



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

2



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

3

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

4

Кто может входить в состав команды?



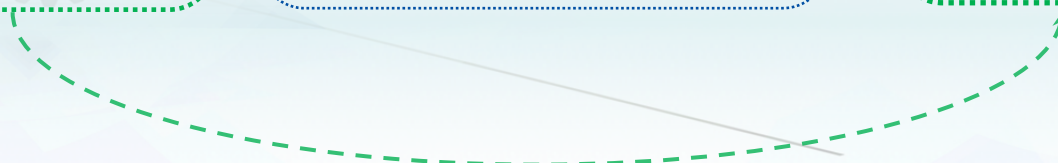
Специалист по ИБ



Разработчик со
знанием основ ИБ



Специалист по ИБ со
знаниями разработки ПО





Анализ существующих процессов разработки и включение в них

5



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

6

Изменение архитектур
и увеличение взаимодействия
с разработчиками



Корректировка

- внутренних документов
- проектов договоров
- проектов ТТ/ТЗ



Добавление новых
инструментов для
проведения проверок



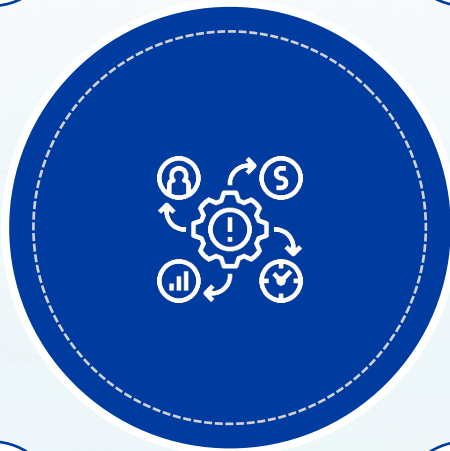
Изменение процесса
предоставления исходного
кода и сборок



Изменение процессов
сопровождения ПО



Изменение процессов
обнаружения и устранения
уязвимостей





Зачем нужен процесс безопасной разработки на стороне заказчика?

7



Контроль требований ИБ

Внутренние требования
Требования регуляторов



Выявление проблем при переносе ПО в реальную среду выполнения



Недоверие к РБПО у разработчика



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!

1234567890D48E1563QW