

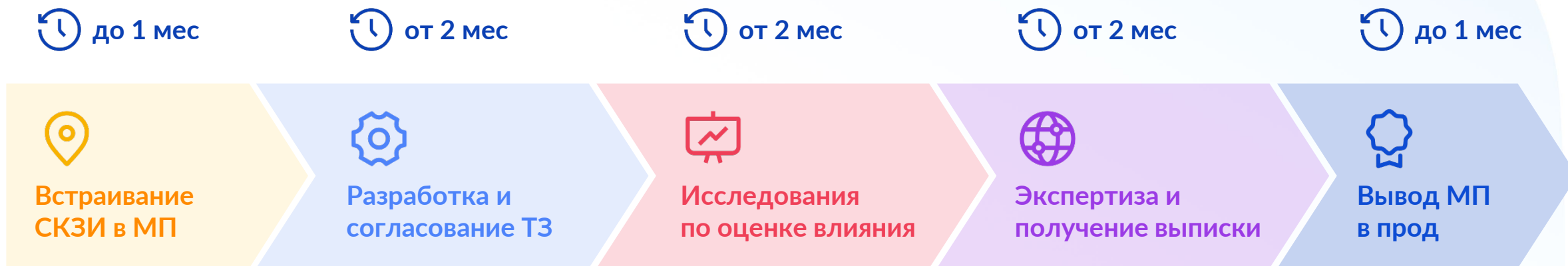
# Развитие «гражданской» криптографии

Выпуск обновлений мобильных приложений с встроенным СКЗИ: проблемы и частные решения

Роман Кондратенко, РТЛабс

# ПОЛОЖЕНИЕ ПКЗ-2005




Проведение работ по оценке влияния МП на выполнение предъявленных к СКЗИ требований



Итого: от 8 и более месяцев

## Актуальность

Потребность в расширении функционала  
МП «Госуслуги»

-  ГОСТ TLS
-  Поддержка криптографических протоколов ЕСИА
-  Проверка и формирование ЭП  
(функционал «Госключача»)

## Проблематика

- Частота выпуска обновлений МП со встроенным СКЗИ — несколько раз в квартал
- Проведение повторной ОВ при обновлении МП (изменение СФ СКЗИ) — от 6 и более месяцев

# РЕШЕНИЕ

## Организационное

Разработка регламента проведения исследований по оценке влияния мобильных приложений на встроенное СКЗИ и его согласование с ЦЗИСС ФСБ России

## Техническое

Создание в АО «РТЛабс» сборочного конвейера для встраивания СКЗИ в мобильные приложения

# Организационная составляющая решения



Разработка регламента проведения исследований по оценке влияния мобильных приложений на встроенное СКЗИ и его согласование с ЦЗИСС ФСБ России

## Организации — участники взаимодействия:

- Разработчик МП
- Производитель СКЗИ
- Испытательная лаборатория
- ЦЗИСС ФСБ России

## Апробация решения для МП:

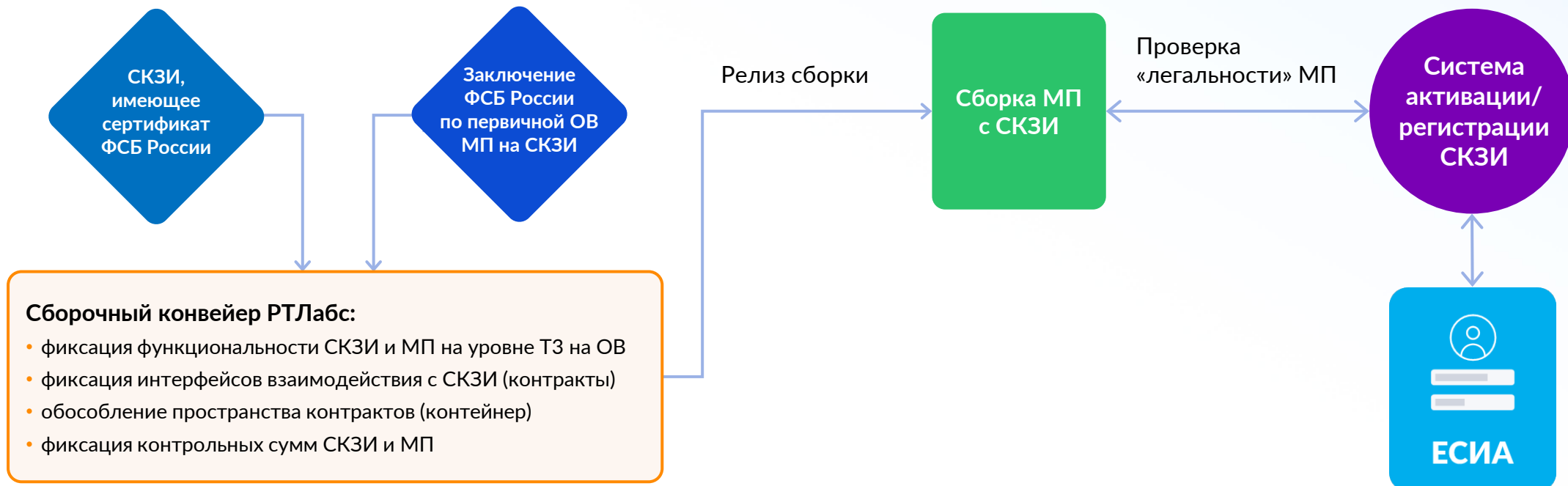
- Госуслуги
- Госуслуги. Карта болельщика



