



Московский институт электроники
и математики им. А.Н. Тихонова

DevOps/DevSecOps.
Безопасная разработка

2024

Конвейер безопасной разработки ПО

Елаев Сергей



План по теме

1. Теория. Стандарты. Методологии. Угрозы при БРПО.
2. Процессы БРПО. Описание конвейера и инструменты БРПО.

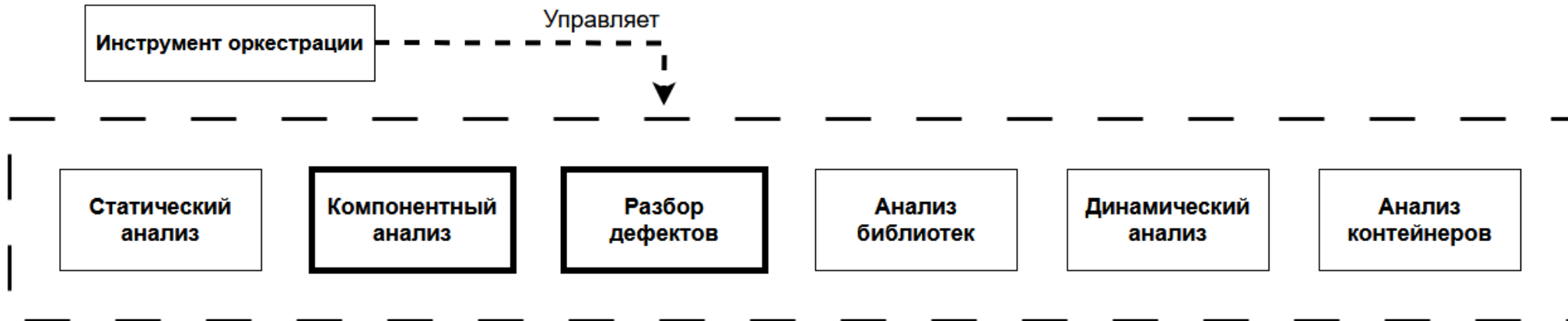


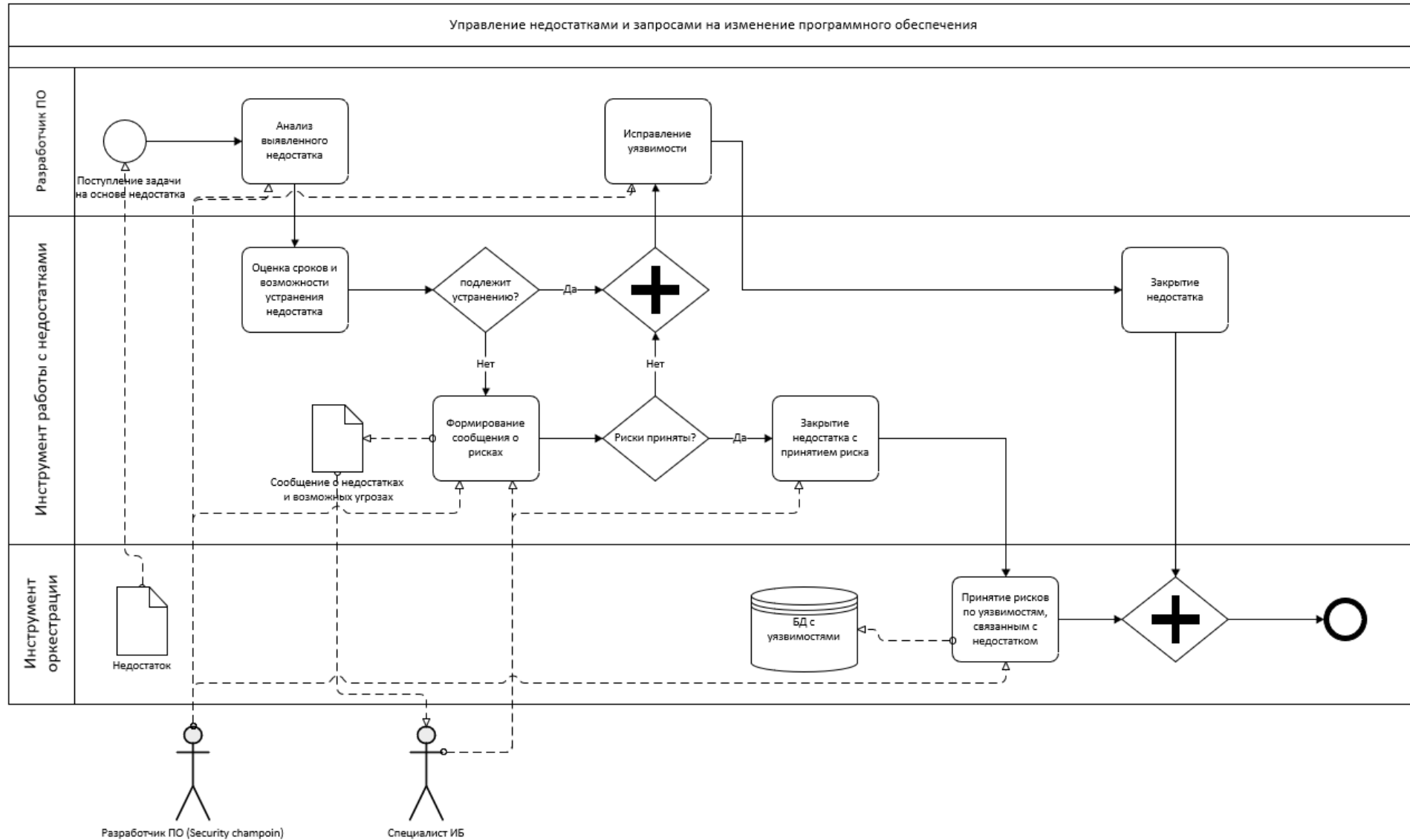
План занятия

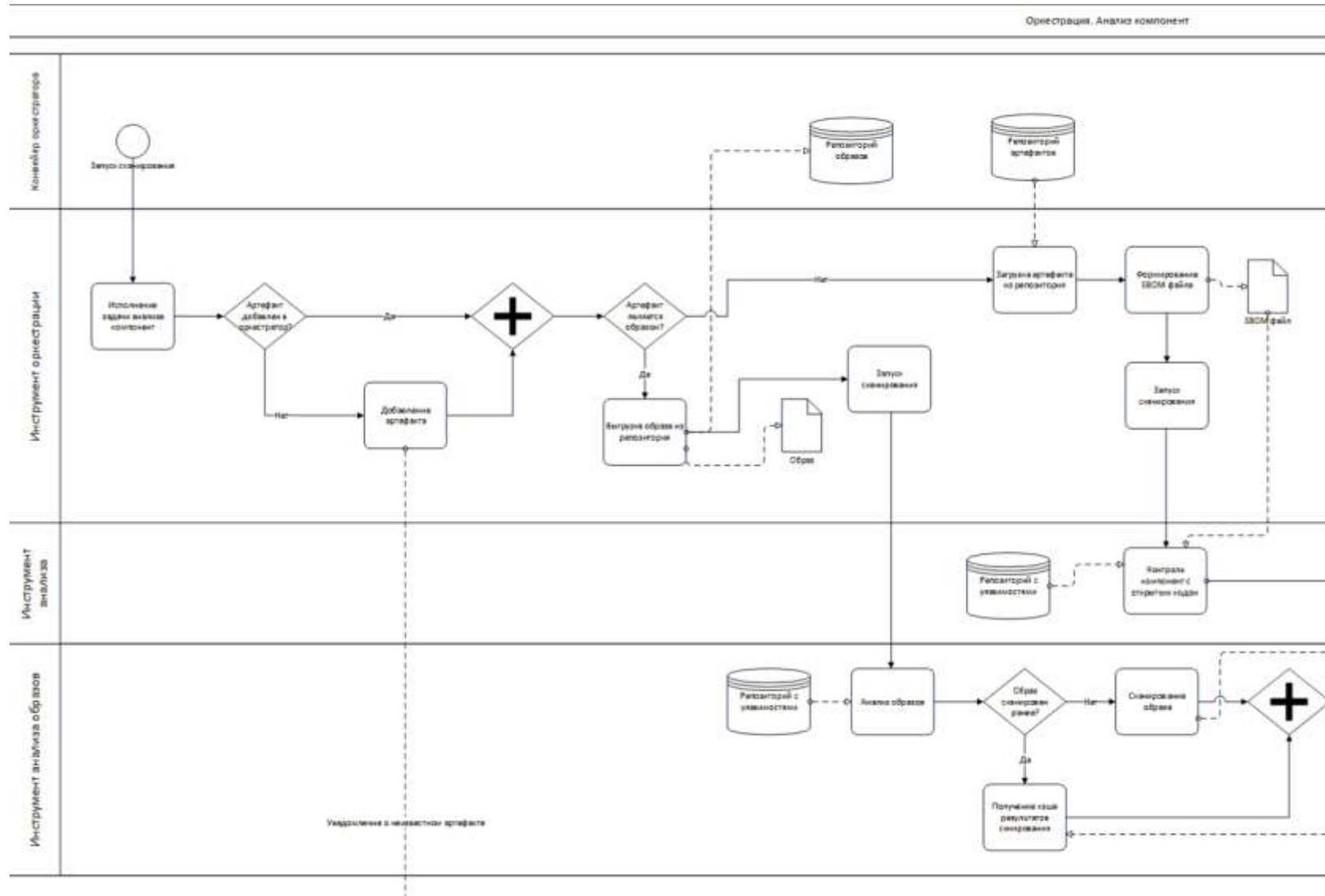
1. Процессы БРПО
2. Описание конвейера БРПО

