СИСТЕМНЫЙ ОПЕРАТОР
ЕДИНОЙ ЭНЕРГЕТИЧЕСКОЙ СИСТЕМЫ
RUSSIAN POWER SYSTEM OPERATOR

Опыт внедрения процесса безопасной разработки в АО «СО ЕЭС»

Александр Малахов

Порядок организации процесса безопасной разработки

Определение цели и области действия

Определение команды

Анализ существующих процессов

Проработка способов достижения целей

Определение набора инструментов (OpenSource / Enterprise)

Включение в существующие процессы

Цели и область действия

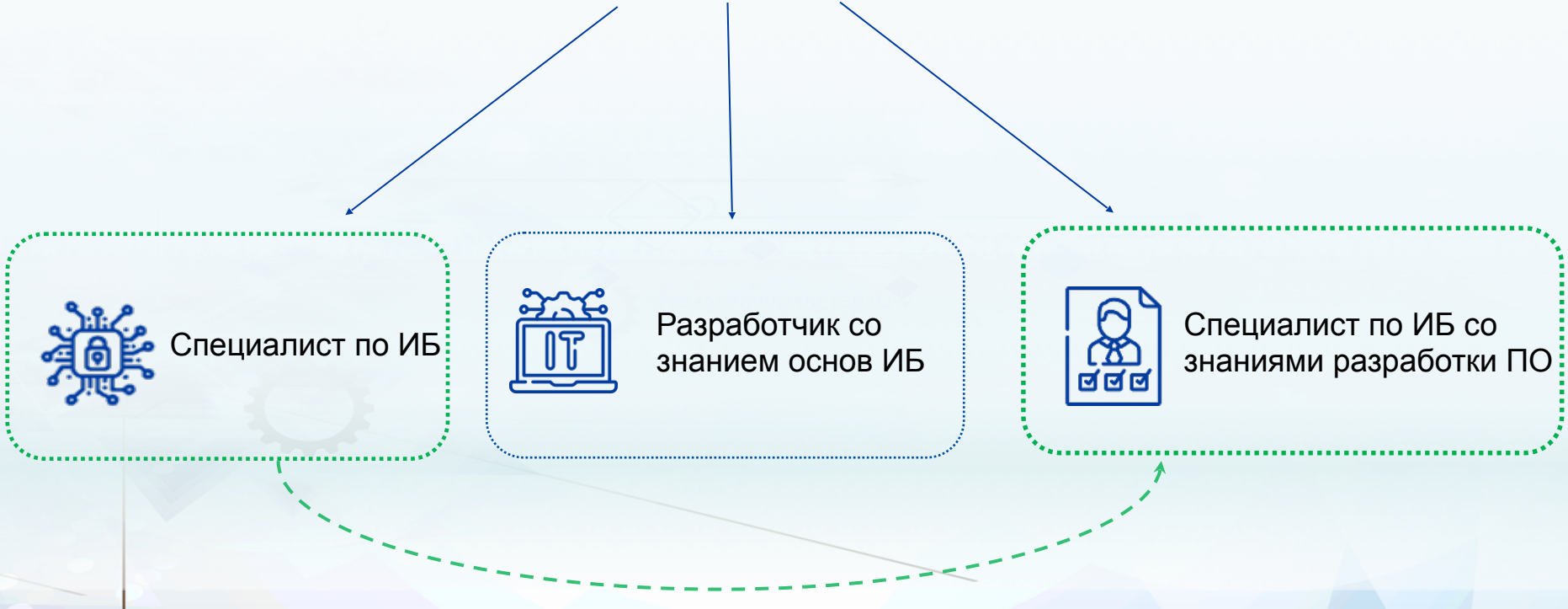
Выполнение требований ИБ
- Внешние
- Внутренние

Контроль требований ИБ

№	Критерий	Да	Нет
01	Критическая система для бизнес-процессов / объект КИИ	+10	0
02	Система с высокими требованиями обслуживания (24/7)	+5	-2
03	Система связана с критическими системами (каскадный риск)	+7	-2
04	Система или часть системы имеют выход в сеть интернет	+5	-2
05	Проект носит вспомогательный характер	-5	+5

Состав команды управления процессами безопасной разработки

Кто может входить в состав команды?