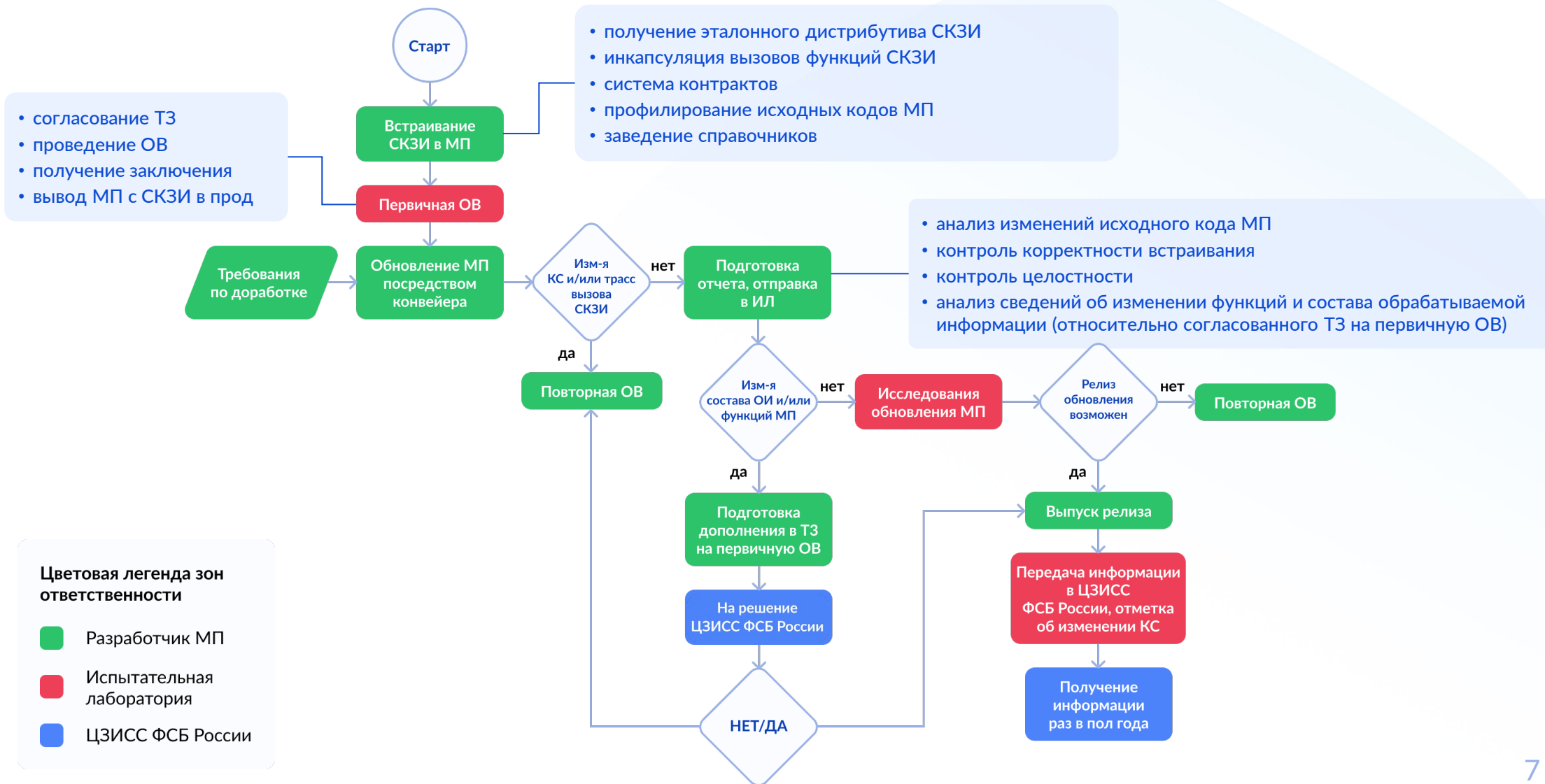
# Техническая составляющая решения

✔ Разработали специальную архитектуру приложения

Схема выпуска релиза МП с встроенным СКЗИ с использованием сборочного конвейера

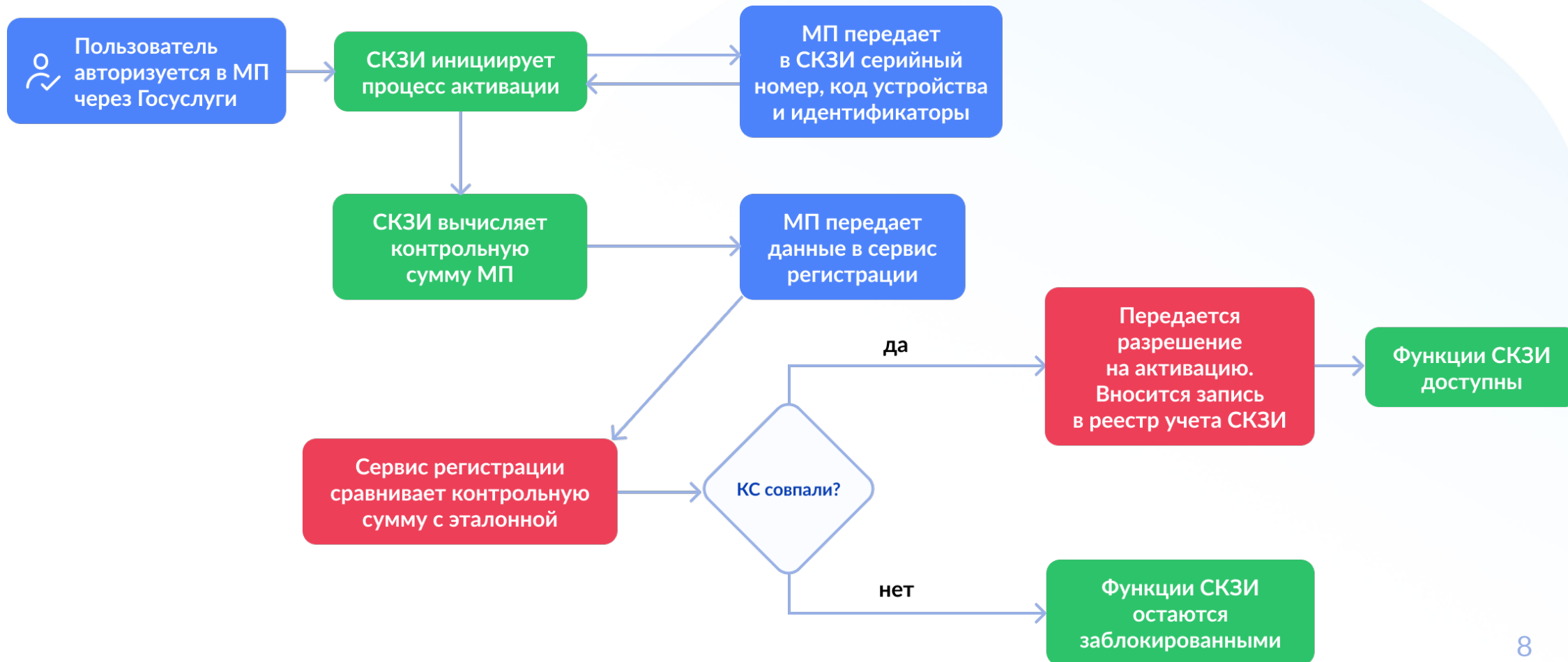


# Как соответствовать требованиям?



# Как контролировать легальность сборки?

Схема активации СКЗИ в составе приложения








## Особенности разработки мобильного приложения:

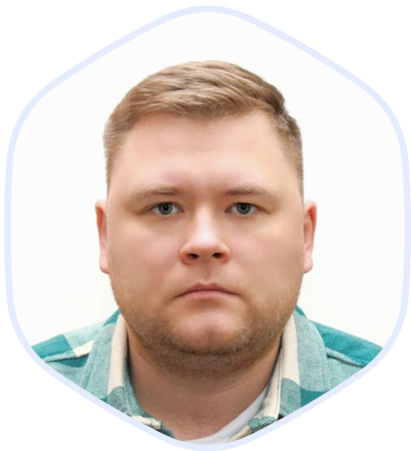
- проектирование архитектуры мобильного приложения — инкапсуляция вызовов функций СКЗИ, контроль неизменности трасс вызова СКЗИ, система контрактов
- профилирование исходных кодов МП по идентификаторам, явно указывающим на признаки вызова функций СКЗИ

## Особенности сборки МП и дополнительные инструменты контроля на этапе разработки:

- контроль целостности дистрибутива СКЗИ
- заведение справочников: идентификаторов профилирования, цепочек вызовов СКЗИ, контрольных сумм мобильного приложения и СКЗИ
- проверка релизной сборки на соответствие эталонным значениям из справочников
- проверка неизменности трасс вызовов СКЗИ
- сбор перечня изменений по исходным кодам мобильного приложения
- формирование отчетов

- ✓  Согласован Регламент проведения оценки влияния в условиях регулярного изменения бизнес-функций приложения
- ✓  Ожидаемые сроки рассмотрения релиза лабораторией сравнимы со сроками рассмотрения приложения магазинами приложений, процессы проходят параллельно
- ✓  Реализован ТЕХНОЛОГИЧЕСКИЙ подход к контролю исполнения требований Положения ПКЗ-2005 при коротком релизном цикле мобильного приложения

# Ваши вопросы и уточнения



**Роман Кондратенко**

Старший системный аналитик РТЛабс

✉ [roman.kondratenko@rtlabs.ru](mailto:roman.kondratenko@rtlabs.ru)

📍 [ko\\_rom\\_se](#)