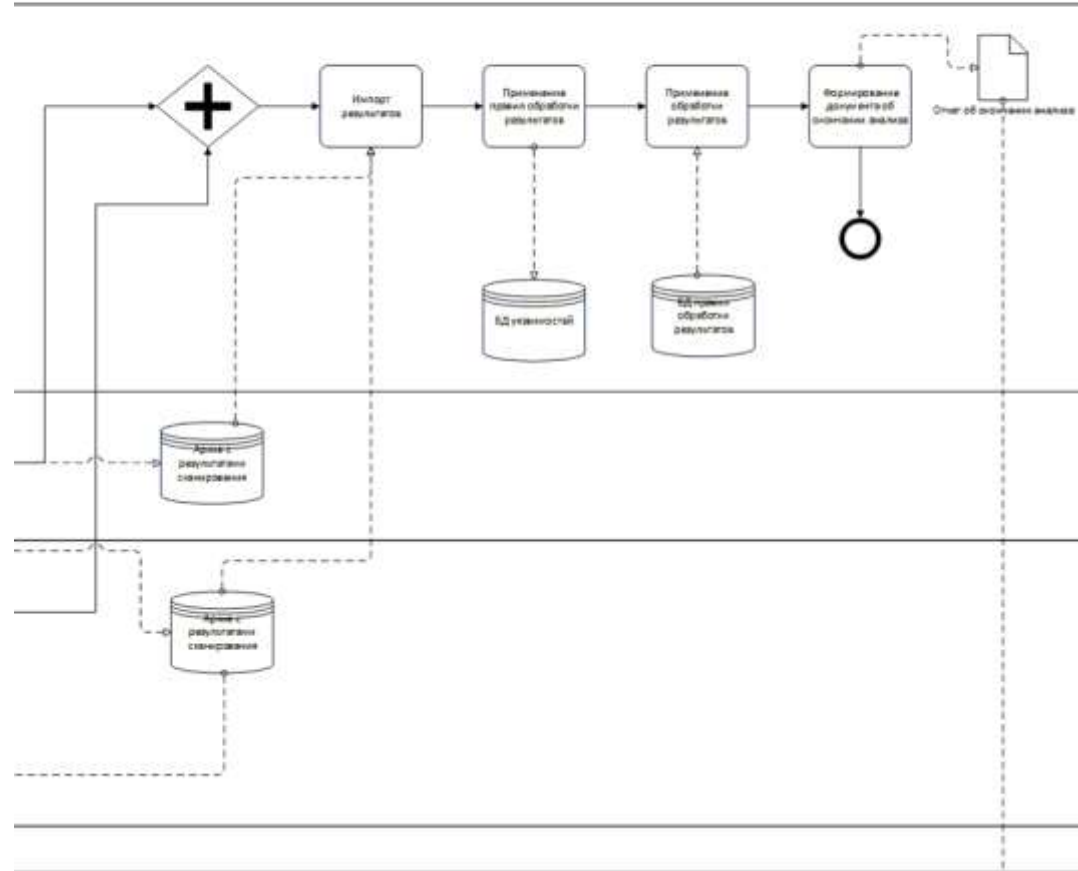


Процессы оркестратора конвейера БРПО



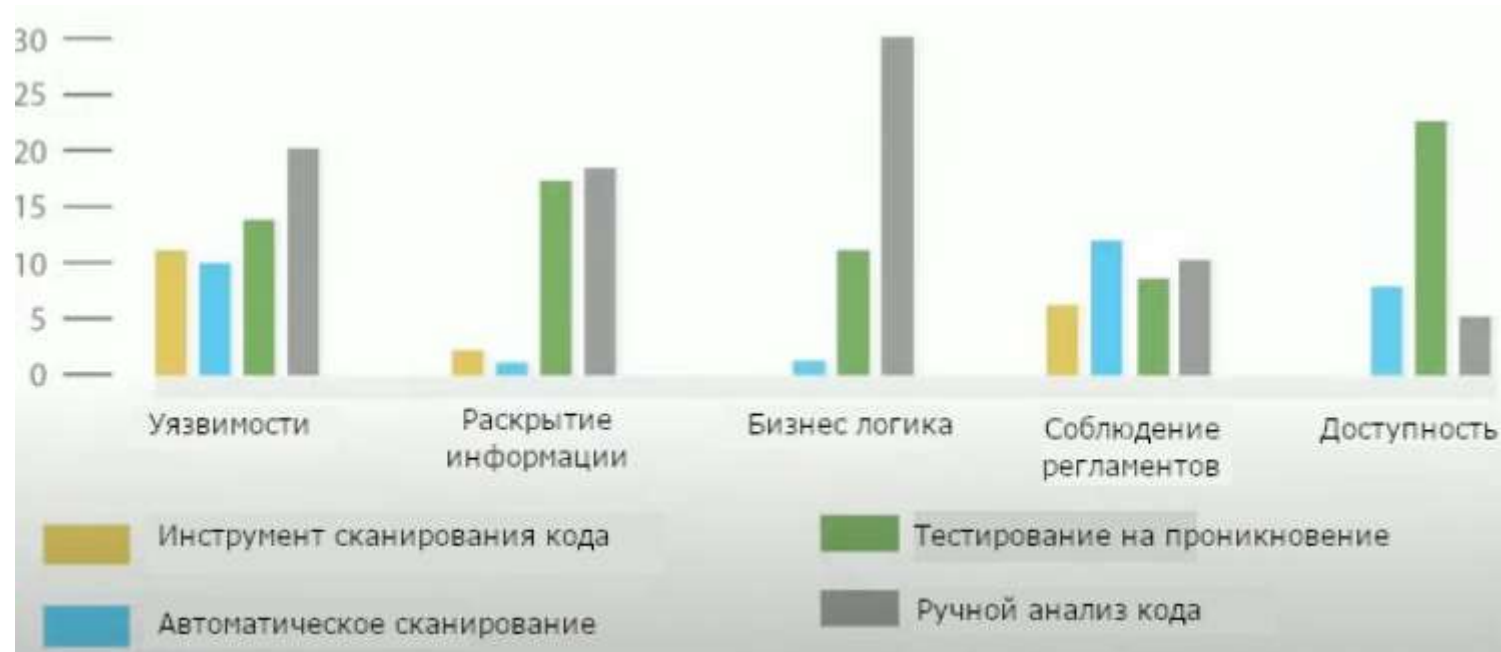


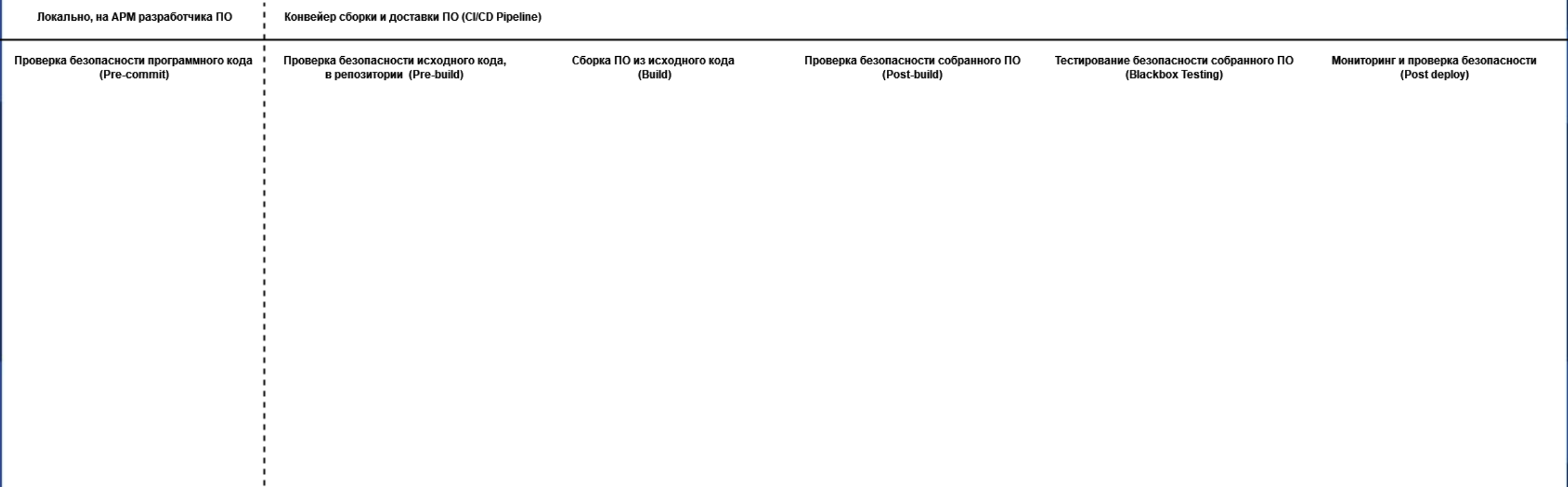






Каким способом находятся уязвимости в исходном коде







Локально, на АРМ разработчика ПО

Конвейер сборки и доставки ПО (CI/CD Pipeline)