Анализ существующих процессов разработки и включение в них

Анализ:
- архитектуры
- требований ИБ

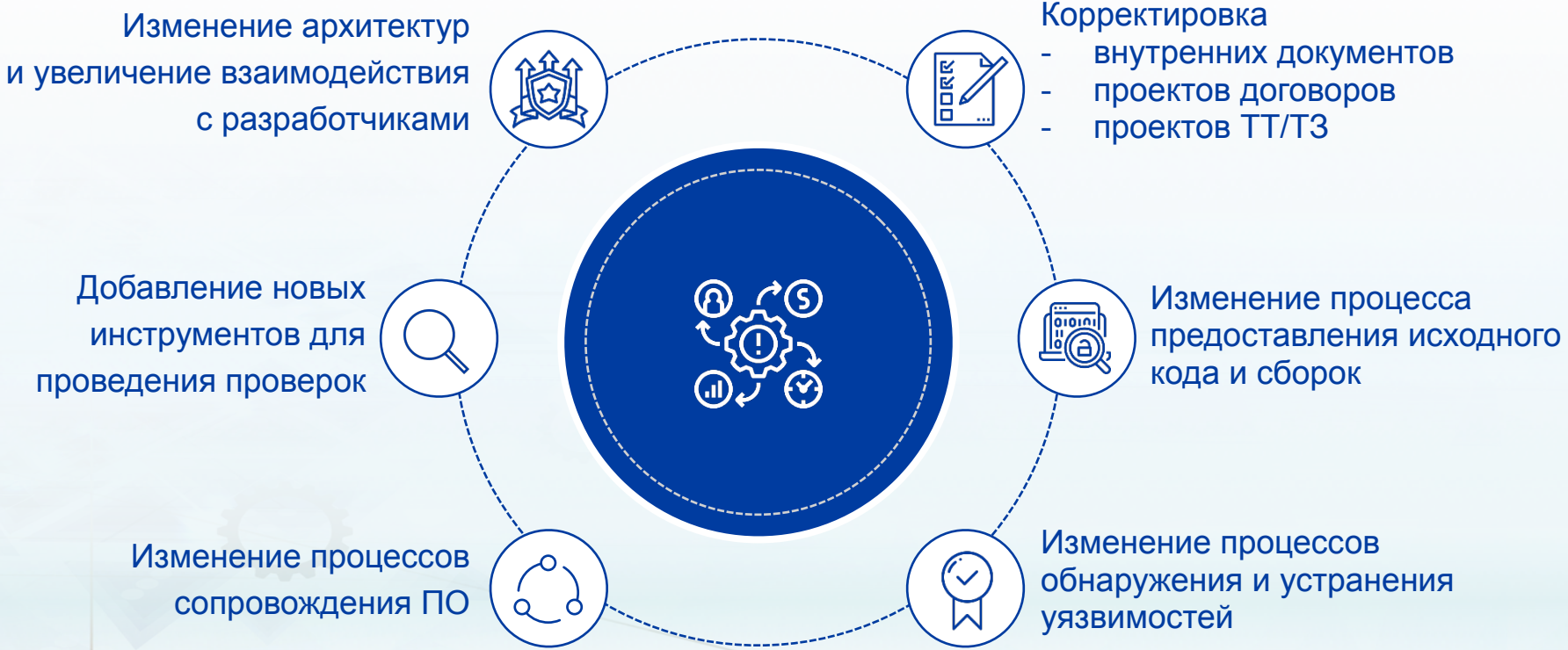
Оценка рисков
Моделирование угроз

SAST/DAST/SCA
Участие команды ИБ
Пересмотр угроз/ рисков

Проверка:
- исходного кода
- ПО
- конфигурации
- среды функционирования
- анализ документации

Анализ изменений
Регулярная проверка среды функционирования
Повторный анализ ИК
Контроль уязвимостей в зависимостях

Проработка способов достижения целей и определение набора инструментов



Зачем нужен процесс безопасной разработки на стороне заказчика?

Контроль требований ИБ

Внутренние требования
Требования регуляторов

Выявление проблем при переносе ПО в реальную среду выполнения

Недоверие к РБПО у разработчика

Выводы

Безопасная разработка

Безопасная разработка требует усиление логической связки всех компонентов системы

Весь процесс не уложится в один документ

Необходимо выделить, что можно проверить на стороне заказчика и что на стороне разработчика

Спасибо за внимание!