Безопасный DevOps

Swordfish Security

Газизова Светлана

Руководитель направления аудита
безопасной разработки

sgazizova@swordfishsecurity.ru
tg @gazizovasg

Почему есть смысл меня слушать?

#ктоя

руководитель направления аудита безопасной разработки: выстраиваю процессы, занимаюсь стратегией AppSec и всея, что около☺
автор и тренер курсов DevSecOps

#ктомы

архитекторы, консультанты, инженеры процессов безопасной разработки
внедряли DevSecOps/Appsec в финтех, банки, ИТ-компании, здравоохранение, гос.сектор

О чем поговорим?

«С чем боролись, на то и напоролись» или влияние автоматизации на безопасность.

Программа минимум: как начать, чтобы недолго и недорого?

Процесс, который и есть результат.

Интересное наблюдение

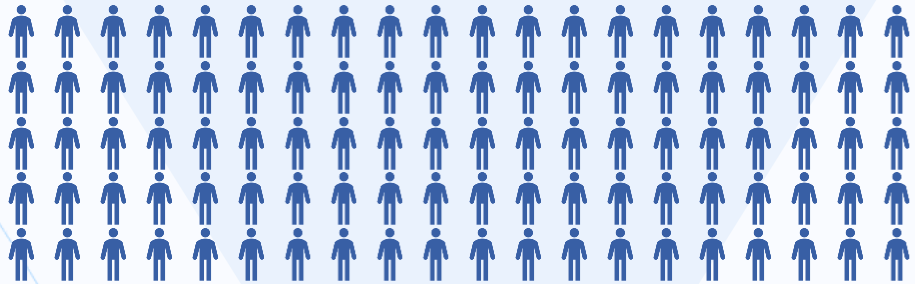

WAJ | Shutterstock

Зачем мне AppSec?

DEV secops

Соотношение

100:10:1



Разработчики ПО
(Development)

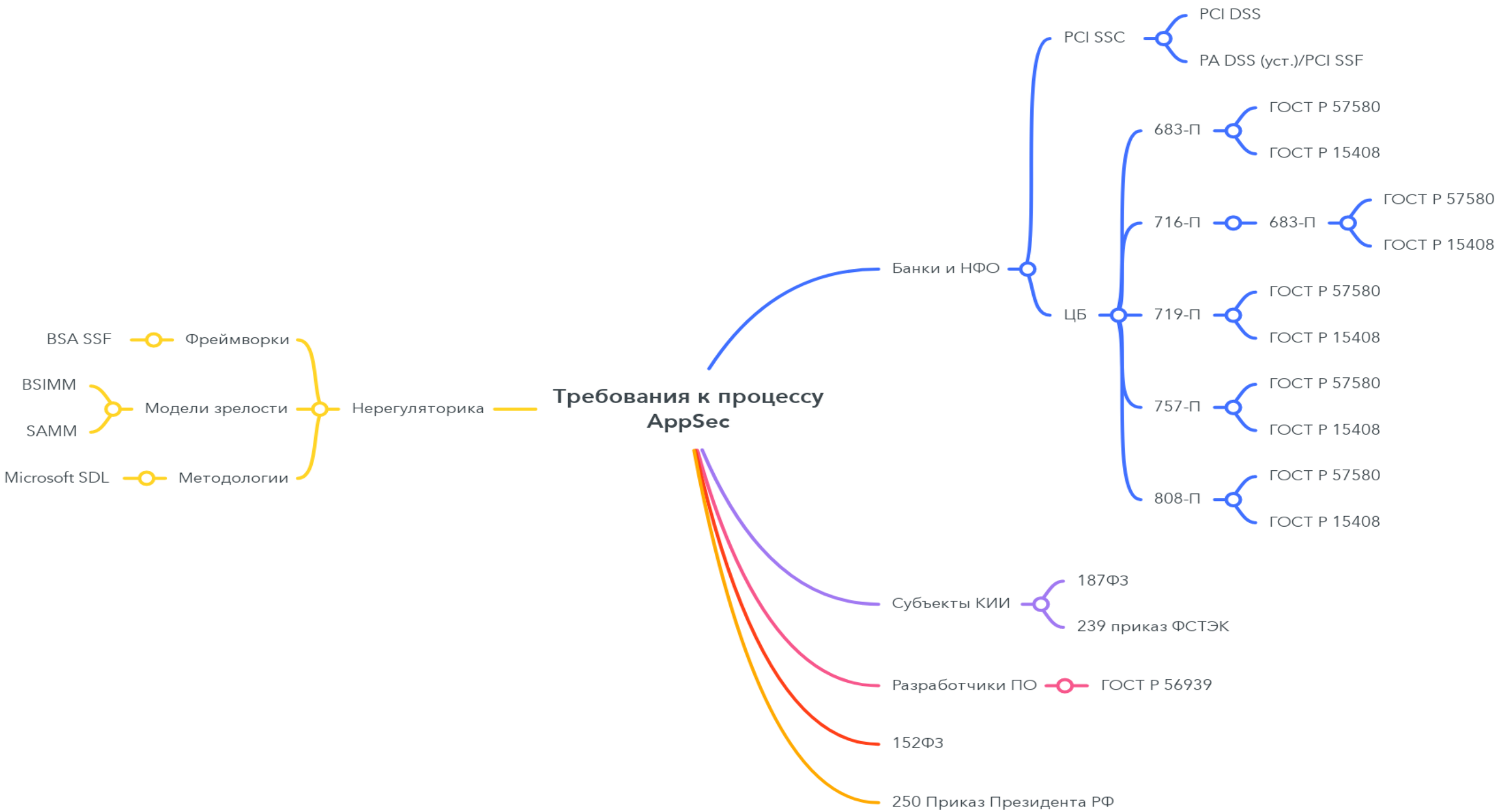
Инженеры сопровождения
(Operations)

