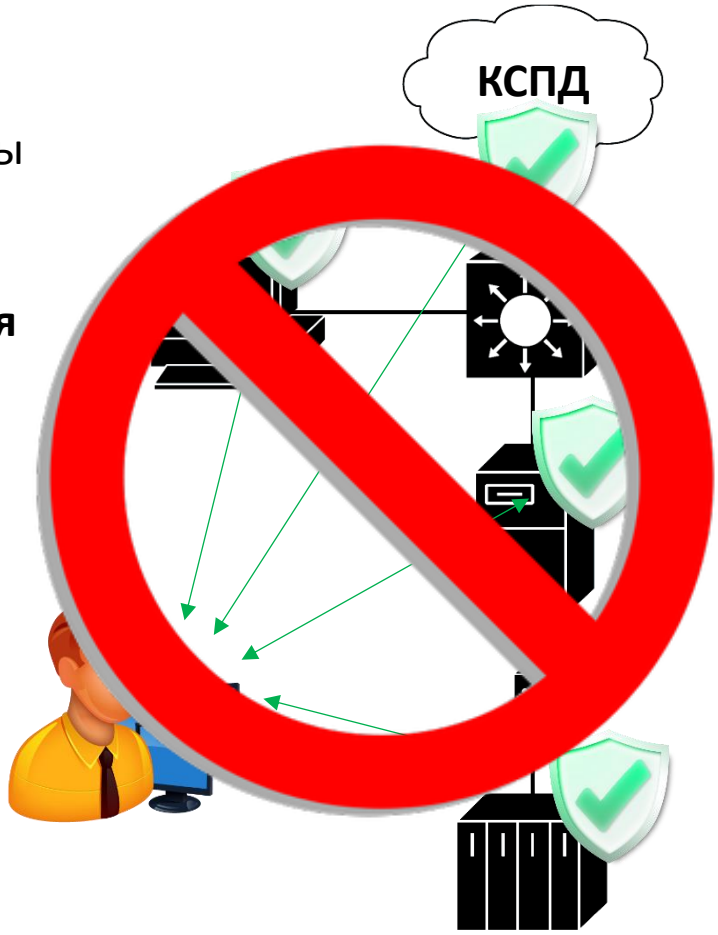
- Отечественные

Решения от разработчиков АСУ ТП

Особенности применения технических мер защиты

Технические меры защиты информации реализуются посредством применения средств защиты информации, имеющих необходимые функции безопасности. В качестве средств защиты информации **в первую очередь подлежат рассмотрению механизмы защиты (параметры настройки) штатного программного обеспечения** автоматизированной системы управления при их наличии

Приказ ФСТЭК России от 14.03.2014 №31



Результаты аудита

1. **Паспорта объектов защиты**
2. **Оценка соответствия требованиям**
3. **Независимая оценки уровня текущей защищенности**
4. **Получение рекомендаций по устранению обнаруженных недостатков**

Так как же дела в АСУ ТП?

Есть уязвимости? ☑

Есть инциденты? ☑

Реальная угроза/ущерб? ☒

Можно пока расслабиться? ☒

Дальнейшие шаги

- [x] Аудит ИБ АСУ ТП
- [ ] Реализация оперативных мероприятий
- [ ] Реализация мер обеспечения ИБ в ходе сопровождения
- [ ] Проектирование и макетирование СЗИ
- [ ] Поэтапное создание СЗИ
- [ ] Набор и обучение персонала
- [ ] Выстраивание процессов

Благодарим за внимание!

Вопросы?

Роман Попов

Popov_R@eon-russia.ru

Антон Ёркин

ayorkin@ussc.ru

e·on

УЦСБ

Интегратор Сильных Решений