УЦСБ ИНТЕГРАТОР СИЛЬНЫХ РЕШЕНИЙ

Построение системы мониторинга ИБ АСУ ТП

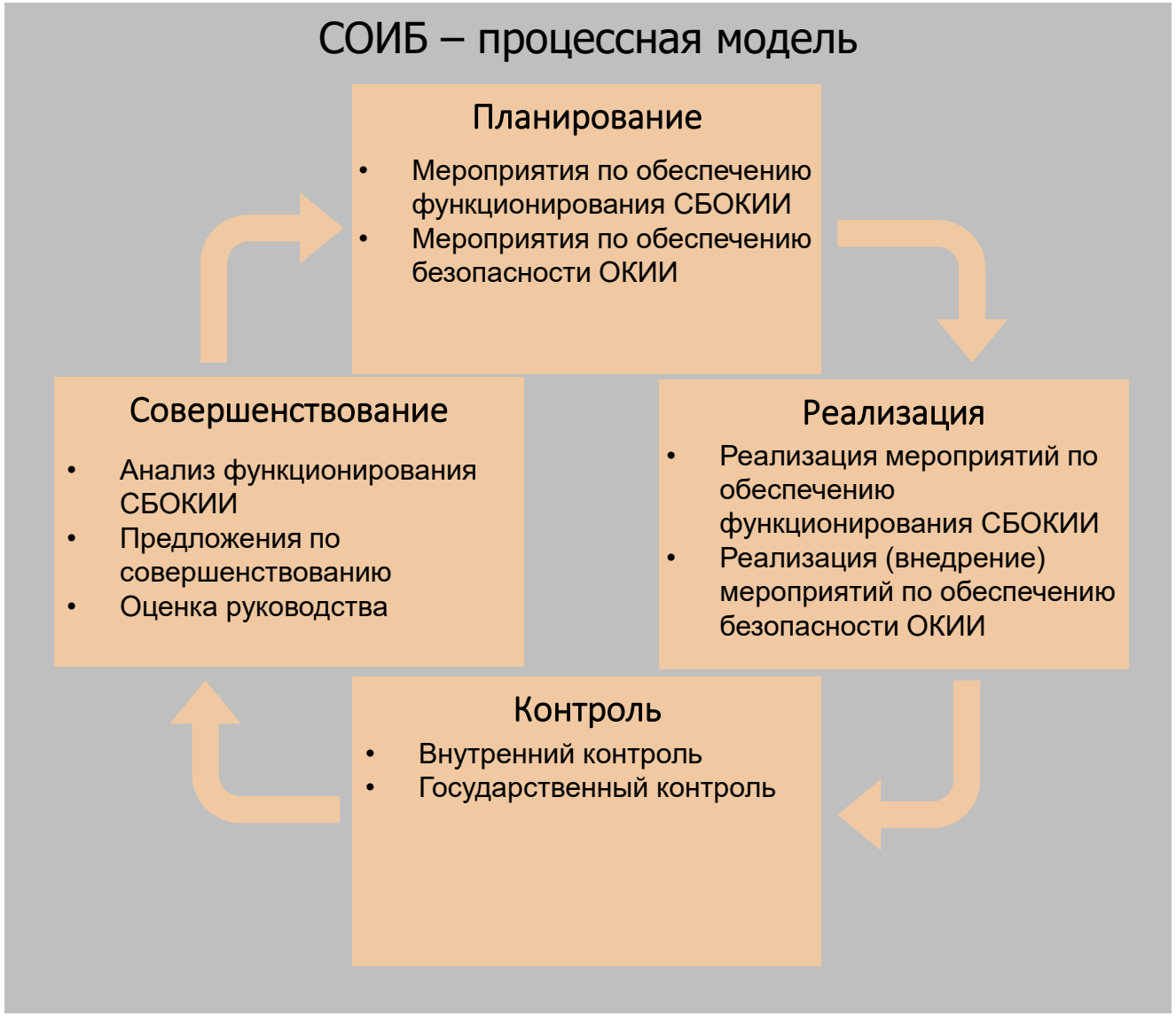
Николай Домуховский
Заместитель генерального директора

Что такое мониторинг ИБ?

Совсем в общем случае:

Мониторинг – процесс сбора информации с целью наблюдений, оценки и прогноза изменений *состояния* объекта

Безопасность – *состояние* защищенности …



Что такое мониторинг ИБ?

Совсем в общем случае:

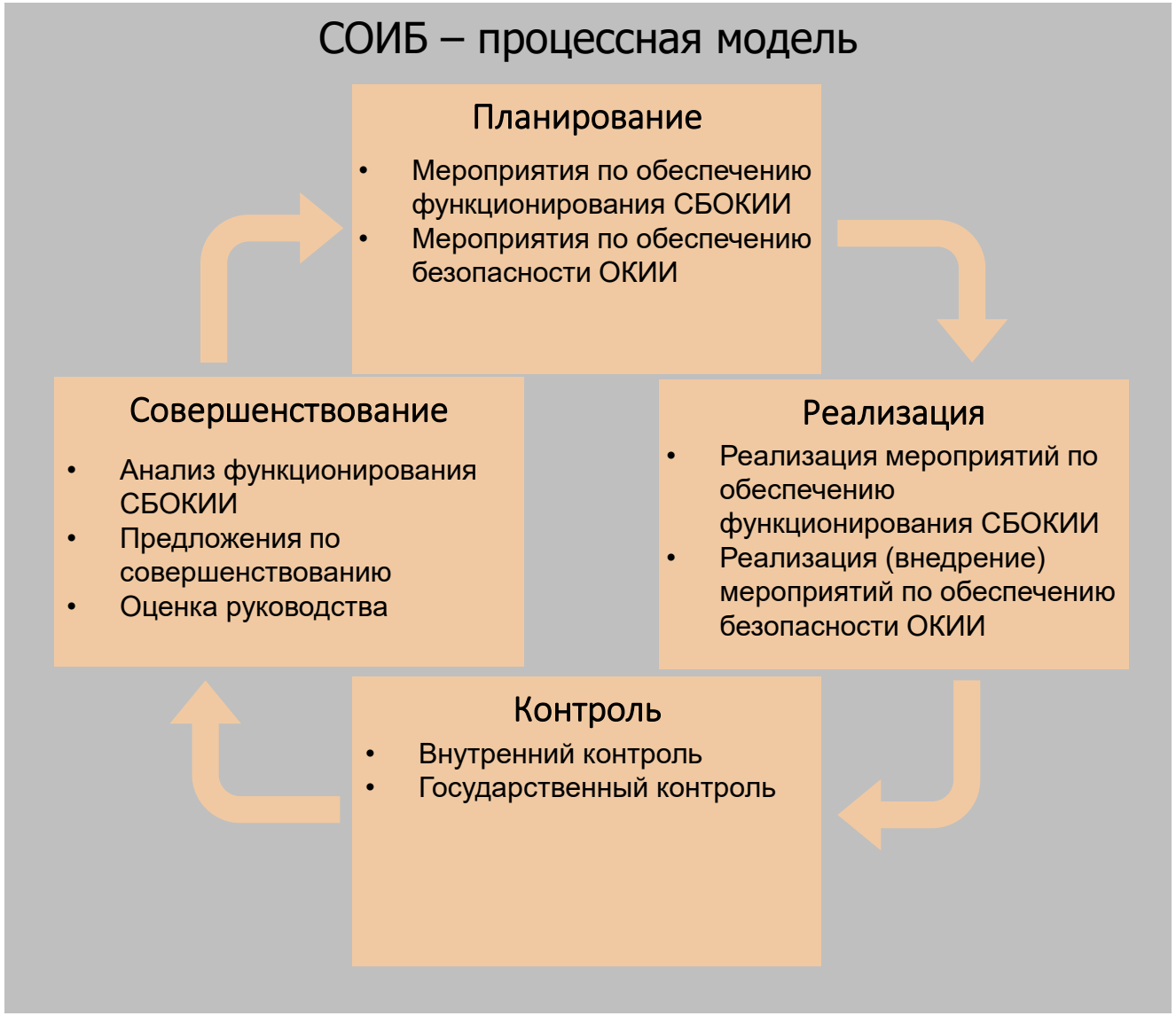
Мониторинг – процесс сбора информации с целью наблюдений, оценки и прогноза изменений *состояния* объекта

Безопасность – *состояние* защищенности …

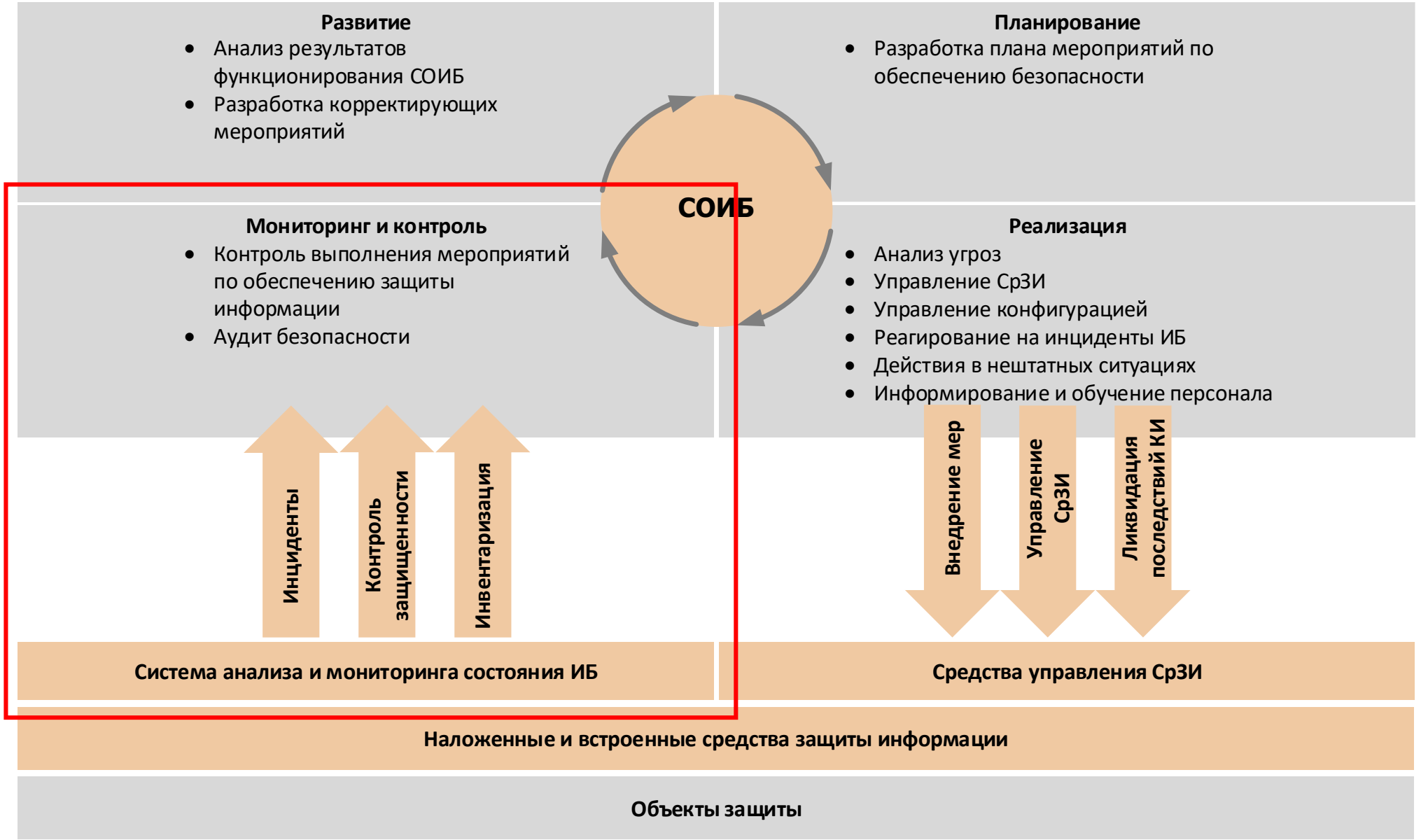
Более специфичный вариант:

мониторинг информационной безопасности: *Процесс* постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления нарушений безопасности информации, угроз безопасности информации и уязвимостей

Проект ГОСТ Р «Защита информации. Мониторинг ИБ. Общие положения»

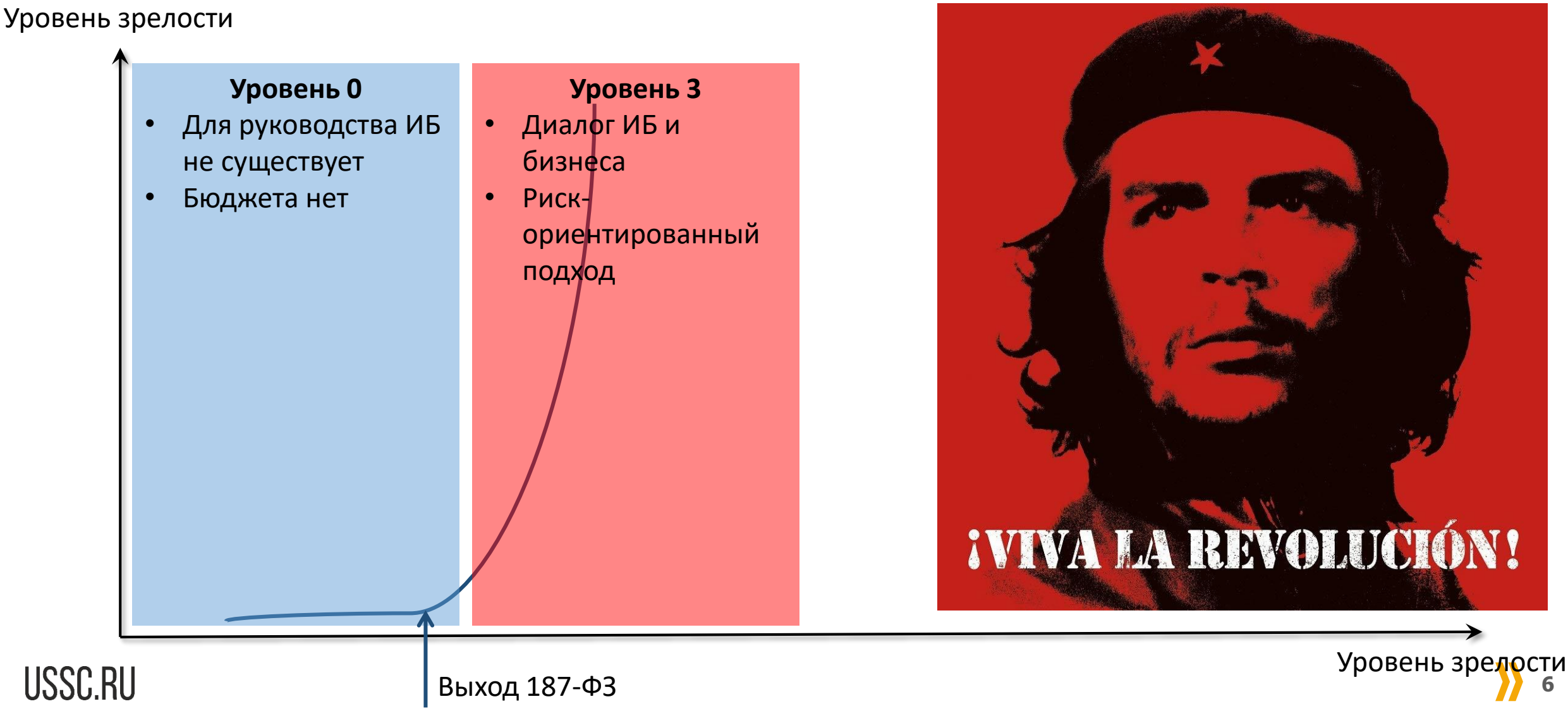


Связь между процессами обеспечения ИБ и программно-техническими средствами

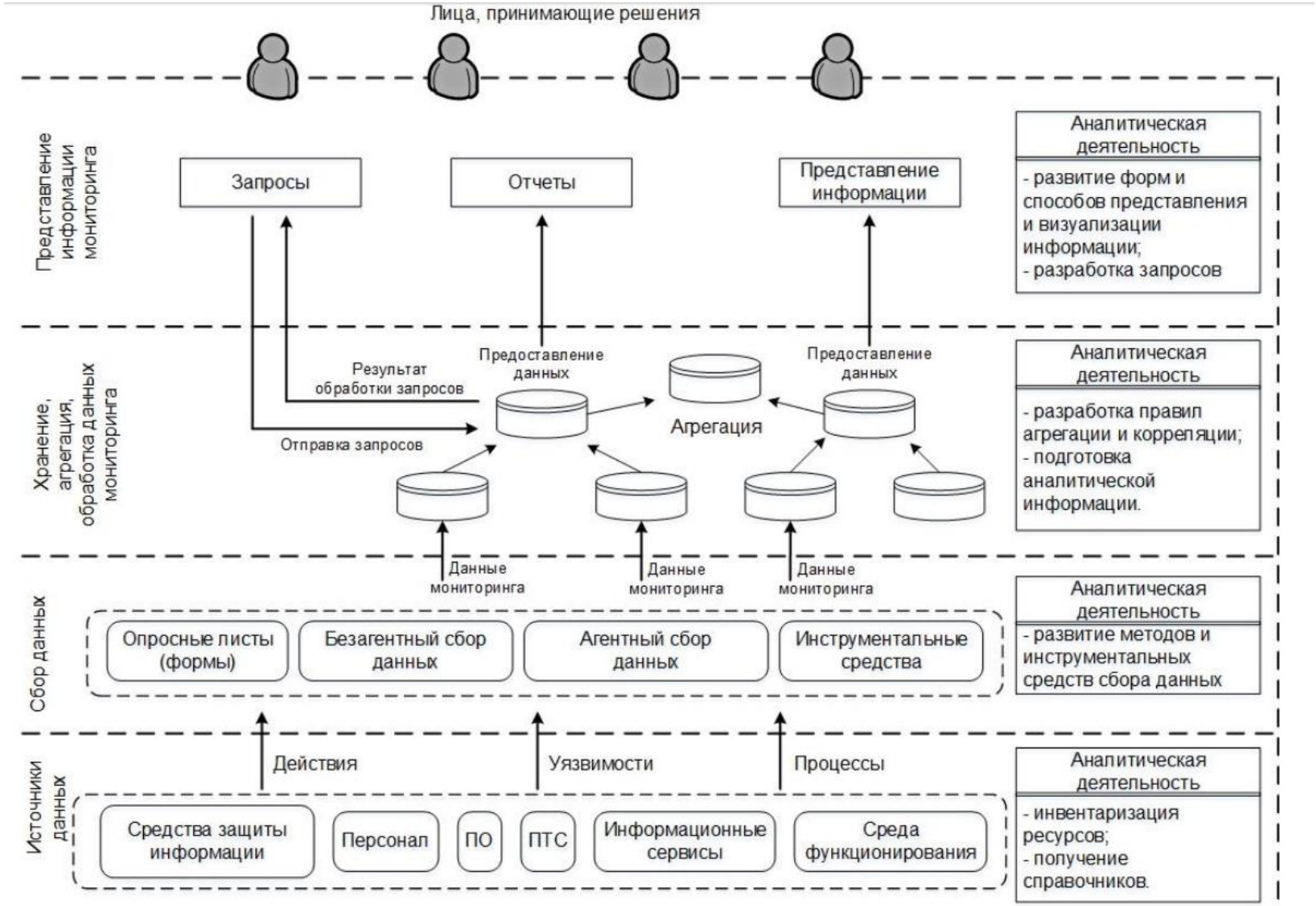