Эксперт ИБ
(Security)

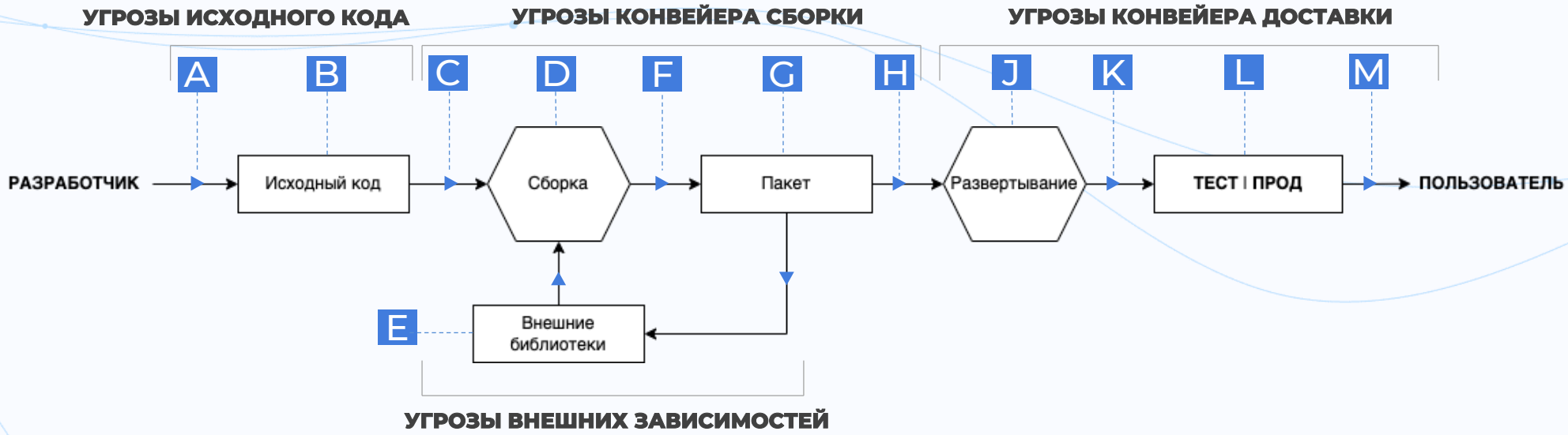
90% инцидентов безопасности вызваны дефектами исходного кода

