

Искусственный автор – привычный контроль

Как контролировать AI-агентов?



Валерий Филатов
Developer Advocate, PVS-Studio



О СПИКЕРЕ

Занимаюсь разработкой и поддержкой интеграций продукта — от IDE до CI/CD.

Регулярно выступаю на конференциях, митапах и вебинарах. Пишу статьи, документацию и другие технические тексты.

Выпустил несколько групп начинающих Python-разработчиков.

Веду авторский Telegram-канал о разработке и технологиях.

Валерий Филатов

Developer Advocate и Project Lead, PVS-Studio

[@feelindex](#) · filatov@pvs-studio.ru

01 Вы находитесь здесь

Defining breakthroughs in AI

AlphaGo

Transformers

word2vec

WaveNet

AlphaFold

Sequence to sequence models

Distillation

Deep reinforcement learning



Картинка со звуком

“

А что делать-то?

Павел Петров

Собирательный образ слушателя доклада

Абстрактный пайплайн

01 **Pre-commit** – линтеры, форматтеры, быстрые unit-тесты

Абстрактный пайплайн

01 **Pre-commit** – линтеры, форматтеры, быстрые unit-тесты

02 **Статический анализ** – автоматизированная проверка исходного кода

Абстрактный пайплайн

- 01 **Pre-commit** – линтеры, форматтеры, быстрые unit-тесты
- 02 **Статический анализ** – автоматизированная проверка исходного кода
- 03 **Code Review** – просмотр диффов, чеклисты

Абстрактный пайплайн

- 01 **Pre-commit** – линтеры, форматтеры, быстрые unit-тесты
- 02 **Статический анализ** – автоматизированная проверка исходного кода
- 03 **Code Review** – просмотр диффов, чеклисты
- 04 **Тестирование** – unit/integration/e2e, coverage

Абстрактный пайплайн

- 01 **Pre-commit** – линтеры, форматтеры, быстрые unit-тесты
- 02 **Статический анализ** – автоматизированная проверка исходного кода
- 03 **Code Review** – просмотр диффов, чеклисты
- 04 **Тестирование** – unit/integration/e2e, coverage
- 05 CI/CD Gates** – условия для мержа/деплойа

Абстрактный пайплайн

- 01 **Pre-commit** – линтеры, форматтеры, быстрые unit-тесты
- 02 **Статический анализ** – автоматизированная проверка исходного кода
- 03 **Code Review** – просмотр диффов, чеклисты
- 04 **Тестирование** – unit/integration/e2e, coverage
- 05 **CI/CD Gates** – условия для мержа/деплойа
- 06 **Incident Response** – откат, post-mortem

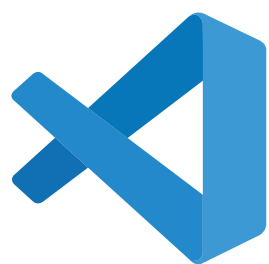
Абстрактный пайплайн

- 01 **Pre-commit** – линтеры, форматтеры, быстрые unit-тесты
- 02 **Статический анализ** – автоматизированная проверка исходного кода
- 03 **Code Review** – просмотр диффов, чеклисты
- 04 **Тестирование** – unit/integration/e2e, coverage
- 05 **CI/CD Gates** – условия для мержа/деплойа
- 06 **Incident Response** – откат, post-mortem

02 SAST и AI

Локальный анализ

- Проверяем код во время разработки из IDE или через CLI



Локальный анализ

- Проверяем код во время разработки из IDE или через CLI
- Используем инкрементальный анализ для ускорения