Традиционная модель зрелости процессов обеспечения ИБ

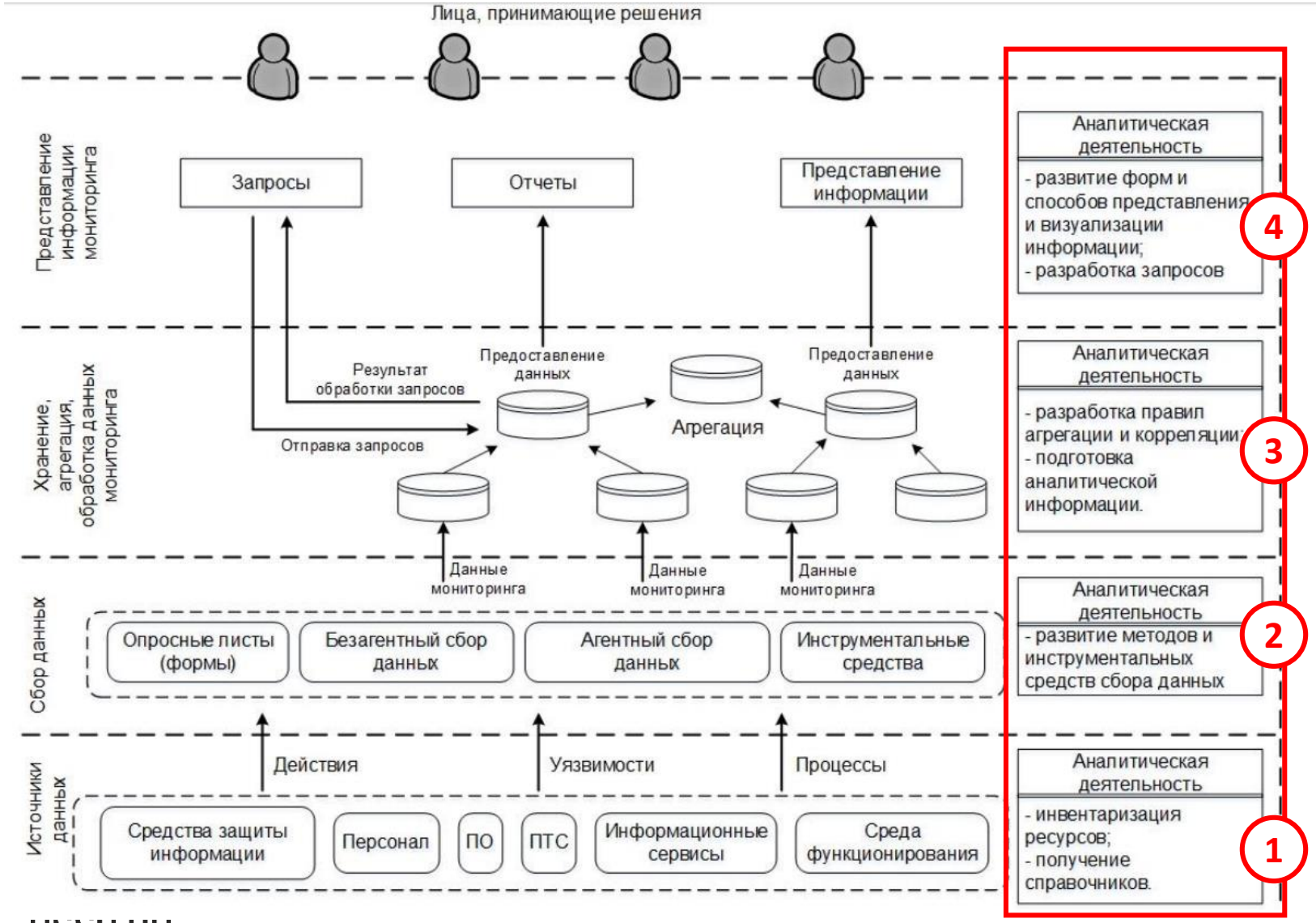
Влияние 187-ФЗ



Референсная модель системы мониторинга ИБ



Референсная модель системы мониторинга ИБ



Готовый план создания системы мониторинга

Этап 1. Инвентаризация и получение справочников

Интервьюирование
- Опрос *эксплуатационного персонала* технологического объекта
- Опрос подразделений, осуществляющих сопровождение ПТС АСУ ПТК
- Опрос сотрудников Отдела ИБ СКЗ