Проверка безопасности программного кода
(Pre-commit)

Проверка безопасности исходного кода,
в репозитории (Pre-build)

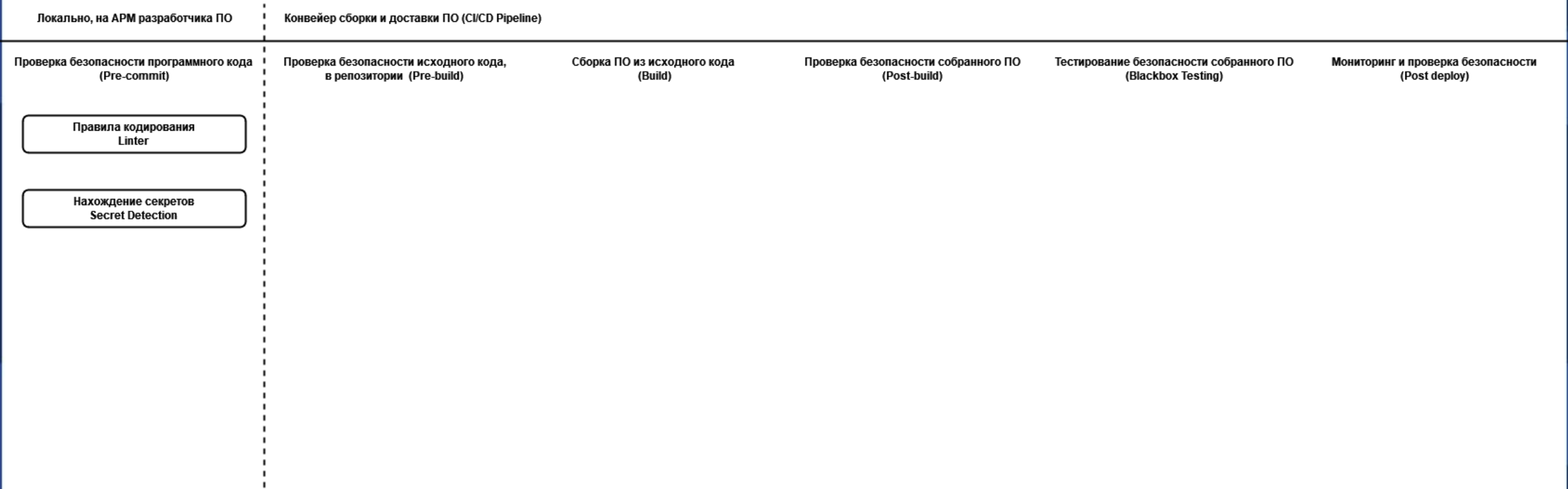
Сборка ПО из исходного кода
(Build)

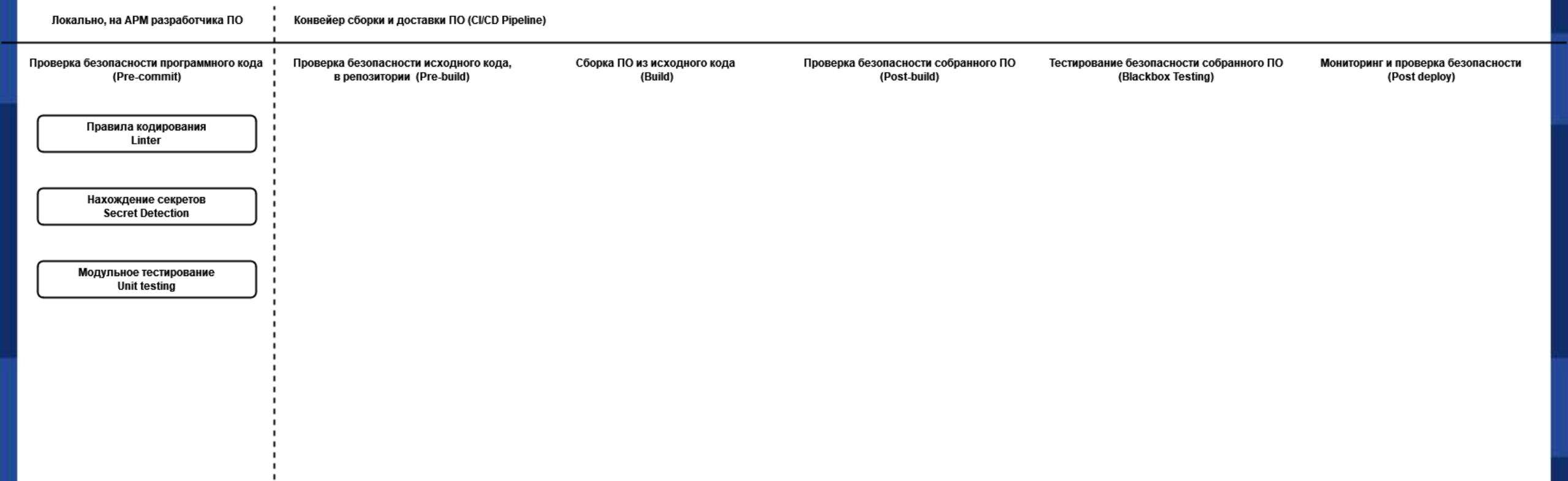
Проверка безопасности собранного ПО
(Post-build)