Локальный анализ

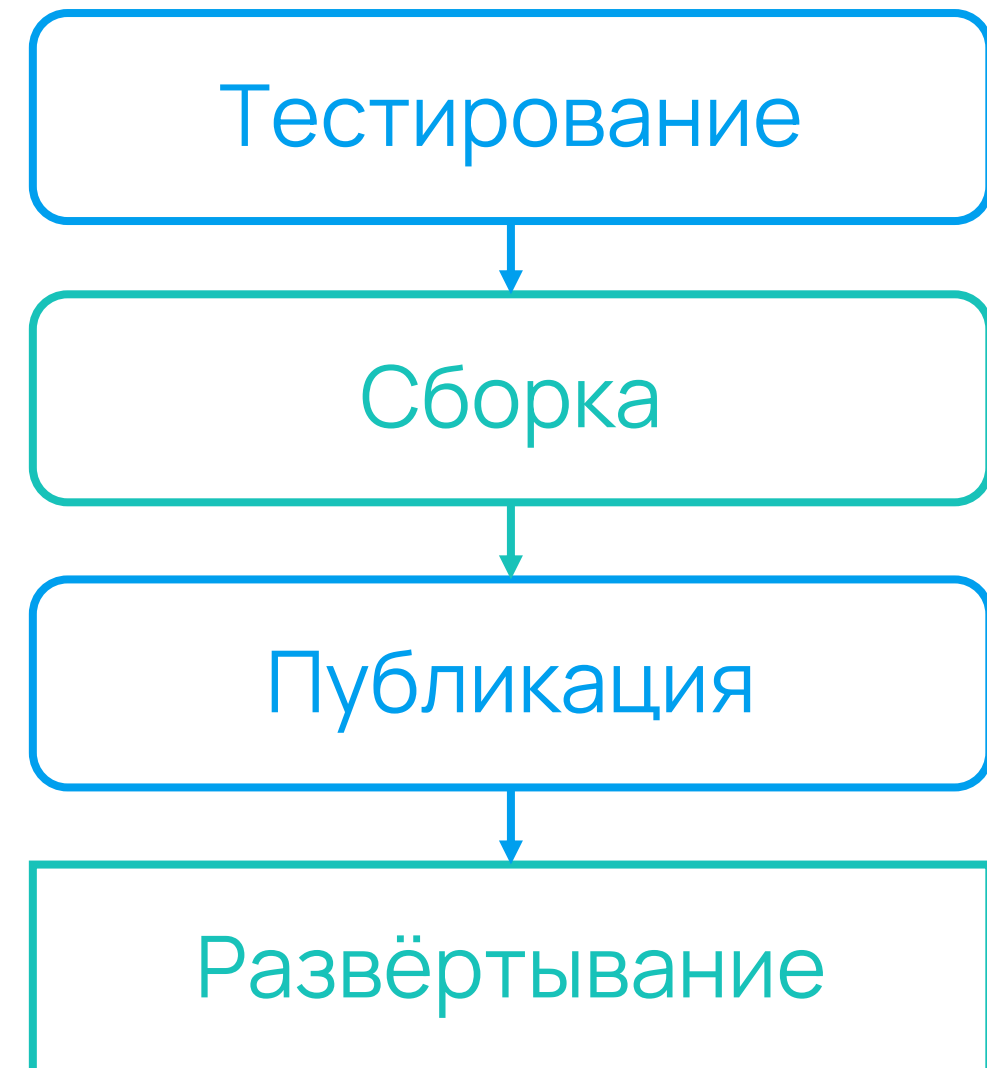
- Проверяем код во время разработки из IDE или через CLI
- Используем инкрементальный анализ для ускорения
- Предварительно настраиваем анализатор