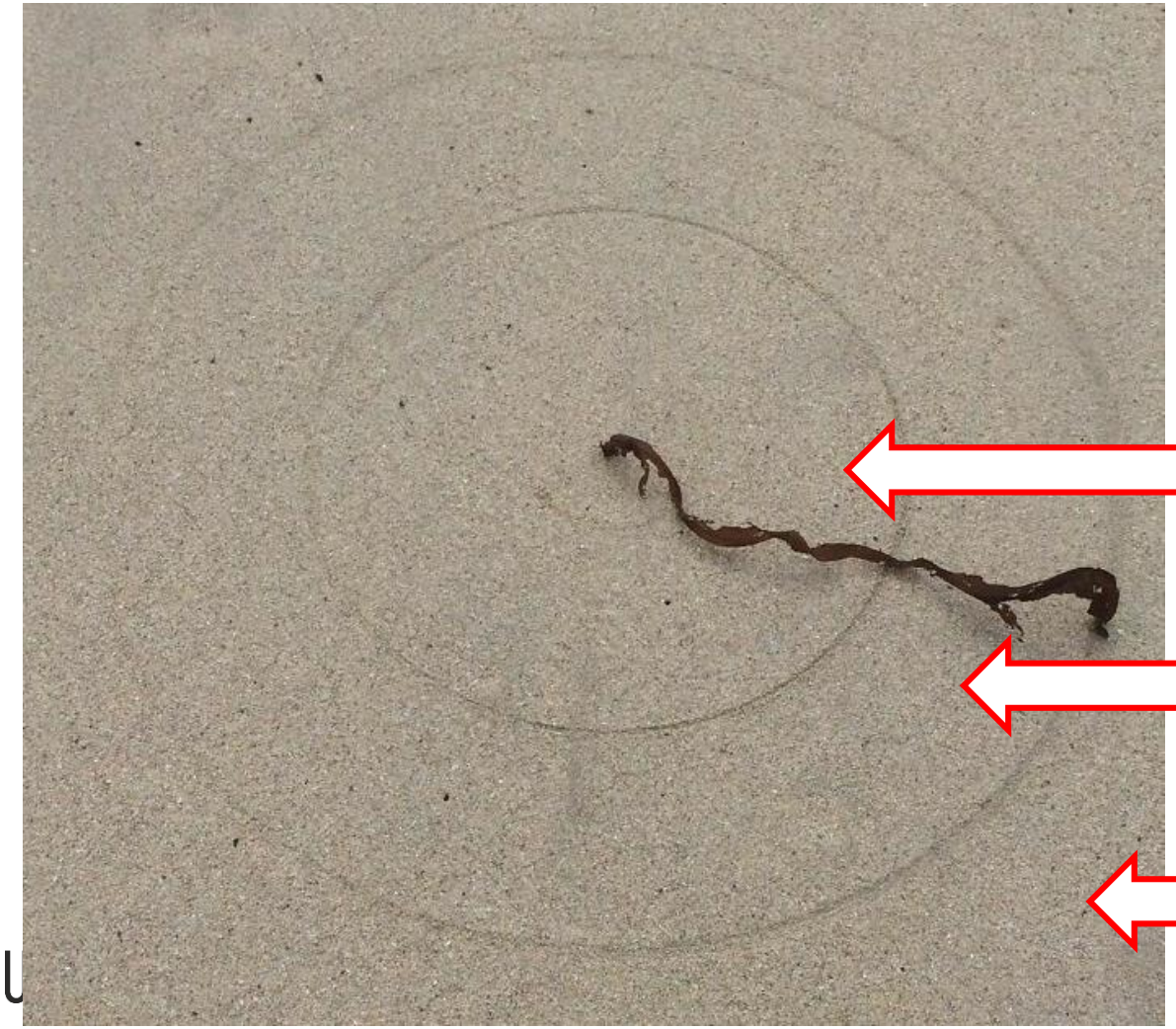
Анализ документации
- Анализ проектной и эксплуатационной документации на АСУ ПТК
- Анализ документации, описывающей *процессы эксплуатации технологического объекта*

Визуальный осмотр и фотографирование
- Осмотр технических средств АСУ ПТК и мест их размещения
- Фотографирование технических средств, шкафов автоматики и пр.

Инструментальное обследование
- Сбор данных встроенными средствами ОС и специального ПО
- Сбор данных при помощи специализированных программных средств
- *Сбор данных самими средствами мониторинга – внедрение через пилот*

Но почему не все так просто?