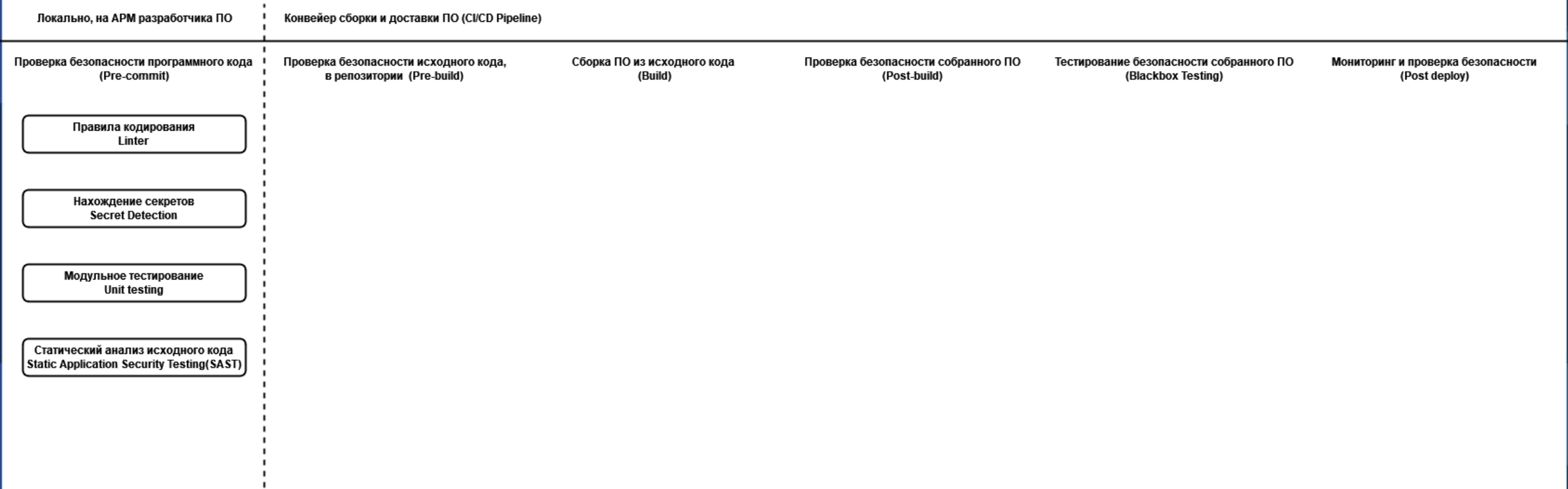
Тестирование безопасности собранного ПО
(Blackbox Testing)

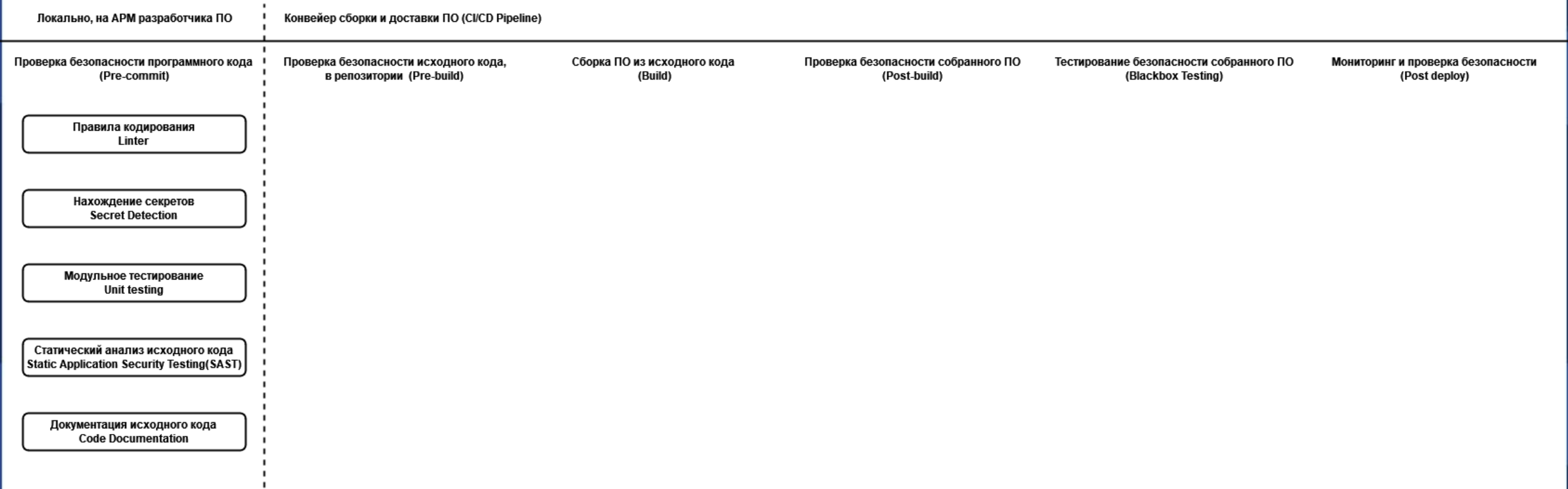
Мониторинг и проверка безопасности
(Post deploy)