Непрерывный анализ

- Проверяем каждое изменение

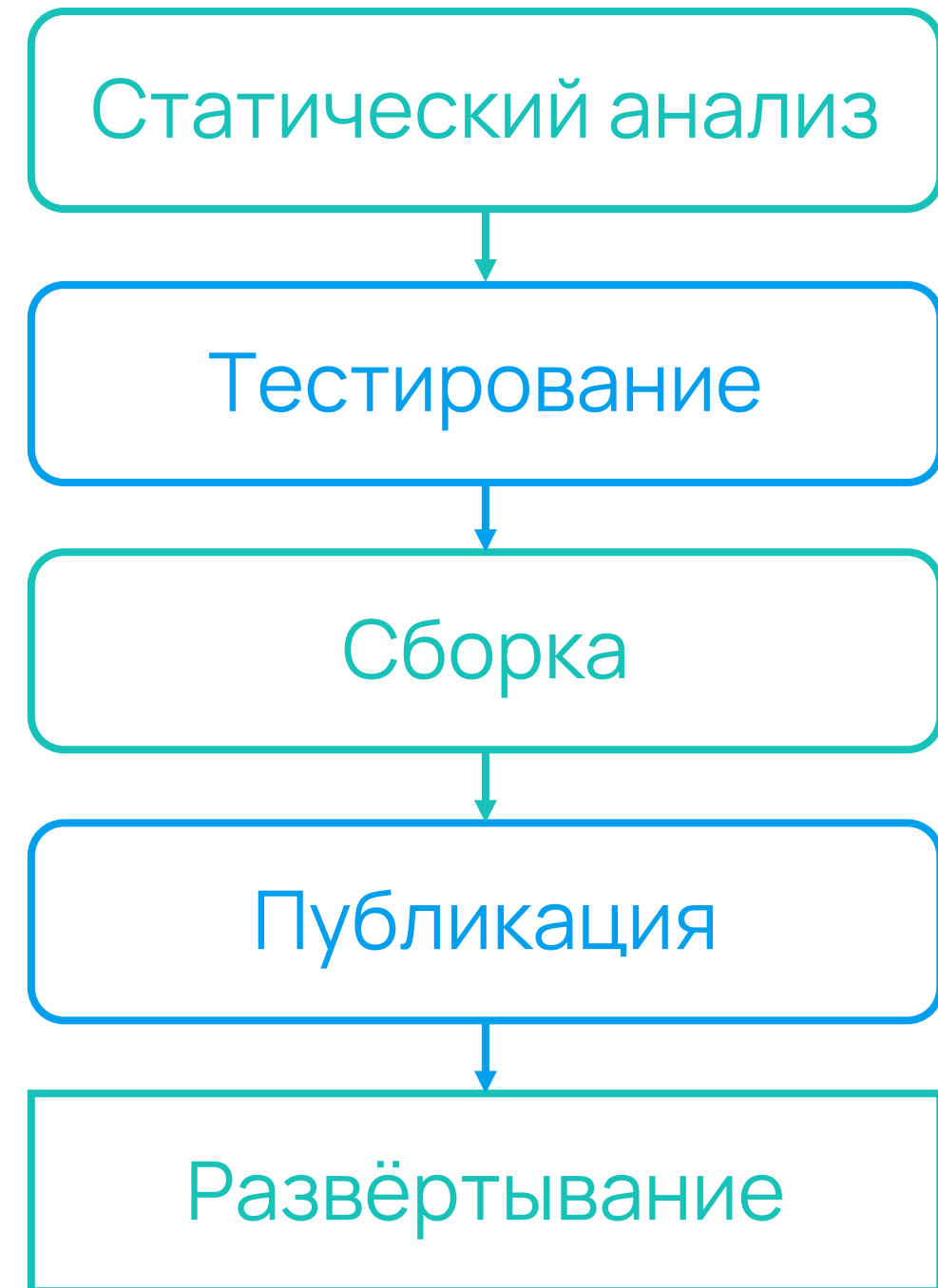
Непрерывный анализ

- Проверяем каждое изменение



Непрерывный анализ

- Проверяем каждое изменение



Непрерывный анализ

- Проверяем каждое изменение

Коммит/PR



Статический анализ



Тестирование



Сборка



Публикация



Развёртывание

Непрерывный анализ

- Проверяем каждое изменение
- Разворачиваем разработчика, если нашлись срабатывания

Регулярный анализ

- Проверяем весь проект целиком в ночных сборках

Регулярный анализ

- Проверяем весь проект целиком в ночных сборках
- Агрегируем результаты в веб-дашборд

[My Issues](#) [All](#)

Filters

Issues in new code

▼ Software Quality ?

Security	1
Reliability	287
Maintainability	150

▼ Severity ?

Blocker	0
High	162
Medium	221
Low	53
Info	2

▼ Clean Code Attribute ?

Consistency	60
Intentionality	330
Adaptability	47
Responsibility	1

☐ Bulk Change

Select issues ▲ ▼ Navigate to issue ◀ ▶ **438** issues **2d 5h** effort

Source/CPack/cmCPackGenerator.cxx

☐ [\[CWE-457\] V730: Not all members of a class are initialized inside the constructor. Consider inspecting: Trace, TraceExpand.](#) Intentionality

Reliability High ▼

cwe cwe-457 ... +

☐ Open ▼

Not assigned ▼

L41 • 18 years ago

Source/CPack/cmCPackLog.cxx

☐ [\[CWE-570\] V547: Expression '!tagString.empty\(\)' is always false.](#) Intentionality

Reliability Medium ▼

cwe pvs-studio ... +

☐ Open ▼

Not assigned ▼

L67 • 10 years ago

☐ [\[CWE-20\] V781: The value of the 'length' index is checked after it was used. Perhaps there is a mistake in program logic.](#) Intentionality

Reliability High ▼

cwe sec ... +

☐ Open ▼

Not assigned ▼

L157 • 10 years ago

Source/CPack/cmCPackNSISGenerator.cxx

☐ [\[CWE-571\] V547: Expression '!gotRegValue' is always true.](#) Intentionality

Reliability Medium ▼

cwe pvs-studio ... +

☐ Open ▼

Not assigned ▼

L480 • 10 years ago

Интерфейс SonarQube

Меняет ли AI что-то в этом пайплайне?

Меняет ли AI что-то в этом пайплайне?

Не-а :)

Что поменялось?

