Практический опыт реализации требований ФЗ-187 «О безопасности критической информационной инфраструктуры» на предприятиях промышленности

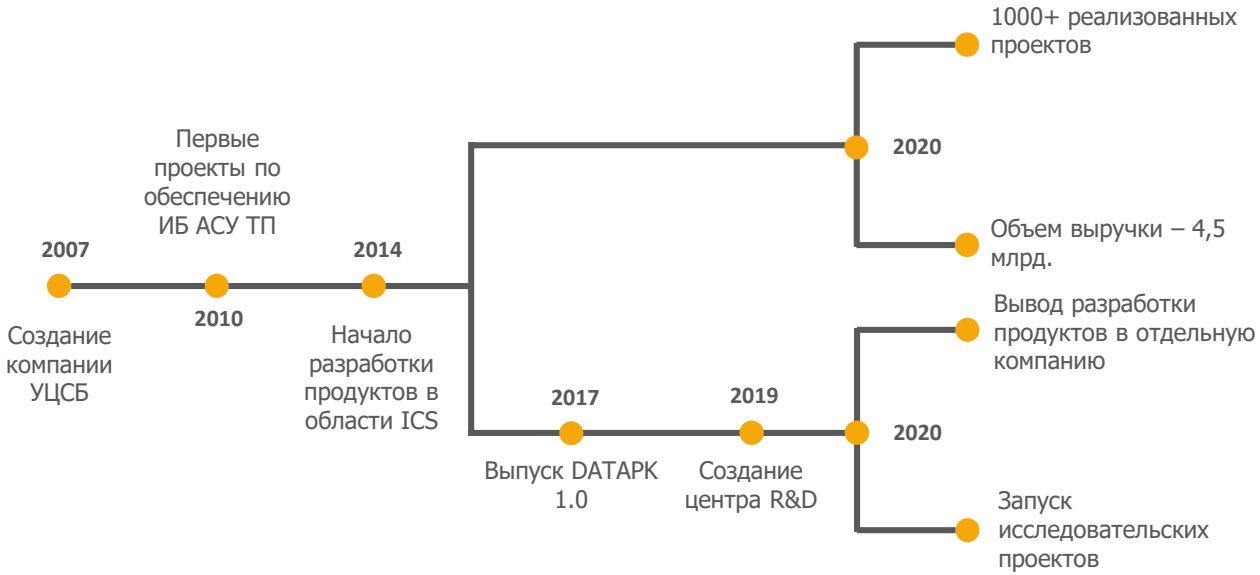
Николай Домуховский

Заместитель генерального директора по научно-технической работе ООО «УЦСБ»

Екатеринбург, 2021

О группе компаний УЦСБ

История компании



Факты

- 2 дочерних предприятия в статусе резидента «Сколково»
- Постоянный член ТК362
- Участник Экспертной подгрупп «Энерджинет» НТИ по кибербезопасности
- 3 патента и 5 свидетельств
- Действующий научно-технический совет

6 из 10 крупнейших металлургических компаний РФ

7 из 10 крупнейших нефтегазовых компаний РФ

6 из 10 крупнейших химических предприятий РФ

6 из 10 крупнейших энергетических компаний РФ

СБОКИИ. Общая структура

Приказ №235

Система безопасности объекта КИИ

Силы

Подразделения, ответственные за безопасность
Подразделения, эксплуатирующие ЗОКИИ
Подразделения, обслуживающие ЗОКИИ

Организационно-распорядительные документы

Цели, задачи, правила и процедуры обеспечения безопасности значимого объекта

Средства

Программные и программно-аппаратные СрЗИ

Приказ №239

СБОКИИ – долгий путь к совершенству

USSC

Категорирование ОКИИ

- Создание комиссии
- Проведение категорирования
- Оформление акта
- Направление результатов во ФСТЭК России

Создание СБОКИИ

- Создание сил СБОКИИ
- Создание средств СБОКИИ
- Разработка ОРД

Функционирование СБОКИИ

Планирование

- Мероприятия по обеспечению функционирования СБОКИИ
- Мероприятия по обеспечению безопасности ОКИИ

Реализация

- Реализация мероприятий по обеспечению функционирования СБОКИИ
- Реализация (внедрение) мероприятий по обеспечению безопасности ОКИИ