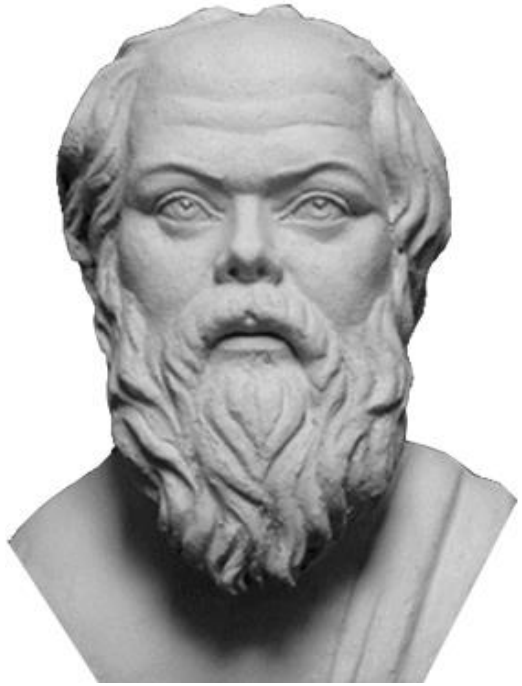
Наши знания об объекте мониторинга



То, что описано в документации

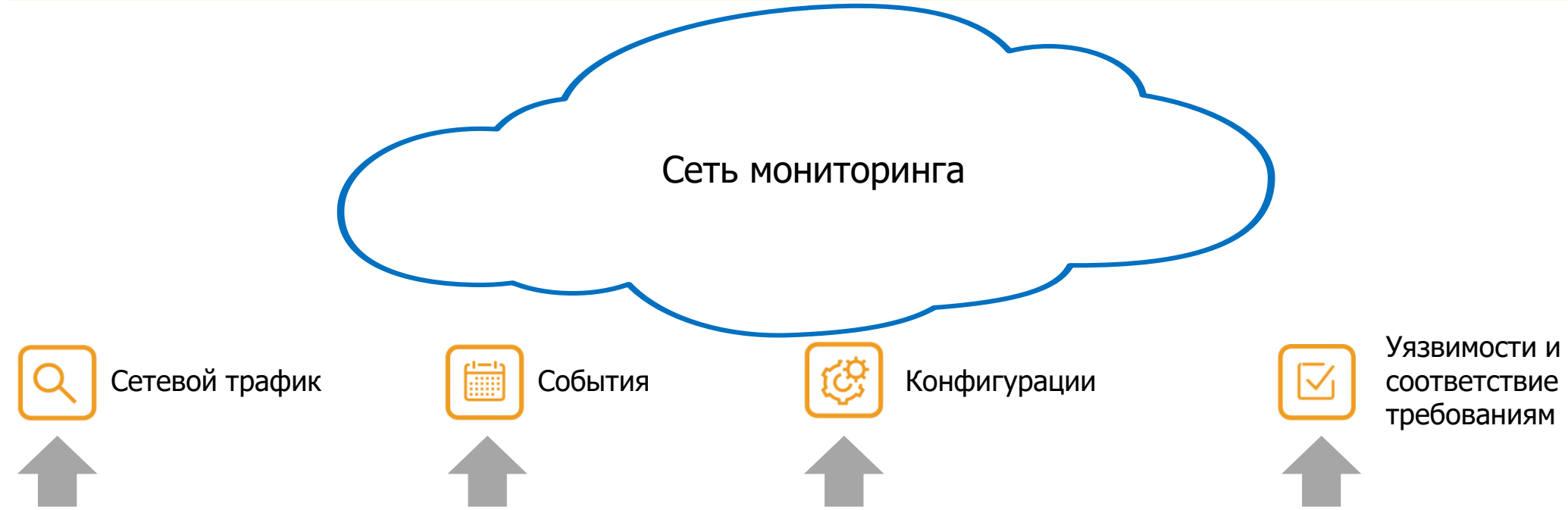
То, что удалось собрать в ходе обследования

То, что реально входит в состав системы



Этап 2. ~~Развитие~~ внедрение методов и инструментальных средств сбора данных

Инструментальное средство сбора данных мониторинга



Объект мониторинга ИБ

Этап 2. ~~Развитие~~ внедрение методов и инструментальных средств сбора данных

Инструментальное средство сбора данных мониторинга

Сетевой трафик

События

Конфигурации

Уязвимости и соответствие требованиям

Объект мониторинга ИБ

Построение сети мониторинга

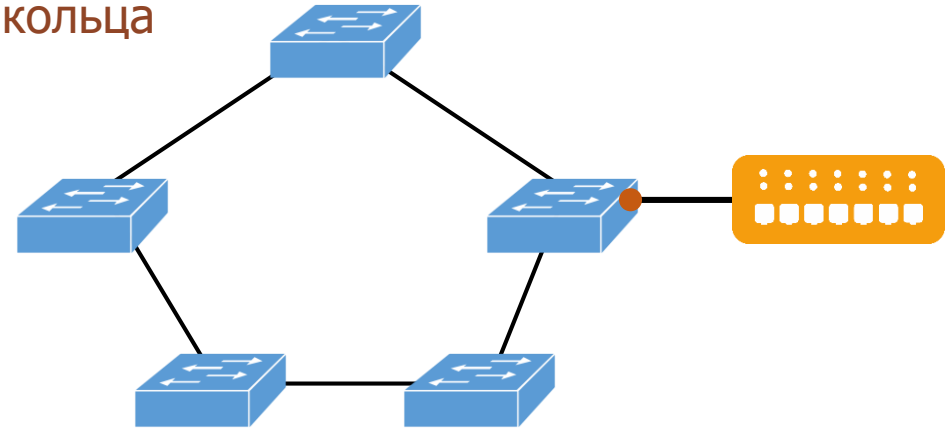
Вариант построения	Плюсы	Минусы
Модернизация сети АСУ ТП	• 100%-я видимость сети • Более управляемая и надежная сеть	• Дорого • Долго • Может потребоваться согласование проектировщиков АСУ ТП
Отдельная сеть мониторинга	• Нет дополнительной нагрузки на технологическую сеть • Быстрее и дешевле модернизации	• Могут потребоваться дополнительные физические каналы связи • Требуется портовая емкость на АСО АСУ ТП
Увеличение числа сенсоров	• Отсутствие влияния на сеть АСУ ТП • Можно задействовать существующее оборудование	• Требуется портовая емкость на АСО АСУ ТП • Дополнительные затраты на лицензии ПО мониторинга сети

