AKTIV.
CONSULTING

Внедрение процесса безопасной разработки ПО в субъектах КИИ

Александр Моисеев

Ведущий консультант по информационной безопасности AKTIV.CONSULTING

Инфобереg, 7–9 сентября 2022

О чем сегодня пойдет речь

01

Препятствия для внедрения БРПО

02

Рассмотрим пример проекта по внедрению БРПО

03

Рассмотрим типовой пример процессов БРПО

Драйверы внедрения БРПО

01 **Требования регулятора**

02 **Политика активного импортозамещения на ЗО КИИ**

(к 2024 году затраты госкомпаний на отечественные IT-продукты оцениваются в 650 млрд руб.)

03 **Бизнес потребность**

	Конечные пользователи ПО	Разработчики ПО
Бизнес-цели	▪ Обеспечение непрерывности бизнеса (управление рисками) ▪ Соответствие требованиям регулятора	▪ Увеличение объемов продаж ПО (доп. конкурентные преимущества) ▪ Сокращение стоимости разработки продукта

Резюме:
в большинстве случаев процедуры БРПО в требуемом объеме **не внедрены,** организации зачастую не знают, с какой стороны «подступиться» к столь комплексным изменениям.

Препятствия для внедрения БРПО

- Обоснование внедрения БРПО
- «Сопротивление» разработчиков
- Трактовка требований регулятора
- Неопределенность влияния на существующие бизнес - процессы
- Постановка кроссфункционального взаимодействия

Решение:

к БРПО нужно подходить сперва как к проекту, в ходе которого в текущую разработку будут внедрены процессы.

Зависимость параметров проекта от типа разработки

Основные процессы БРПО

Тип 1 «внутренняя»	Менеджмент БРПО	Разработка ПО	Поддержка ПО в ходе ЖЦ	Обучение персонала	Управление конфигу-рацией	Управление инфраструктурой среды разработки	Правовое регулирование
Тип 2 «заказная»	Менеджмент БРПО	Получение свидетельств по процессам (в максимально полном объеме)					Правовое регулирование
Тип 3 «вендорская»	Менеджмент БРПО	Получение свидетельств по процессам (в достаточном объеме)					Правовое регулирование

Пример проекта по внедрению БРПО

1 этап **Обоснование**

Результат этапа:
ТЭО и принятое на его основе решение руководства

2 этап **GAP-анализ**

Результат этапа:
орг. и тех. меры

3 этап **Разработка дорожной карты**

Результат этапа:
подготовка «Дорожной карты...»