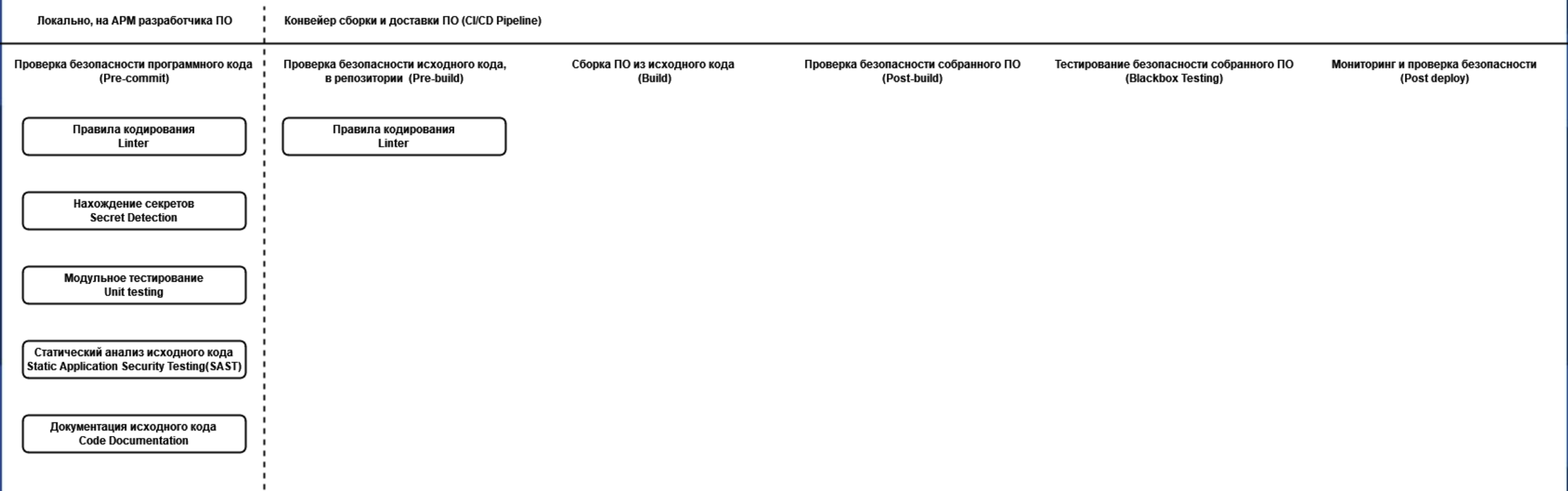
Правила кодирования
Linter

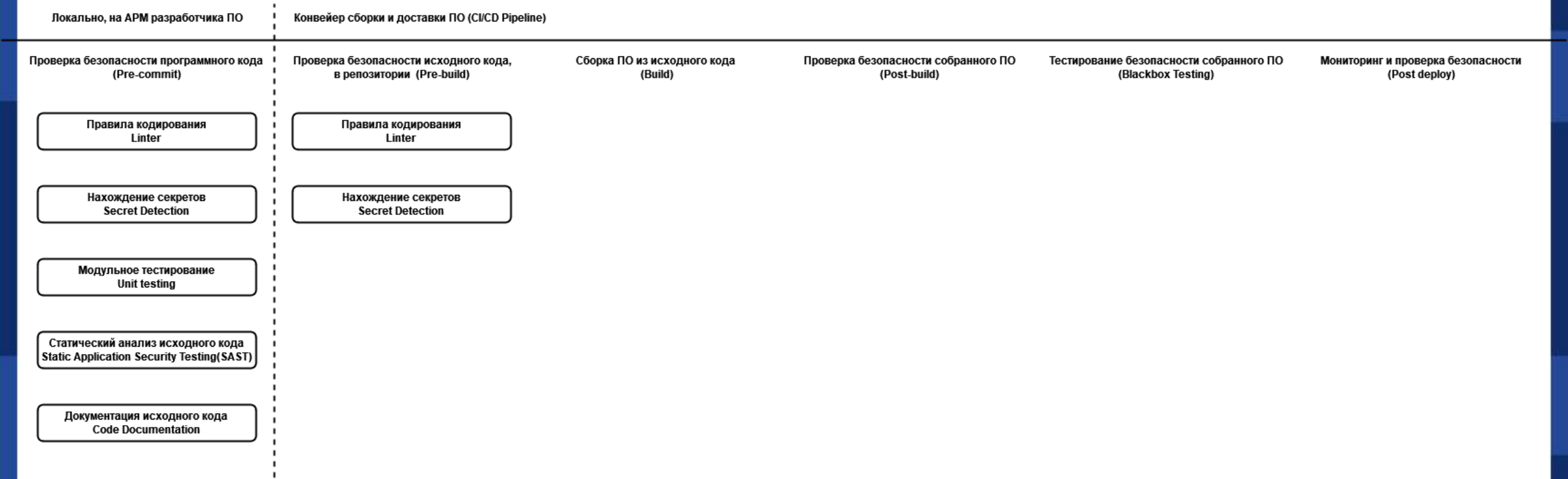


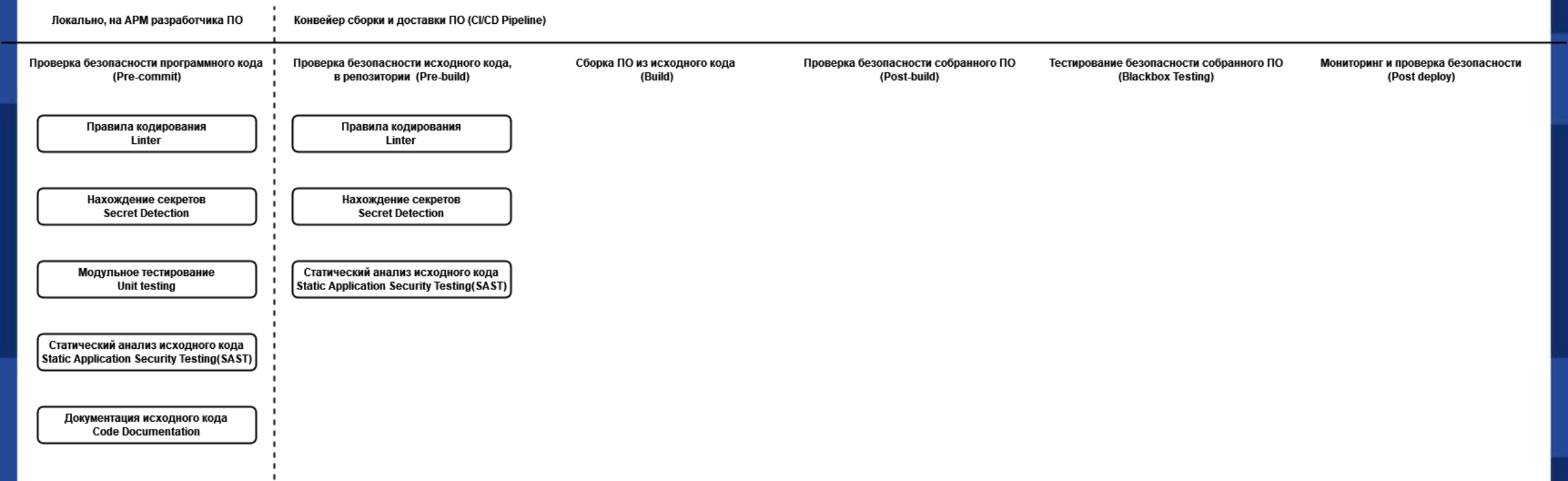


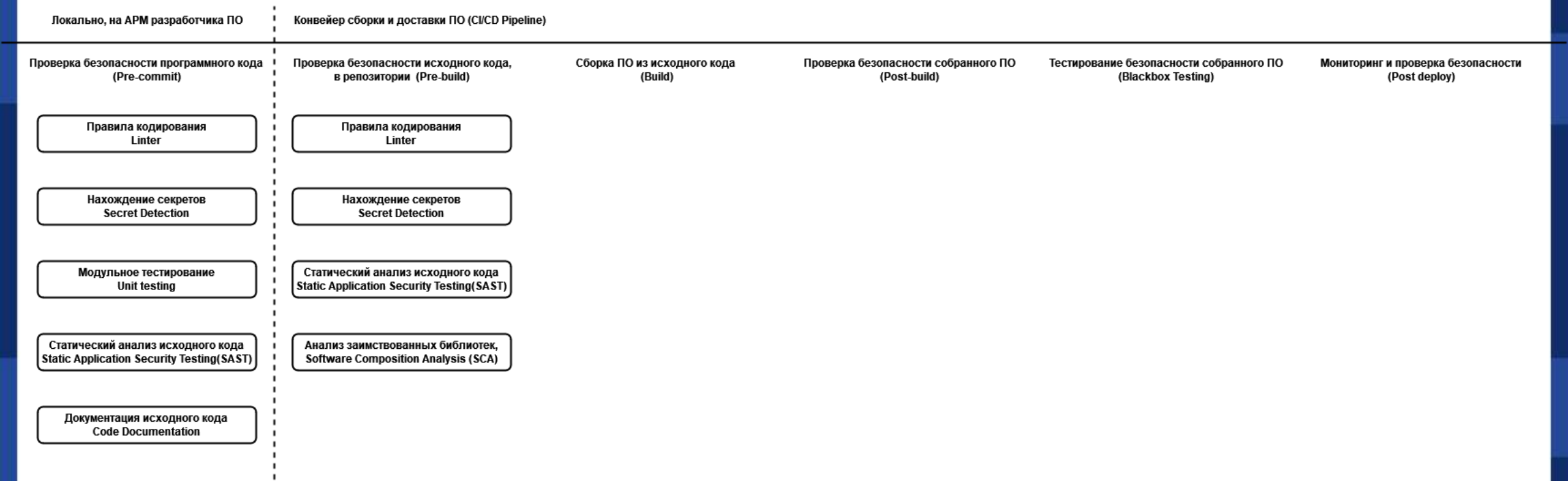


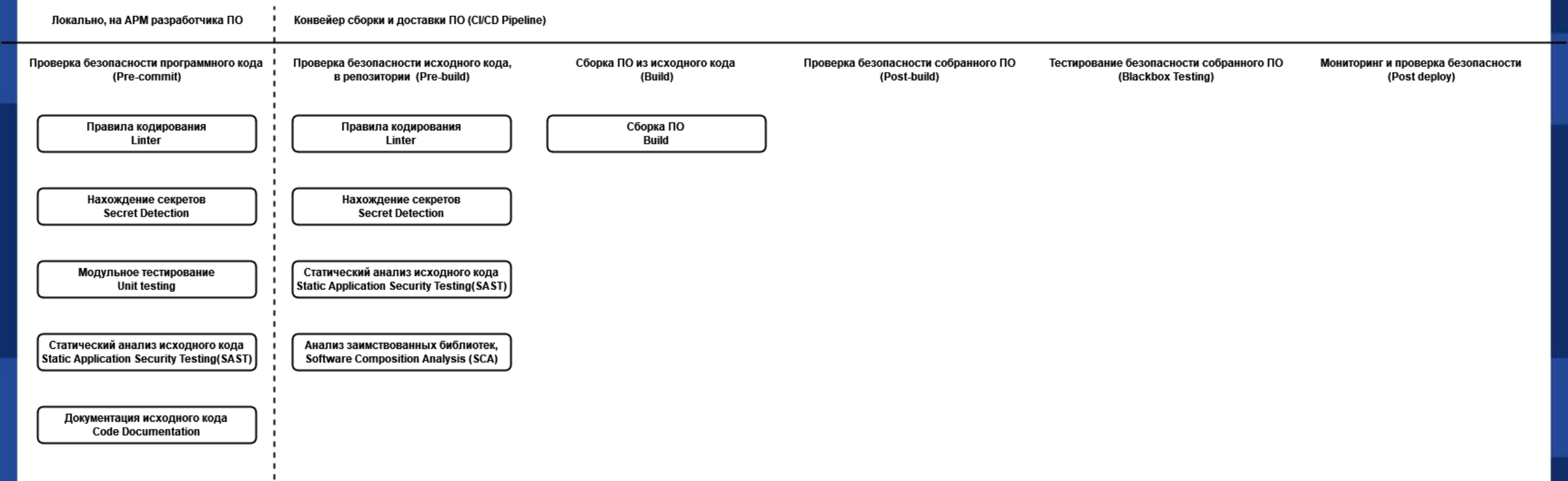














Локально, на АРМ разработчика ПО

Конвейер сборки и доставки ПО (CI/CD Pipeline)

Проверка безопасности программного кода
(Pre-commit)

Правила кодирования
Lint

Нахождение секретов
Secret Detection

Модульное тестирование
Unit testing

Статический анализ исходного кода
Static Application Security Testing(SAST)

Документация исходного кода
Code Documentation

Проверка безопасности исходного кода,
в репозитории (Pre-build)

Правила кодирования
Lint

Нахождение секретов
Secret Detection

Статический анализ исходного кода
Static Application Security Testing(SAST)

Анализ заимствованных библиотек,
Software Composition Analysis (SCA)

Сборка ПО из исходного кода
(Build)

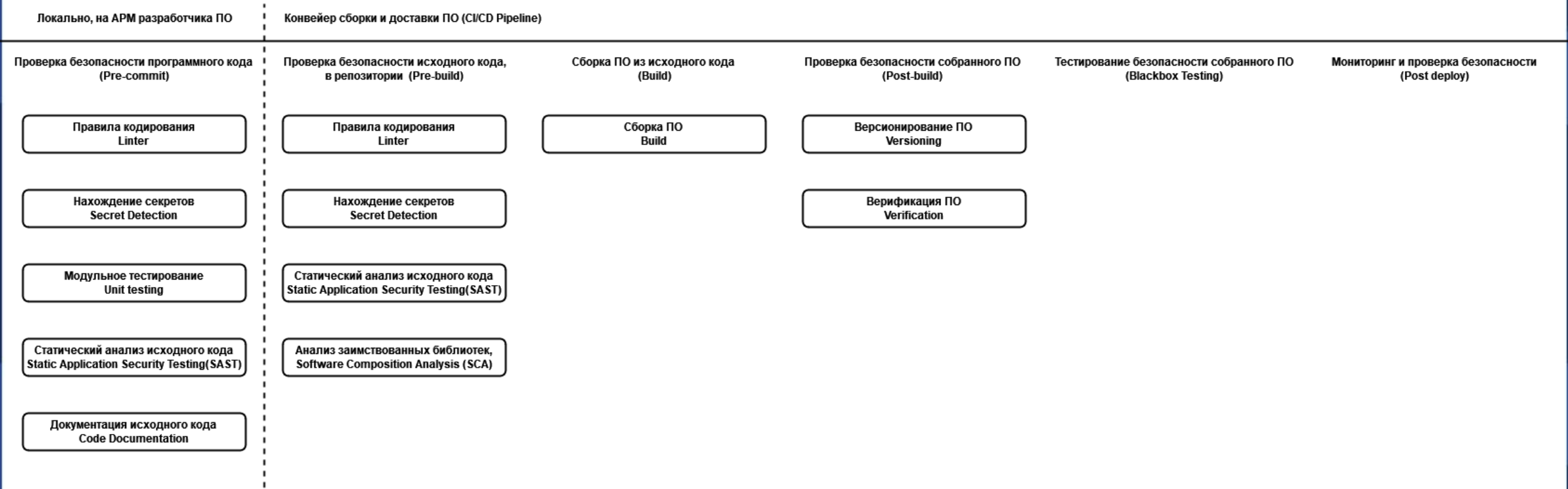
Сборка ПО
Build

Проверка безопасности собранного ПО
(Post-build)

Версионирование ПО
Versioning

Тестирование безопасности собранного ПО
(Blackbox Testing)

Мониторинг и проверка безопасности
(Post deploy)





Локально, на АРМ разработчика ПО

Конвейер сборки и доставки ПО (CI/CD Pipeline)

Проверка безопасности программного кода
(Pre-commit)

Правила кодирования
Linters

Нахождение секретов
Secret Detection

Модульное тестирование
Unit testing

Статический анализ исходного кода
Static Application Security Testing(SAST)

Документация исходного кода
Code Documentation

Проверка безопасности исходного кода,
в репозитории (Pre-build)

Правила кодирования
Linters

Нахождение секретов
Secret Detection

Статический анализ исходного кода
Static Application Security Testing(SAST)

Анализ заимствованных библиотек,
Software Composition Analysis (SCA)

Сборка ПО из исходного кода
(Build)

Сборка ПО
Build

Проверка безопасности собранного ПО