21% утечек данных вызван уязвимостями программного обеспечения

1 из 3 приложений содержит критическую уязвимость


Требования к процессу AppSec
Банки и НФО
PCI SSC
PCI DSS
PA DSS (уст.)/PCI SSF
ЦБ
683-П
ГОСТ Р 57580
ГОСТ Р 15408
716-П
683-П
ГОСТ Р 57580
ГОСТ Р 15408
719-П
ГОСТ Р 57580
ГОСТ Р 15408
757-П
ГОСТ Р 57580
ГОСТ Р 15408
808-П
ГОСТ Р 57580
ГОСТ Р 15408
Субъекты КИИ
187ФЗ
239 приказ ФСТЭК
Разработчики ПО
ГОСТ Р 56939
152ФЗ
250 Приказ Президента РФ
Нерегуляторика
Модели зрелости
BSIMM
SAMM
Фреймворки
BSA SSF
Методологии
Microsoft SDL

«Восстание машин»



УГРОЗЫ ИСХОДНОГО КОДА

A Обход процесса ревью кода

B Компрометация системы управления исходным кодом

УГРОЗЫ КОНВЕЙЕРА СБОРКИ

C Несанкционированная модификация кода

D Компрометация системы сборки

F Обход CI/CD процесса

G Компрометация репозитория

H Использование уязвимого пакета

УГРОЗЫ ВНЕШНИХ ЗАВИСИМОСТЕЙ

E Использование уязвимых библиотек / зловредных компонент с открытым исходным кодом

УГРОЗЫ КОНВЕЙЕРА ДОСТАВКИ

J Компрометация системы развертывания

K Использование уязвимых контейнеров

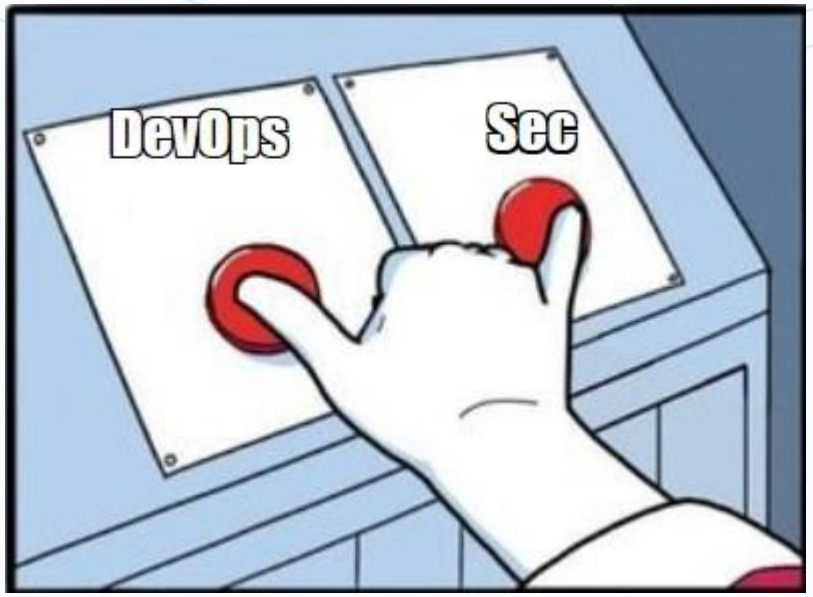
L Компрометация инфраструктурного окружения

M Эксплуатация уязвимых интерфейсов

Хороший DevOps – безопасный DevOps

Хорошее ПО делает именно то, что описано в спецификации требований.

Защищенное ПО делает именно то, что описано в спецификации требований **и ничего более.**



Безопасность – мера качества!

Окей, а как мне сделать разработку безопасной?

С чего начать?