До AI

Разработчик проверяет свой код

Правки **разработчика** проверяются в CI перед слиянием

Вместе с AI

Агент запускает анализ как этап верификации

Правки **агента** проверяются в CI перед слиянием

Но агенту нужна помощь, чтобы разобраться



AGENTS.md



CLAUDE.md

РЕПОЗИТОРИЙ

pvs-js-skill

Скилл для запуска анализатора PVS-Studio
на JavaScript и TypeScript коде



03 Улучшайзинг

Агентский пайплайн

01 **Pre-commit** – линтеры, форматтеры, быстрые unit-тесты

Агентский пайплайн

01 **Pre-commit** – агент становится автором коммита, локальные AI-линтеры

Агентский пайплайн

- 01 **Pre-commit** – агент становится автором коммита, локальные AI-линтеры
- 02 **Статический анализ** – автоматизированная проверка исходного кода

Агентский пайплайн

- 01 **Pre-commit** – агент становится автором коммита, локальные AI-линтеры
- 02 **Статический анализ** – AI проверяет свой код

Агентский пайплайн

- 01 **Pre-commit** – агент становится автором коммита, локальные AI-линтеры
- 02 **Статический анализ** – AI проверяет свой код
- 03 **Code Review** – просмотр диффов, чеклисты

Агентский пайплайн

- 01 **Pre-commit** – агент становится автором коммита, локальные AI-линтеры
- 02 **Статический анализ** – AI проверяет свой код
- 03 **Code Review** – добавляется агент-ревьюер

Агентский пайплайн

- 01 **Pre-commit** – агент становится автором коммита, локальные AI-линтеры
- 02 **Статический анализ** – AI проверяет свой код
- 03 **Code Review** – добавляется агент-ревьюер
- 04 **Тестирование** – unit/integration/e2e, coverage

Агентский пайплайн

- 01 **Pre-commit** – агент становится автором коммита, локальные AI-линтеры
- 02 **Статический анализ** – AI проверяет свой код
- 03 **Code Review** – добавляется агент-ревьюер
- 04 **Тестирование** – агент генерирует тесты

Агентский пайплайн

- 01 **Pre-commit** – агент становится автором коммита, локальные AI-линтеры
- 02 **Статический анализ** – AI проверяет свой код
- 03 **Code Review** – добавляется агент-ревьюер
- 04 **Тестирование** – агент генерирует тесты
- 05 **CI/CD Gates** – условия для мержа/деплойа

Агентский пайплайн

- 01 **Pre-commit** – агент становится автором коммита, локальные AI-линтеры
- 02 **Статический анализ** – AI проверяет свой код
- 03 **Code Review** – добавляется агент-ревьюер
- 04 **Тестирование** – агент генерирует тесты
- 05 **CI/CD Gates** – агент самостоятельно чинит падения

Агентский пайплайн

- 01 **Pre-commit** – агент становится автором коммита, локальные AI-линтеры
- 02 **Статический анализ** – AI проверяет свой код
- 03 **Code Review** – добавляется агент-ревьюер
- 04 **Тестирование** – агент генерирует тесты
- 05 **CI/CD Gates** – агент самостоятельно чинит падения
- 06 **Incident Response** – откат, post-mortem

Агентский пайплайн

- 01 **Pre-commit** – агент становится автором коммита, локальные AI-линтеры
- 02 **Статический анализ** – AI проверяет свой код
- 03 **Code Review** – добавляется агент-ревьюер
- 04 **Тестирование** – агент генерирует тесты
- 05 **CI/CD Gates** – агент самостоятельно чинит падения
- 06 **Incident Response** – агент участвует в анализе и сам инициирует откат

Агентский пайплайн

- 01 **Pre-commit** – агент становится автором коммита, локальные AI-линтеры
- 02 **Статический анализ** – AI проверяет свой код
- 03 **Code Review** – добавляется агент-ревьюер
- 04 **Тестирование** – агент генерирует тесты
- 05 **CI/CD Gates** – агент самостоятельно чинит падения
- 06 **Incident Response** – агент участвует в анализе и сам инициирует откат

Но не стоит увлекаться слишком сильно

04 Эндшпиль

“

Тестирование может показать наличие дефектов в программе, но не доказать их отсутствие.

Эдсгер Дейкстра

Учёный в области информатики

TELEGRAM-КАНАЛ

@feelindex

Разработка, чистый код, AI, безопасность — и ещё миллион тем для холиваров.



Отсканируйте, чтобы подписаться

Остались вопросы?

Пришло время их задать

Валерий Филатов

Developer Advocate, PVS-Studio

[@feelindex](#) · filatov@pvs-studio.ru