Контроль

- Внутренний контроль
- Государственный контроль

Совершенствование

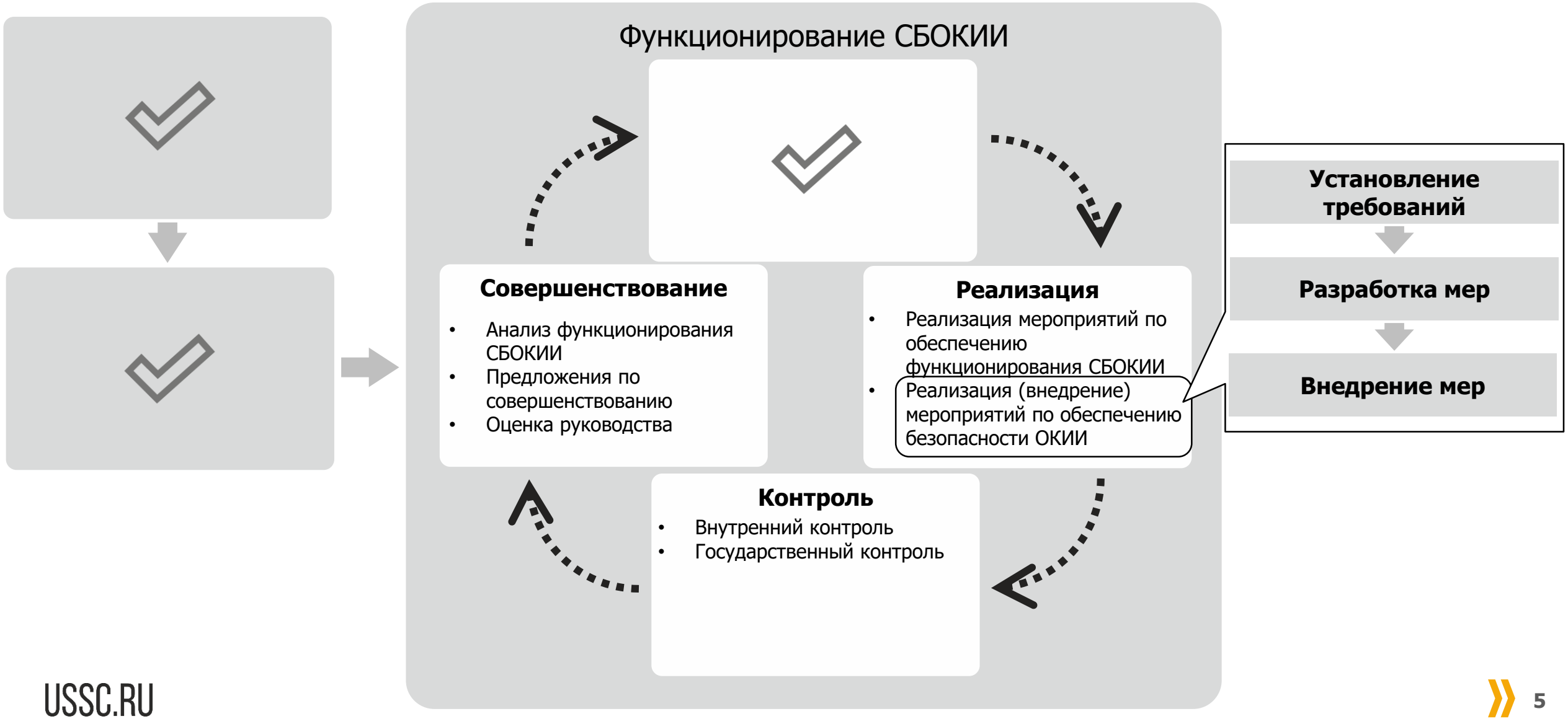
- Анализ функционирования СБОКИИ
- Предложения по совершенствованию
- Оценка руководства