Стоит отказаться от мечты анализировать 100% трафика технологической сети

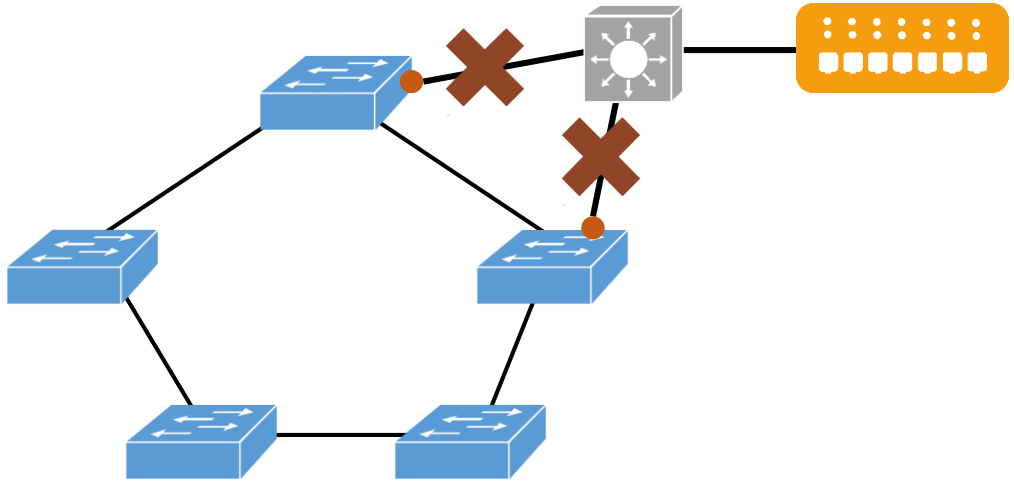
Сеть мониторинга. Tips & Tricks

USSC

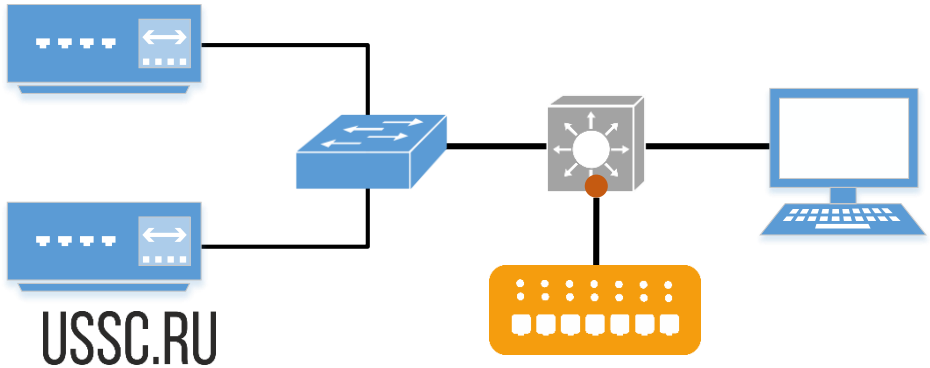
Трафик кольца может быть снят через любой коммутатор кольца



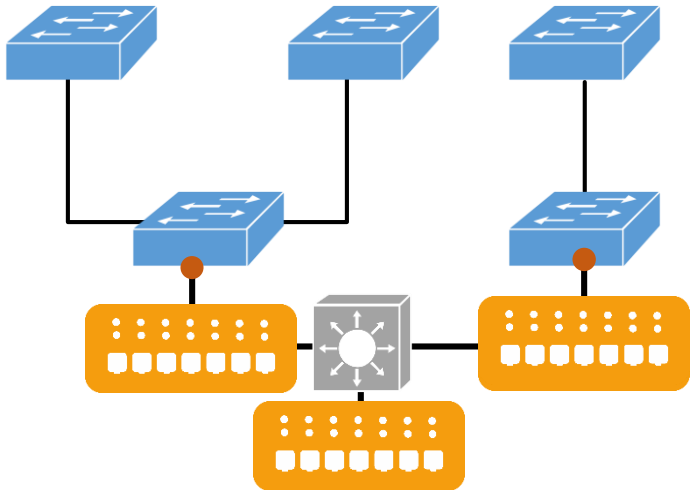
Не рассчитывать на STP!



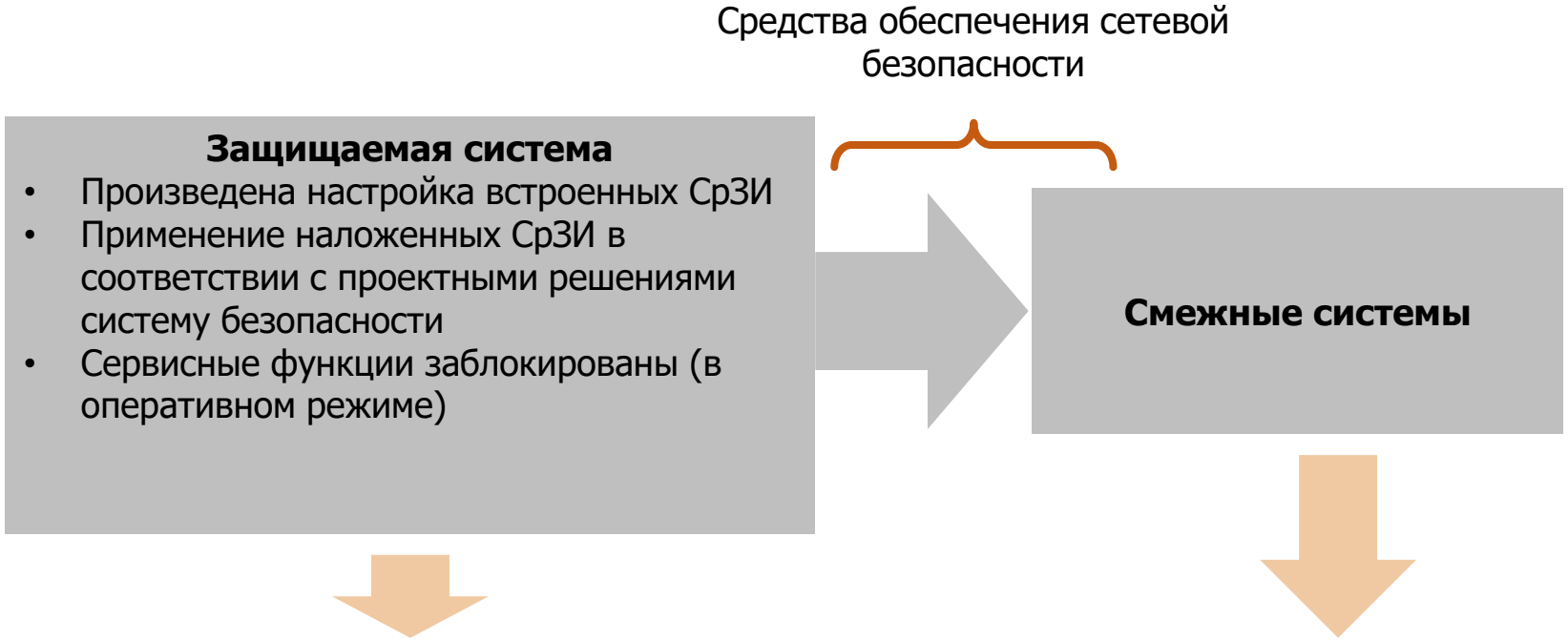
Если 100% трафика не получить – выбирать точку съема с основными информационными потоками



Строить независимую сеть мониторинга



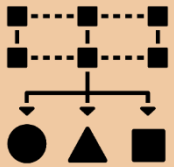
Этап 3. Агрегация, корреляция или что нам нужно видеть в системе мониторинга?