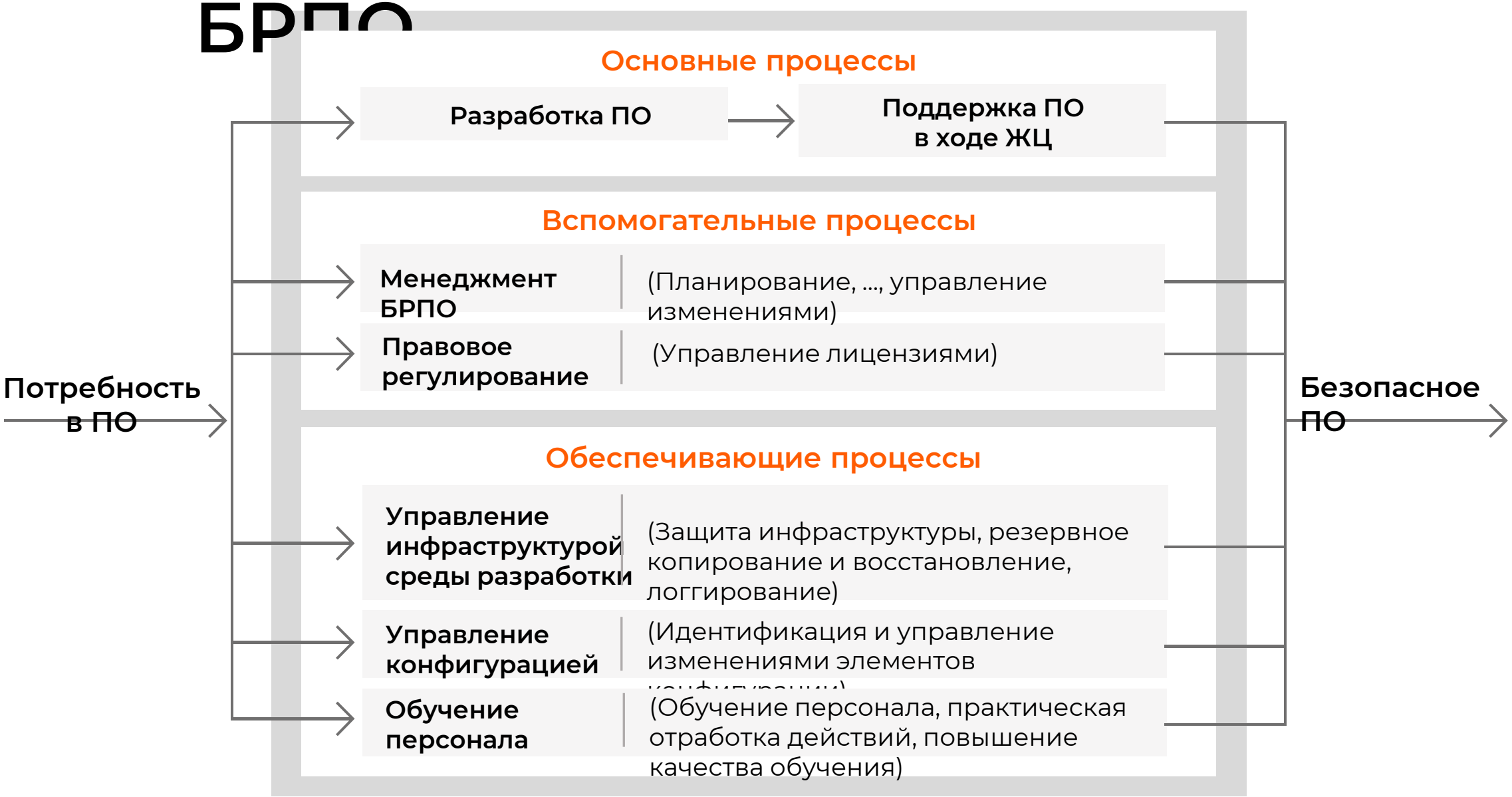
4 этап **Внедрение процессов**

Результат этапа:
функционирующие процессы БРПО

5 этап **Контроль**

Результат этапа:
свидетельства функционирования БРПО

Типовой пример процессов БРПО



Подпроцессы разработки и поддержки ПО

Разработка ПО

- Разработка «Руководства по БРПО»
- Анализ и моделирование угроз
- Сопоставление функций и интерфейсов с подсистемами ПО (для ЗО КИИ 1 кат.)
- Статический анализ кода
- Фаззинг-тестирование
- Динамический анализ кода (для ЗО КИИ 1 кат.)

Поддержка ПО в ходе ЖЦ

- Систематическое выявление уязвимостей в ходе ЖЦ
- Оповещение пользователей об ошибках, выявленных уязвимостях, компенсирующих мерах
- Оповещение об окончании ЖЦ ПО и завершении технической поддержки (для ЗО КИИ 1 кат.)

Методологии: ГОСТ Р 56939, ГОСТ Р ИСО МЭК 27034xx, ГОСТ Р ИСО МЭК 15408xx, ГОСТ Р 59193, ГОСТ Р 59194, ГОСТ Р 58412, Методика по моделированию угроз ФСТЭК (2021), БДУ ФСТЭК, Методика ФСТЭК ВУ и НДВ (2020)*, проекты ГОСТ ТК 362, ГОСТ Р 58143, приказ ФСТЭК 76 от 02.06.2020

* - ограниченного распространения

Инструменты: SAST, DAST, Fuzzing, SCA, Pentest, ...

Резюме:

для внедрения процессов БРПО в минимально требуемом объеме есть все необходимое — драйверы, методики, инструменты.

В качестве резюме

Проект по внедрению БРПО в объеме требований ФСТЭК России это подъемная задача, и она не разрушит имеющиеся процессы разработки, потому что:

01

Гибкий проектный подход ко внедрению БРПО:

- гарантирует достижение востребованного результата в ограниченные сроки
- имеет ответственного за внедрение (руководителя проекта)
- внедрение происходит в соответствии с дорожной картой

02

Процессный подход позволяет:

- учитывать индивидуальные особенности организации
- достигать мультипликативного эффекта от взаимодействия обособленных функциональных подразделений

AKTIV.
CONSULTING

Александр Моисеев

Ведущий консультант
по информационной безопасности

moiseev@aktiv.consulting

Олег Симаков

Руководитель направления
по работе с клиентами

simakov@aktiv.consulting