(Post-build)

Версионирование ПО
Versioning

Верификация ПО
Verification

Проверка бинарных артефактов
Binary SCA

Тестирование безопасности собранного ПО
(Blackbox Testing)

Мониторинг и проверка безопасности
(Post deploy)



Локально, на АРМ разработчика ПО

Конвейер сборки и доставки ПО (CI/CD Pipeline)

Проверка безопасности программного кода
(Pre-commit)

Правила кодирования
Lint

Нахождение секретов
Secret Detection

Модульное тестирование
Unit testing

Статический анализ исходного кода
Static Application Security Testing(SAST)

Документация исходного кода
Code Documentation

Проверка безопасности исходного кода,
в репозитории (Pre-build)

Правила кодирования
Lint

Нахождение секретов
Secret Detection

Статический анализ исходного кода
Static Application Security Testing(SAST)

Анализ заимствованных библиотек,
Software Composition Analysis (SCA)

Сборка ПО из исходного кода
(Build)

Сборка ПО
Build

Проверка безопасности собранного ПО
(Post-build)

Версионирование ПО
Versioning

Верификация ПО
Verification

Проверка бинарных артефактов
Binary SCA

Тестирование безопасности собранного ПО
(Blackbox Testing)

Динамический анализ ПО
Dynamic Application Security Testing

Мониторинг и проверка безопасности
(Post deploy)



Локально, на АРМ разработчика ПО

Конвейер сборки и доставки ПО (CI/CD Pipeline)

Проверка безопасности программного кода
(Pre-commit)

Правила кодирования
Lint

Нахождение секретов
Secret Detection

Модульное тестирование
Unit testing

Статический анализ исходного кода
Static Application Security Testing(SAST)

Документация исходного кода
Code Documentation

Проверка безопасности исходного кода,
в репозитории (Pre-build)

Правила кодирования
Lint

Нахождение секретов
Secret Detection

Статический анализ исходного кода
Static Application Security Testing(SAST)

Анализ заимствованных библиотек,
Software Composition Analysis (SCA)

Сборка ПО из исходного кода
(Build)