- Начальное состояние системы предполагается безопасным (например, проведена приемка СБОКИИ)
- Средства мониторинга ИБ отслеживают изменения в конфигурации (состав объектов, конфигурации оборудования и ПО, информационные потоки)
- Средства мониторинга ИБ анализируют события ИБ и визуализируют результаты корреляции
- Средства мониторинга ИБ осуществляют поиск известных уязвимостей и проводят оценку конфигураций на соответствие требованиям

Повышение информативности данных мониторинга

Приоритизация:
- учет критичности события, объекта, системы и пр.
- показывать только то, что требует понятной реакции оператора
- разделение данных по времени («свежие» и «несвежие» инциденты)



Классификация:
- по источникам (производство, АСУ ТП, объект АСУ ТП)
- по типам (инцидент, тревога, информационное сообщение)
- по временным отрезкам (оперативные, архивные)
- …

Обогащение:
- добавление данных инвентаризации от различных источников
- расшифровка служебных полей событий
- добавление структур данных для оперативной работы (карточка инцидента и пр.)

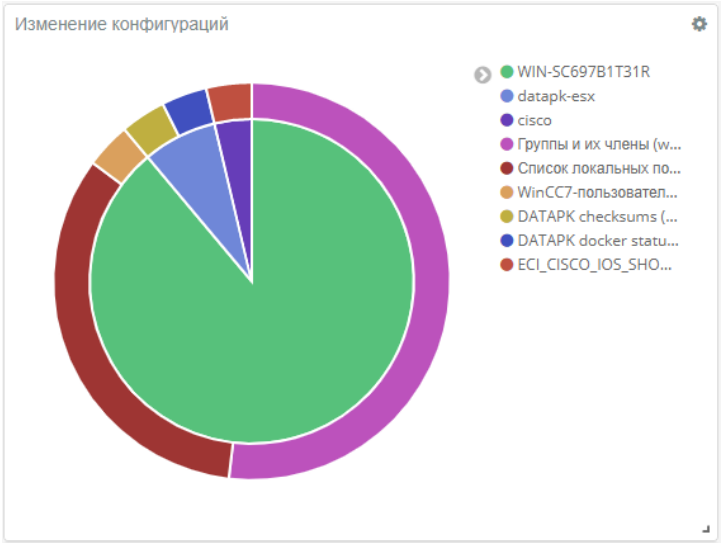
Этап 4. Представление данных – формы, отчеты и пр.

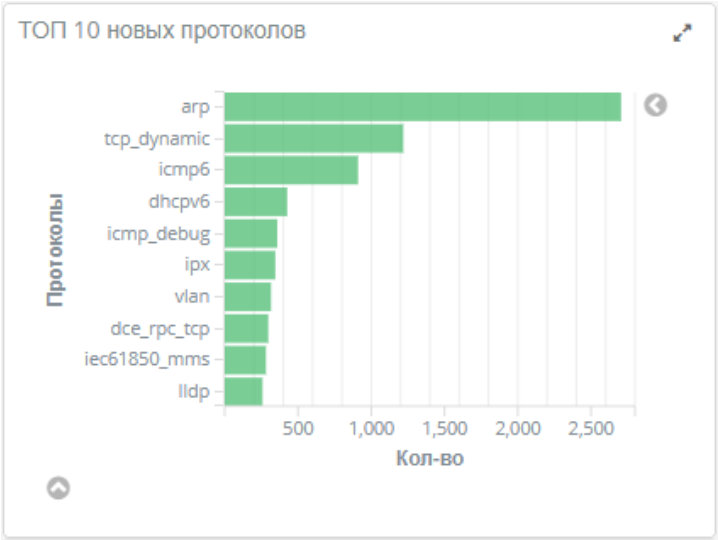
Эти прекрасные демонстрации интерфейсов средств обнаружения инцидентов в промышленных системах и способы их использования аналитиками… не нужны. Интерфейсы уйдут в прошлое. Аналитики не хотят смотреть в эти экраны.

Dale Peterson, «The Future Of ICS Security Products»

DATAPK

- Нет единственно правильного интерфейса представления данных
- Побеждает способность кастомизации и возможность интеграции (экспорт данных мониторинга или передача в смежные системы)
- Важны правильные процессы обработки данных мониторинга





А что дальше?

ГосСОПКА

Сведения о компьютерных инцидентах

CMDB, ИТ-мониторинг

Сведения о ИТ-активах

Система автоматизации процессов управления ИБ

- Инвентаризация информационных ресурсов
- Автоматизация категорирования ОКИИ
- Автоматизация анализа угроз ИБ
- Автоматизация управления инцидентами ИБ
- …

Автоматизация бизнес-процессов

BPM, СЭД

- **сведения об объектах защиты**
- **уязвимостях**
- **инцидентах**

Система обеспечения ИБ

Создание системы мониторинга ИБ. Ключевые факторы успеха

1. **Не оставлять белых пятен в плане**
   Сразу определите кто и как будет наводить порядок в промышленной сети

2. **Обеспечить безопасность объекта мониторинга**
   Не забудьте о настройке параметров безопасности объектов промышленной сети

3. **Keep it simple stupid**
   Не надо внедрять высокие технологии в промышленную сеть

4. **80:20**
   Не надо стремиться анализировать 100% трафика (по крайней мере сразу)

5. **Думать о SOCe**
   Что будет выступать в роли SOC и кто будет им пользоваться?

USSC

СПАСИБО ЗА ВНИМАНИЕ!

ВОПРОСЫ?

Николай Домуховский

Заместитель генерального директора

Тел.: +7 (343) 379-98-34

info@ussc.ru

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ | USSC.RU