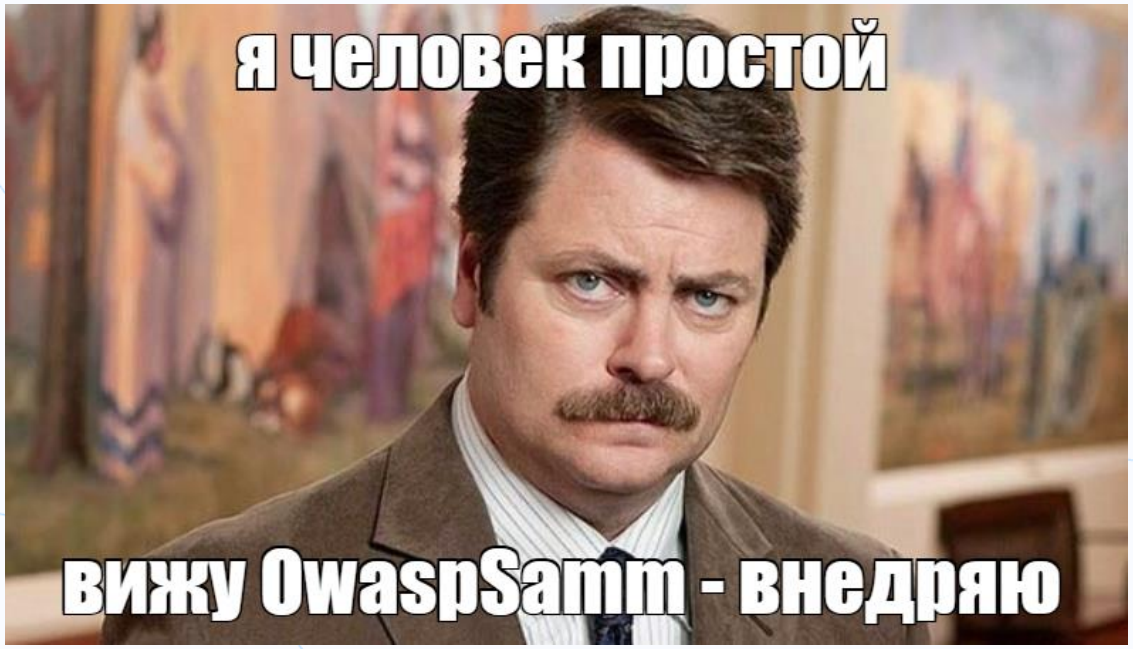
Инструменты безопасной разработки – **есть**!

Инструменты безопасной разработки – **работают**!

Люди **знают,** как работают инструменты и что с этим делать!

Методология

Копать отсюда и до обеда!



Фреймворки и модели зрелости:

BSIMM
OwaspSAMM
...

Методология

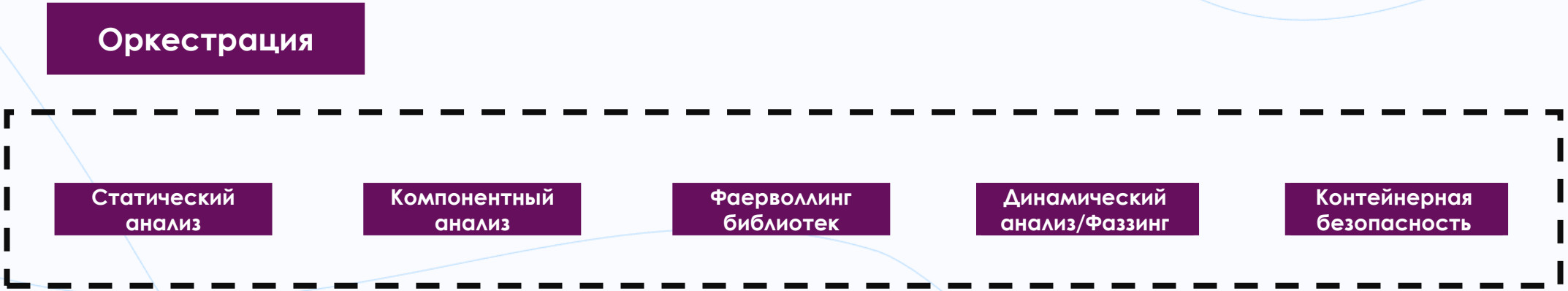
Начатое дело доводи до конца!

ГОСТы и другие стандарты:

ГОСТ 56939
ГОСТ 15408
PCI DSS
ISO 27xxx
…

Программа минимум

Чем меньше у вас ресурсов, тем правильнее надо делать сначала.