Установление требований

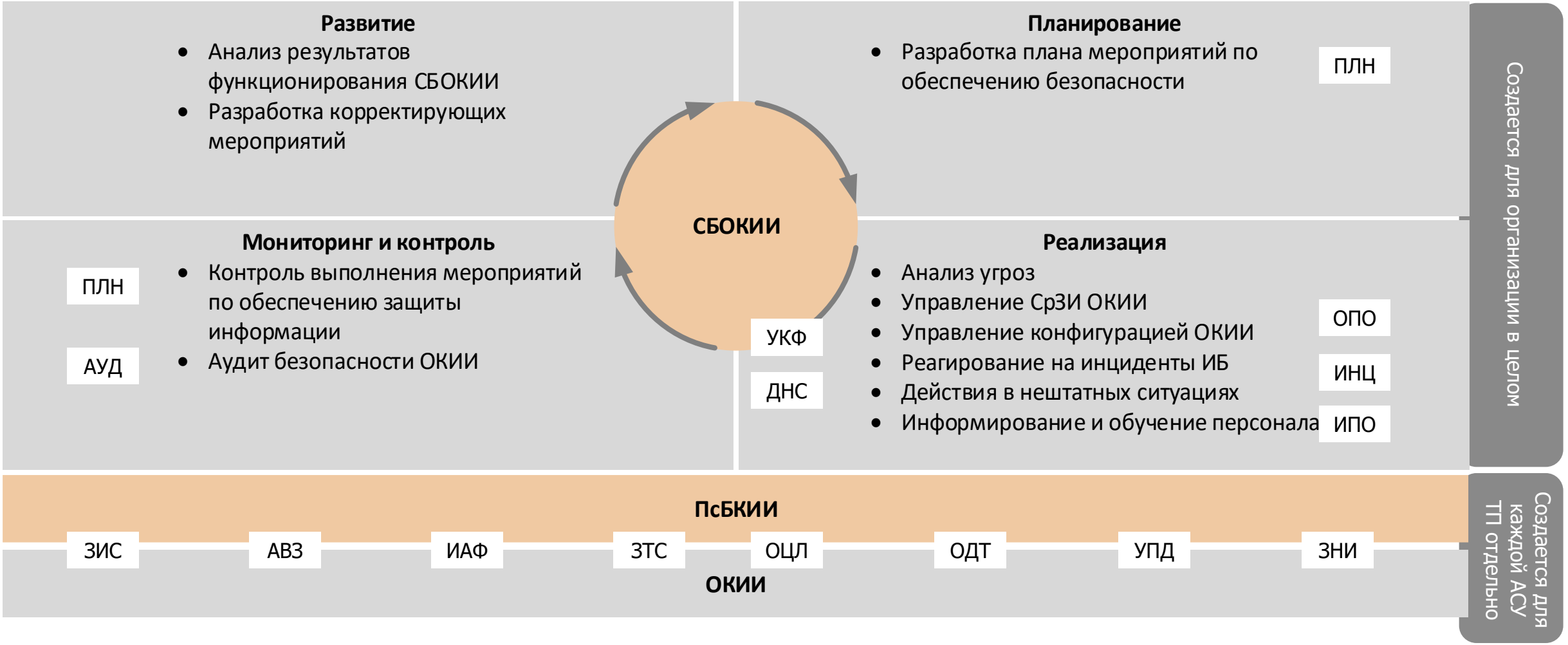
Разработка мер

Внедрение мер

СБОКИИ – долгий путь к совершенству



СБОКИИ и ПсБОКИИ

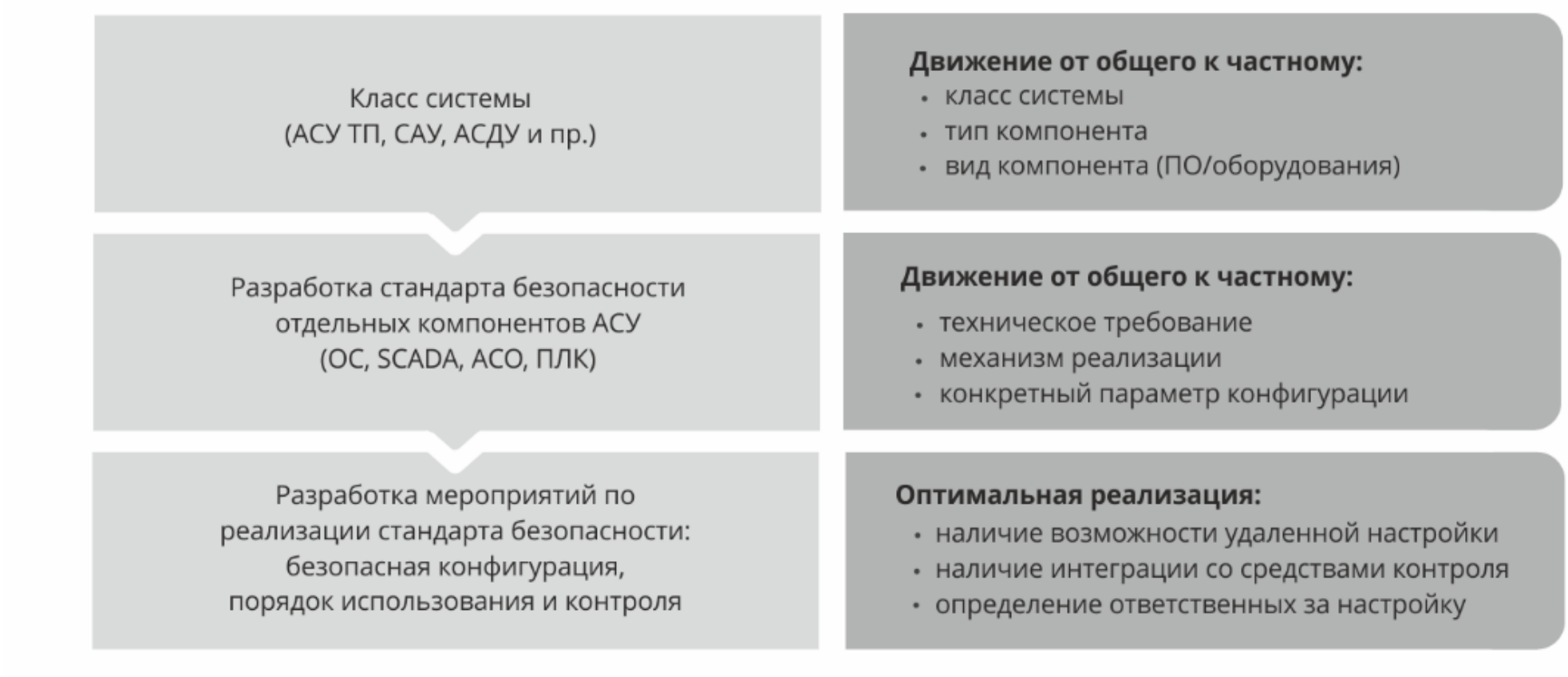


Реализация технических мер

Встроенные СрЗИ
- Меньше негативного влияния на стабильность ОКИИ
- Должны присутствовать изначально
- Уникальны для каждого вида ПО
- Рекомендованы как приоритетные в Приказе 239

Наложенные СрЗИ
- Необходимо обоснование отсутствия негативного влияния
- Требуют для работы дополнительные ресурсы компонентов ОКИИ
- Развитые механизмы централизованного управления

Эффективная реализация встроенных мер



Создание и эксплуатация СБОКИИ – общее дело

USSC

Руководитель субъекта КИИ

- Создает СБОКИИ
- Определяет состав сил и функции участников
- Назначает подразделение по безопасности
- Утверждает планы и результаты контроля

Подразделение по безопасности

- Анализ угроз
- Реализация требований
- Реализация организационно-технических мер
- Реагирование на инциденты
- Оценка соответствия
- Совершенствование СБОКИИ

Подразделение, эксплуатирующее ОКИИ

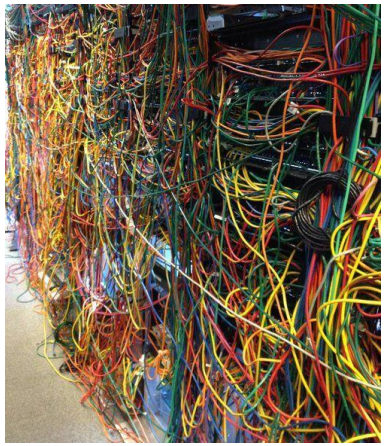
- Эксплуатация ОКИИ в соответствии с правилами по безопасности
- Участие в мероприятиях по: категорированию ОКИИ, планированию мероприятий, контролю за исполнением, подготовке предложений по совершенствованию