Сборка ПО
Build

Проверка безопасности собранного ПО
(Post-build)

Версионирование ПО
Versioning

Верификация ПО
Verification

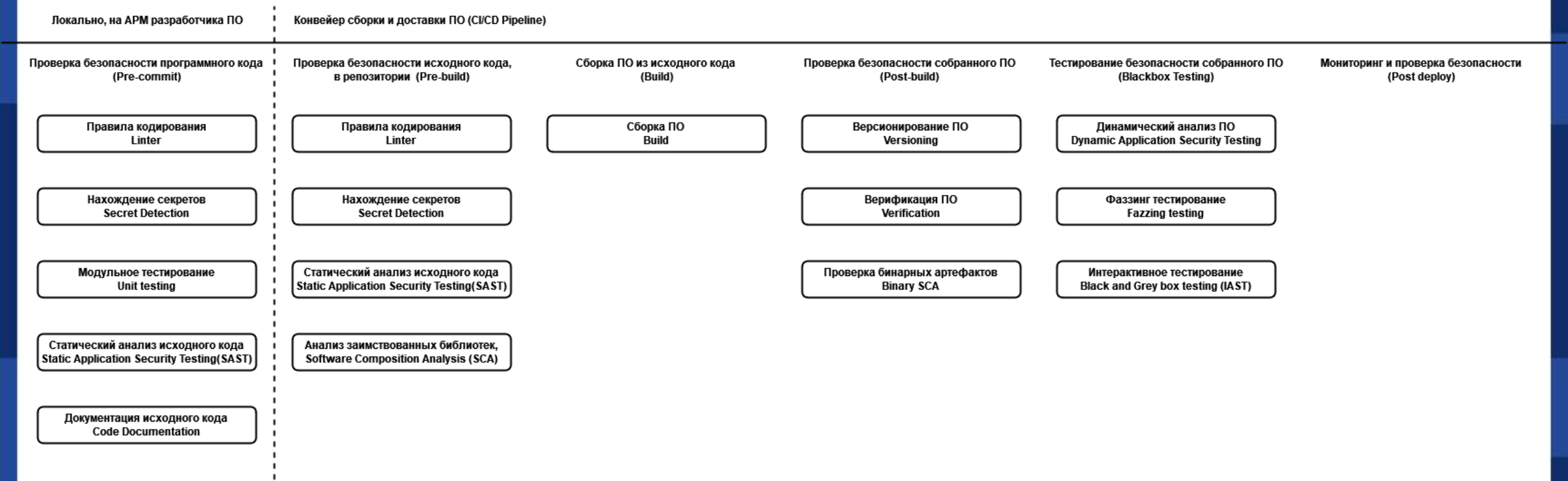
Проверка бинарных артефактов
Binary SCA

Тестирование безопасности собранного ПО
(Blackbox Testing)

Динамический анализ ПО
Dynamic Application Security Testing

Фаззинг тестирование
Fuzzing testing

Мониторинг и проверка безопасности
(Post deploy)





Локально, на АРМ разработчика ПО

Конвейер сборки и доставки ПО (CI/CD Pipeline)

Проверка безопасности программного кода
(Pre-commit)

Правила кодирования
Linters

Нахождение секретов
Secret Detection

Модульное тестирование
Unit testing

Статический анализ исходного кода
Static Application Security Testing (SAST)

Документация исходного кода
Code Documentation

Проверка безопасности исходного кода,
в репозитории (Pre-build)

Правила кодирования
Linters

Нахождение секретов
Secret Detection

Статический анализ исходного кода
Static Application Security Testing (SAST)

Анализ заимствованных библиотек,
Software Composition Analysis (SCA)

Сборка ПО из исходного кода
(Build)

Сборка ПО
Build

Проверка безопасности собранного ПО
(Post-build)

Версионирование ПО
Versioning

Верификация ПО
Verification

Проверка бинарных артефактов
Binary SCA

Тестирование безопасности собранного ПО
(Blackbox Testing)

Динамический анализ ПО
Dynamic Application Security Testing

Фаззинг тестирование
Fuzzing testing

Интерактивное тестирование
Black and Grey box testing (IAST)

Интерактивное тестирование
Black and Grey box testing (IAST)

Мониторинг и проверка безопасности
(Post deploy)



Локально, на АРМ разработчика ПО

Конвейер сборки и доставки ПО (CI/CD Pipeline)

Проверка безопасности программного кода
(Pre-commit)

Правила кодирования
Lint

Нахождение секретов
Secret Detection

Модульное тестирование
Unit testing

Статический анализ исходного кода
Static Application Security Testing(SAST)

Документация исходного кода
Code Documentation

Проверка безопасности исходного кода,
в репозитории (Pre-build)

Правила кодирования
Lint

Нахождение секретов
Secret Detection

Статический анализ исходного кода
Static Application Security Testing(SAST)

Анализ заимствованных библиотек,
Software Composition Analysis (SCA)

Сборка ПО из исходного кода
(Build)

Сборка ПО
Build

Проверка безопасности собранного ПО
(Post-build)

Версионирование ПО
Versioning

Верификация ПО
Verification

Проверка бинарных артефактов
Binary SCA

Тестирование безопасности собранного ПО
(Blackbox Testing)

Динамический анализ ПО
Dynamic Application Security Testing

Фаззинг тестирование
Fuzzing testing

Интерактивное тестирование
Black and Grey box testing (IAST)

Интерактивное тестирование
Black and Grey box testing (IAST)

Анализ сетевого трафика
Out-of-band Application Security (OAST)

Мониторинг и проверка безопасности
(Post deploy)



Локально, на АРМ разработчика ПО

Конвейер сборки и доставки ПО (CI/CD Pipeline)

Проверка безопасности программного кода
(Pre-commit)

Правила кодирования
Lint

Нахождение секретов
Secret Detection

Модульное тестирование
Unit testing

Статический анализ исходного кода
Static Application Security Testing(SAST)

Документация исходного кода
Code Documentation

Проверка безопасности исходного кода,
в репозитории (Pre-build)

Правила кодирования
Lint

Нахождение секретов
Secret Detection

Статический анализ исходного кода
Static Application Security Testing(SAST)

Анализ заимствованных библиотек,
Software Composition Analysis (SCA)

Сборка ПО из исходного кода
(Build)

Сборка ПО
Build

Проверка безопасности собранного ПО
(Post-build)

Версионирование ПО
Versioning

Верификация ПО
Verification

Проверка бинарных артефактов
Binary SCA

Тестирование безопасности собранного ПО
(Blackbox Testing)

Динамический анализ ПО
Dynamic Application Security Testing

Фаззинг тестирование
Fuzzing testing

Интерактивное тестирование
Black and Grey box testing (IAST)

Интерактивное тестирование
Black and Grey box testing (IAST)

Анализ сетевого трафика
Out-of-band Application Security (OAST)

Мониторинг и проверка безопасности
(Post deploy)

Межсетевой экран L3
Anti DDoS



Локально, на АРМ разработчика ПО

Конвейер сборки и доставки ПО (CI/CD Pipeline)

Проверка безопасности программного кода
(Pre-commit)

Правила кодирования
Linters

Нахождение секретов
Secret Detection

Модульное тестирование
Unit testing

Статический анализ исходного кода
Static Application Security Testing (SAST)

Документация исходного кода
Code Documentation

Проверка безопасности исходного кода,
в репозитории (Pre-build)

Правила кодирования
Linters

Нахождение секретов
Secret Detection

Статический анализ исходного кода
Static Application Security Testing (SAST)

Анализ заимствованных библиотек,
Software Composition Analysis (SCA)

Сборка ПО из исходного кода
(Build)

Сборка ПО
Build

Проверка безопасности собранного ПО
(Post-build)

Версионирование ПО
Versioning

Верификация ПО
Verification

Проверка бинарных артефактов
Binary SCA

Тестирование безопасности собранного ПО
(Blackbox Testing)

Динамический анализ ПО
Dynamic Application Security Testing

Фаззинг тестирование
Fuzzing testing

Интерактивное тестирование
Black and Grey box testing (IAST)