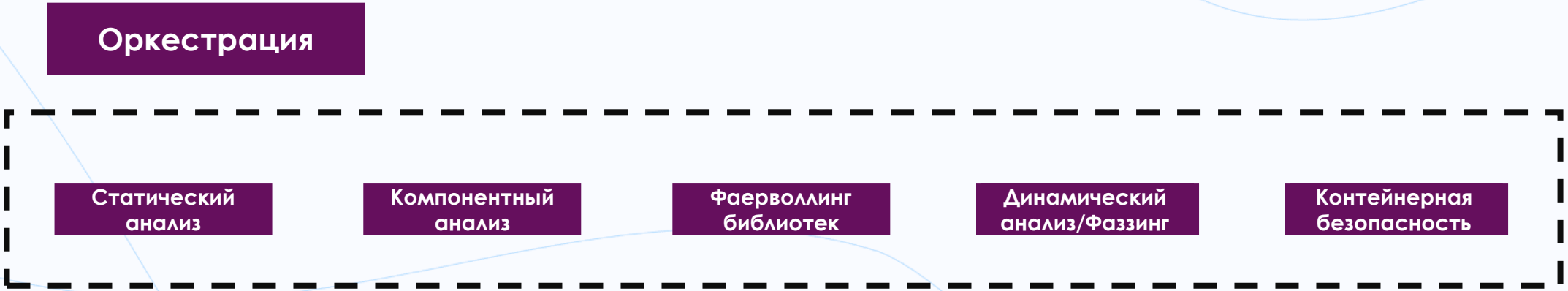


! Все решения подобраны с учетом используемого технологического стека и при обязательном соблюдении одного из двух критериев:

1. Инструмент Open Source
2. Инструмент разработан в РФ/Вендор не находится на территории недружественного государства

Это что, программа минимум?..

Чем меньше у вас ресурсов, тем правильнее надо делать сначала.



! Все решения подобраны с учетом используемого технологического стека и при обязательном соблюдении одного из двух критериев:

1. Инструмент Open Source
2. Инструмент разработан в РФ/Вендор не находится на территории недружественного государства

Программа минимум:)

Развитие экспертизы

- В командах разработки выделить роль **Security Champion’a**, обеспечить полномочиями и ресурсами.

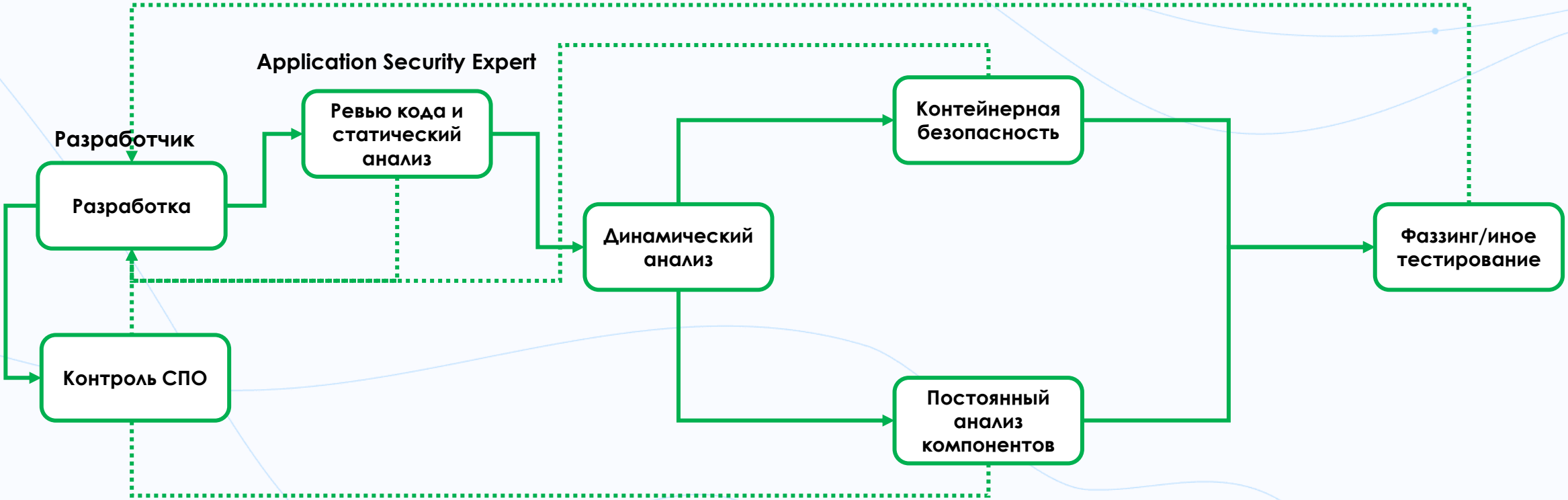
- Создать **центр компетенций Application Security** для создания внутренней экспертизы в области разработки защищенного ПО, внедрения программ осведомленности, обучения, руководств по проектированию и разработке защищенных систем, приложений и сервисов.