Подразделение, обеспечивающее функционирование

- Сопровождение ОКИИ в соответствии с правилами по безопасности
- Участие в мероприятиях по: категорированию ОКИИ, планированию мероприятий, контролю за исполнением, подготовке предложений по совершенствованию

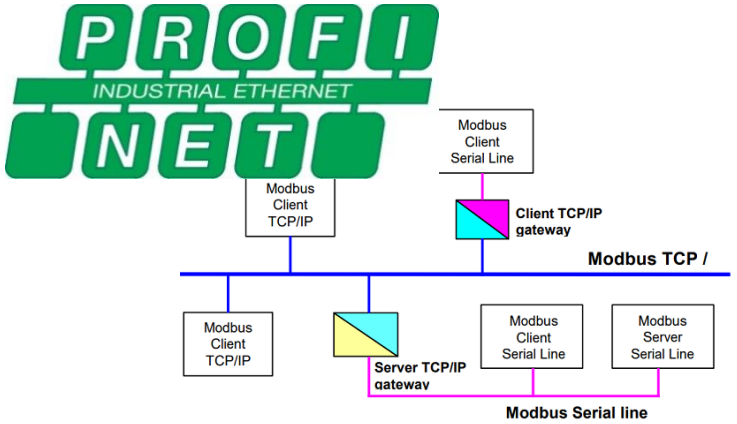
Приказ 235 не определяет явно ответственных за мероприятия: управление СрЗИ, управление конфигурацией ОКИИ и действия в нештатных ситуациях. Конкретное распределение функций должно определяться в ОРД

(не)готовность ОКИИ к внедрению защитных мер



Отсутствует или неактуальная документация на АСУ ТП

Устаревшее оборудование и ПО



Устаревшие или специализированные сетевые протоколы

Модернизация инфраструктуры

- Дополнительные капитальные затраты
- Требует привлечения разработчика АСУ ТП
- Оптимально с точки зрения совокупной стоимости владения
- Инфраструктурой легко управлять и контролировать

Замена организационными мероприятиями

- Просто разработать
- Сложно реально внедрить
- Существенно дороже с точки зрения операционных затрат
- Сложно контролировать

Об «опасности» организационных мероприятий

Работники, эксплуатирующие значимые объекты критической информационной инфраструктуры (пользователи), а также работники, обеспечивающие функционирование значимых объектов критической информационной инфраструктуры, должны выполнять свои обязанности на значимых объектах критической информационной инфраструктуры **в соответствии с правилами безопасности**, установленными организационно-распорядительными документами по безопасности значимых объектов (инструкциями, руководствами).

п. 15 Приказа 235

Рабочая (эксплуатационная) документация на значимый объект должна содержать:
…
правила эксплуатации программных и программно-аппаратных средств, в том числе средств защиты информации (**правила безопасной эксплуатации**).

П. 11.3 Приказа 239

Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации, - **наказывается …**

Ст. 273.1 п.3 УК РФ

Создание СБОКИИ – ключевые факторы успеха

1	Помнить, что СБОКИИ – общая задача (подключение подразделений по сопровождению АСУ ТП, разработчиков и проектировщиков систем автоматизации)
2	СБОКИИ – хороший повод для модернизации. Попытка обеспечить безопасность устаревшей системы может обойтись дороже
3	Организационные мероприятия должны применяться осознанно – по совокупной стоимости владения они дороже технических
4	СБОКИИ – это совокупность непрерывных процессов. И лучше их сразу оптимизировать и автоматизировать
5	СБОКИИ и ПсБОКИИ могут создаваться независимо
6	Все данные, собранные в процессе создания СБОКИИ должны быть сохранены – они еще пригодятся

USSC

СПАСИБО ЗА ВНИМАНИЕ

ВОПРОСЫ?

Николай Домуховский

Заместитель генерального директора по научно-технической работе

ndomukhovsky@ussc.ru

+7 (343) 379-98-34

УРАЛЬСКИЙ ЦЕНТР СИСТЕМ БЕЗОПАСНОСТИ | USSC.RU