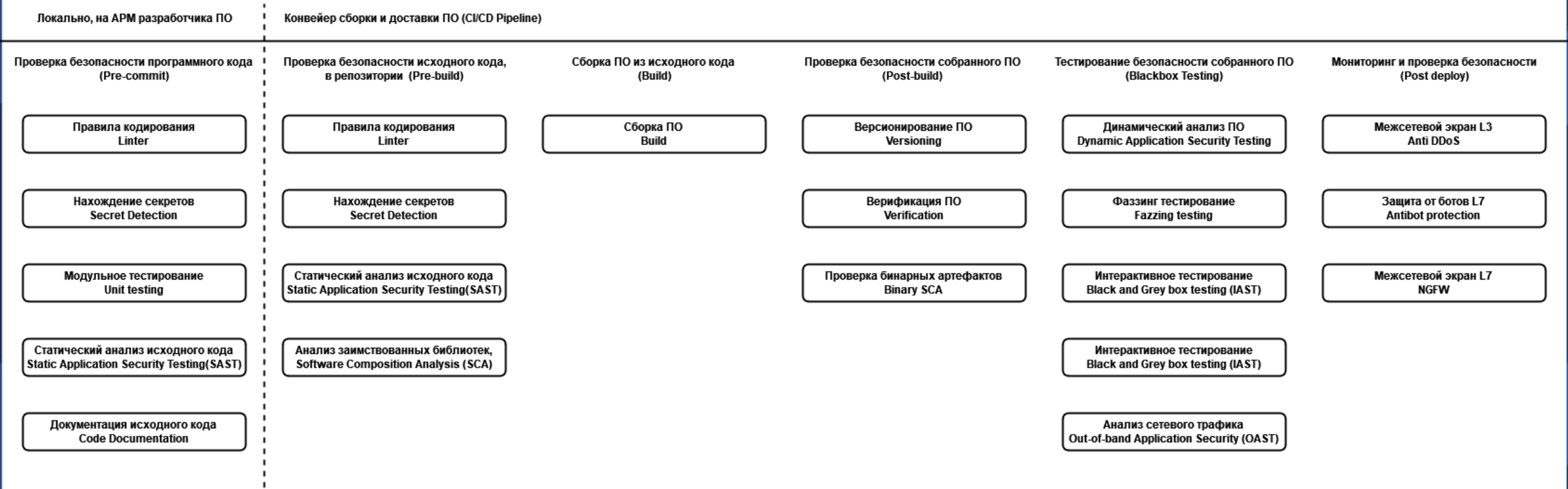
Интерактивное тестирование
Black and Grey box testing (IAST)

Анализ сетевого трафика
Out-of-band Application Security (OAST)

Мониторинг и проверка безопасности
(Post deploy)

Межсетевой экран L3
Anti DDoS

Защита от ботов L7
Antibot protection





Локально, на АРМ разработчика ПО

Конвейер сборки и доставки ПО (CI/CD Pipeline)

Проверка безопасности программного кода
(Pre-commit)

Правила кодирования
Linter

Нахождение секретов
Secret Detection

Модульное тестирование
Unit testing

Статический анализ исходного кода
Static Application Security Testing(SAST)

Документация исходного кода
Code Documentation

Проверка безопасности исходного кода,
в репозитории (Pre-build)

Правила кодирования
Linter

Нахождение секретов
Secret Detection

Статический анализ исходного кода
Static Application Security Testing(SAST)

Анализ заимствованных библиотек,
Software Composition Analysis (SCA)

Сборка ПО из исходного кода
(Build)

Сборка ПО
Build

Проверка безопасности собранного ПО
(Post-build)

Версионирование ПО
Versioning

Верификация ПО
Verification

Проверка бинарных артефактов
Binary SCA

Тестирование безопасности собранного ПО
(Blackbox Testing)

Динамический анализ ПО
Dynamic Application Security Testing

Фаззинг тестирование
Fuzzing testing

Интерактивное тестирование
Black and Grey box testing (IAST)

Интерактивное тестирование
Black and Grey box testing (IAST)

Анализ сетевого трафика
Out-of-band Application Security (OAST)

Мониторинг и проверка безопасности
(Post deploy)

Межсетевой экран L3
Anti DDoS

Защита от ботов L7
Antibot protection

Межсетевой экран L7
NGFW

Ограничение использования ПО
Throttling, Limit req



Локально, на АРМ разработчика ПО

Конвейер сборки и доставки ПО (CI/CD Pipeline)

Проверка безопасности программного кода
(Pre-commit)

Правила кодирования
Linters

Нахождение секретов
Secret Detection

Модульное тестирование
Unit testing

Статический анализ исходного кода
Static Application Security Testing(SAST)

Документация исходного кода
Code Documentation

Проверка безопасности исходного кода,
в репозитории (Pre-build)

Правила кодирования
Linters

Нахождение секретов
Secret Detection

Статический анализ исходного кода
Static Application Security Testing(SAST)

Анализ заимствованных библиотек,
Software Composition Analysis (SCA)

Сборка ПО из исходного кода
(Build)

Сборка ПО
Build

Проверка безопасности собранного ПО
(Post-build)

Версионирование ПО
Versioning

Верификация ПО
Verification

Проверка бинарных артефактов
Binary SCA

Тестирование безопасности собранного ПО
(Blackbox Testing)

Динамический анализ ПО
Dynamic Application Security Testing

Фаззинг тестирование
Fuzzing testing

Интерактивное тестирование
Black and Grey box testing (IAST)

Интерактивное тестирование
Black and Grey box testing (IAST)

Анализ сетевого трафика
Out-of-band Application Security (OAST)

Мониторинг и проверка безопасности
(Post deploy)

Межсетевой экран L3
Anti DDoS

Защита от ботов L7
Antibot protection

Межсетевой экран L7
NGFW

Ограничение использования ПО
Throttling, Limit req

Защита в среде исполнения ПО
RASP



Локально, на АРМ разработчика ПО

Конвейер сборки и доставки ПО (CI/CD Pipeline)

Проверка безопасности программного кода
(Pre-commit)

Правила кодирования
Linters

Нахождение секретов
Secret Detection

Модульное тестирование
Unit testing

Статический анализ исходного кода
Static Application Security Testing(SAST)

Документация исходного кода
Code Documentation

Проверка безопасности исходного кода,
в репозитории (Pre-build)

Правила кодирования
Linters

Нахождение секретов
Secret Detection

Статический анализ исходного кода
Static Application Security Testing(SAST)

Анализ заимствованных библиотек,
Software Composition Analysis (SCA)

Сборка ПО из исходного кода
(Build)

Сборка ПО
Build

Проверка безопасности собранного ПО
(Post-build)

Версионирование ПО
Versioning

Верификация ПО
Verification

Проверка бинарных артефактов
Binary SCA

Тестирование безопасности собранного ПО
(Blackbox Testing)

Динамический анализ ПО
Dynamic Application Security Testing

Фаззинг тестирование
Fuzzing testing

Интерактивное тестирование
Black and Grey box testing (IAST)

Интерактивное тестирование
Black and Grey box testing (IAST)

Анализ сетевого трафика
Out-of-band Application Security (OAST)

Мониторинг и проверка безопасности
(Post deploy)

Межсетевой экран L3
Anti DDoS

Защита от ботов L7
Antibot protection

Межсетевой экран L7
NGFW

Ограничение использования ПО
Throttling, Limit req

Защита в среде исполнения ПО
RASP

Механизмы защиты пользователей
Auth security, Revocation mechanism



Задание 2

Создать репозиторий в
GitLab с проектом из
<https://github.com/snoopysecurity/Vulnerable-Code-Snippets>

Провести анализ работы
инструментов сканирования

* Создать репозиторий с проектом Owasp Juice Shop.
Самостоятельно внедрить инструменты конвейера
БРПО в CI/CD Gitlab.

(количество выявленных инструментами уязвимостей
сохранять в Prometheus или DefectDojo)