- Организовать **внутренний портал AppSec**, где будет располагаться информация, полезная сотрудникам, занятым в области обеспечения безопасности приложений.

Выстраивание процесса

- Определение процесса безопасной разработке на основе существующего **DevOps-процесса.**
- Разработка и внедрение **комплекта документов**, регламентирующих безопасную разработку: процедуры, регламенты, процессы, стандарты, требования
- Адаптация **организационной структуры** под требуемые изменения
- Регулярный **анализ метрик** и контроль улучшений в части безопасной разработки.

Так и какой процесс будет?

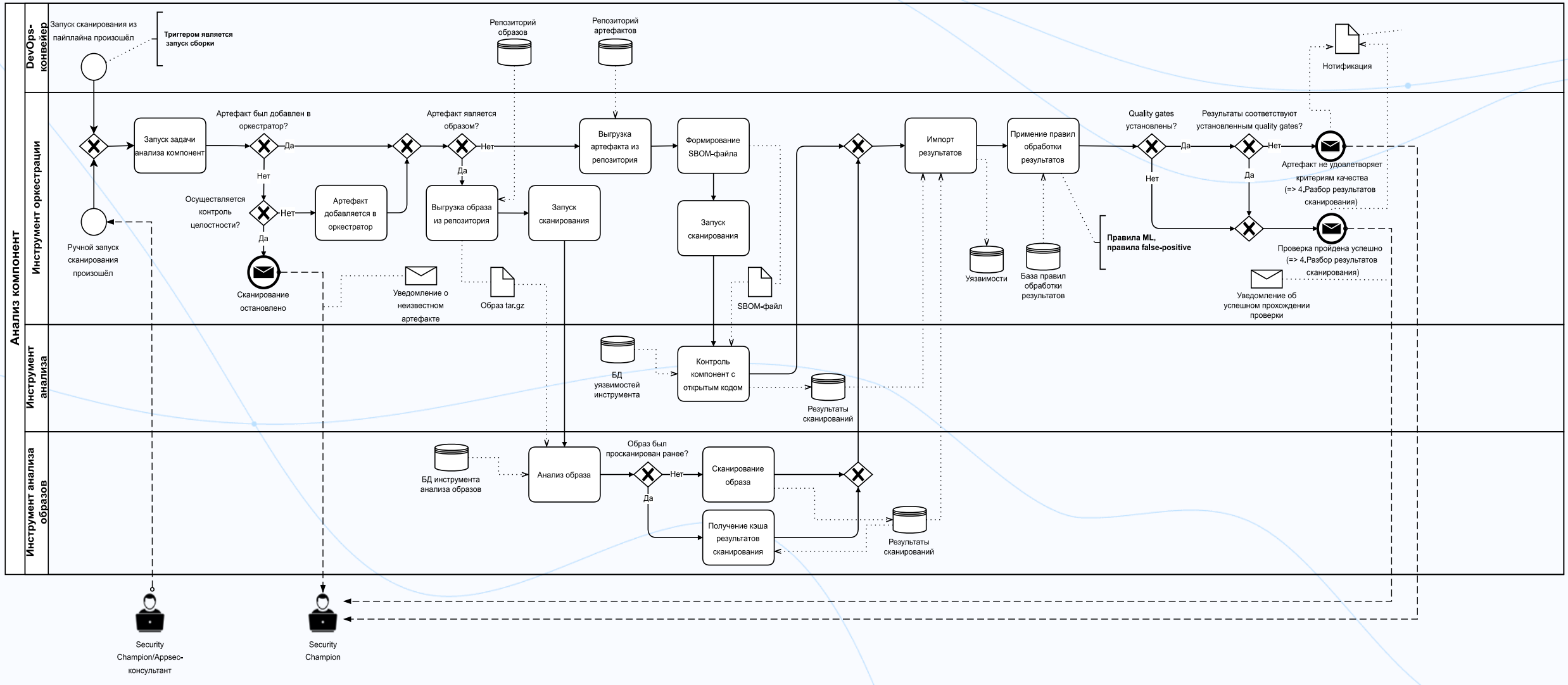


А что внутри процесса?

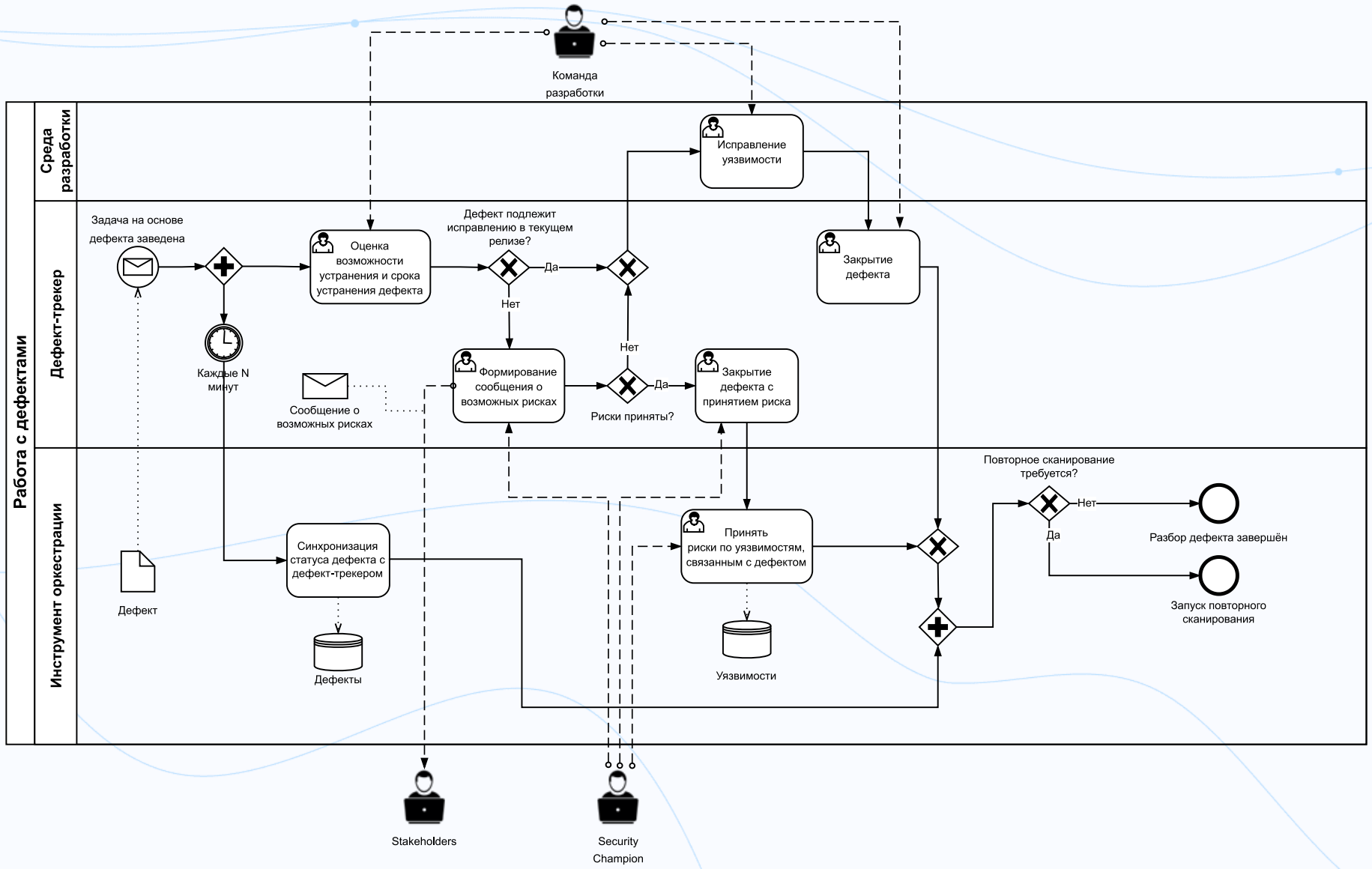
А что внутри процесса?

Тоже процесс!

На примере анализа компонент



А что с разбором дефектов?



Но у вас будет по-другому

Полезные мысли

1. Обеспечьте себя людьми (хорошо, хотя бы одним человеком).

2. Организуйте хотя бы пару инструментов.

3. Внедрите процессные проверки: моделирование угроз, анализ требований ИБ, проверки по архитектурному чек-листу…

4. Делитесь информацией!

Вы еще здесь?

Идеи, вопросы и предложения:

sgazizova@swordfishsecurity.ru
tg @gazizovasg