КАЧЕСТВО И БЕЗОПАСНОСТЬ ПО В ЭПОХУ GenAI

Новая инженерия разработки: ИИ-агенты, quality gates и безопасный код

PVS-Studio

Яндекс

Дмитрий Лавров
Разработчик в Яндекс



Глеб Асламов
Developer Advocate
в PVS-Studio



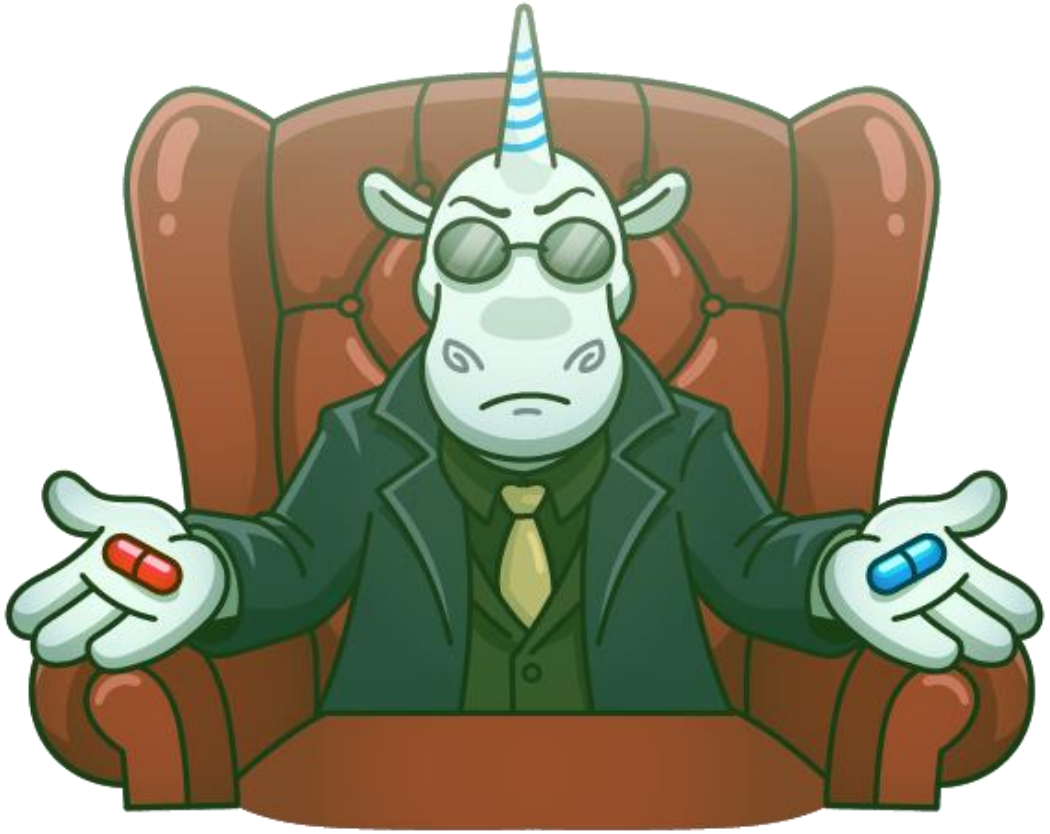
Виталий Пиков
Эксперт в области
безопасной разработки ПО,
амбассадор PVS-Studio



PVS-Studio

Loop engineering

как окно в мир безопасной разработки для ИИ



Глеб Асламов

Senior Developer Advocate, PVS-Studio

17.11.2026

ИИ в РФ

Использование ИИ ещё не показывает уровень доверенной ему автономности

Распространение ИИ в разработке

>80%

участников исследования
применяют ИИ
для разработки кода

54 российских разработчика ПО в выборке
AppSec Solutions и АРПП, сентябрь 2026

Распространение ИИ в разработке

>80%

участников исследования
применяют ИИ
для разработки кода

54 российских разработчика ПО в выборке
AppSec Solutions и АРПП, сентябрь 2026

Цифра описывает использование ИИ, но не права и автономность агентов

Уровни допуска агента

Помощник	Советует человеку и предлагает фрагменты кода

Уровни допуска агента

Помощник	Советует человеку и предлагает фрагменты кода
Участник процесса	Работает в заданной области и проходит проверки

Уровни допуска агента

Помощник	Советует человеку и предлагает фрагменты кода
Участник процесса	Работает в заданной области и проходит проверки
Автономный исполнитель	Сам выбирает действия в пределах выданных прав

Уровни допуска агента

Помощник	Советует человеку и предлагает фрагменты кода
Участник процесса	Работает в заданной области и проходит проверки
Автономный исполнитель	Сам выбирает действия в пределах выданных прав

В безопасном SDLC границы полномочий и условия приёмки заданы явно

Рынок разработки безопасного ПО

≈ 10.000
.000
.000 (млрд)

рублей
оценка рынка РБПО за 2025 год

Экспертная оценка С. Щербакова
«Стахановец», интервью SecPost, 2026

Развивается и нормативная база

ГОСТ Р 56939-2024 Общие требования к процессам РБПО

Развивается и нормативная база

ГОСТ Р 56939-2024 Общие требования к процессам РБПО

ГОСТ Р 71207-2024 Требования к статическому анализу

Развивается и нормативная база

ГОСТ Р 56939-2024	Общие требования к процессам РБПО
ГОСТ Р 71207-2024	Требования к статическому анализу
Еще 7 в 26-27 году	Инструменты, IDE и **ИИ**

Безопасность процесса

Ошибки агента и зависимость
рабочей цепочки от модели

Что меняется с появлением агента

Изменения кода	Исправление может нарушить поведение программы

Что меняется с появлением агента

Изменения кода	Исправление может нарушить поведение программы
Данные и права	Лишние права и передача исходников внешним сервисам

Что меняется с появлением агента

Изменения кода	Исправление может нарушить поведение программы
Данные и права	Лишние права и передача исходников внешним сервисам
Внешние инструкции	Текст в файле или ответе инструмента влияет на действия

Что меняется с появлением агента

Изменения кода	Исправление может нарушить поведение программы
Данные и права	Лишние права и передача исходников внешним сервисам
Внешние инструкции	Текст в файле или ответе инструмента влияет на действия

Чем больше доступных действий, тем важнее технические ограничения

ИИ ищет ошибки и требует проверки

Пример: Big Sleep

Google нашёл уязвимость
в новой версии SQLite

Исправление до релиза

ИИ ищет ошибки и требует проверки

Пример: Big Sleep

Google нашёл уязвимость в новой версии SQLite

Исправление до релиза

Граница вывода

Находка показывает пользу

Полноту проверки проекта оцениваем отдельно

Устойчивость при смене модели

Сильная зависимость

Команды знает только модель
Правила скрыты в диалогах
Результат не воспроизвести
Замена прерывает работу

Устойчивость при смене модели

Сильная зависимость	Управляемая зависимость
Команды знает только модель	Инструменты автономны
Правила скрыты в диалогах	Правила хранятся с кодом
Результат не воспроизвести	Результаты перепроверяемы
Замена прерывает работу	Есть ручной путь и замена

Loop engineering

Агент работает внутри цикла
с явными проверками и условиями приёмки

Quality gate и loop engineering

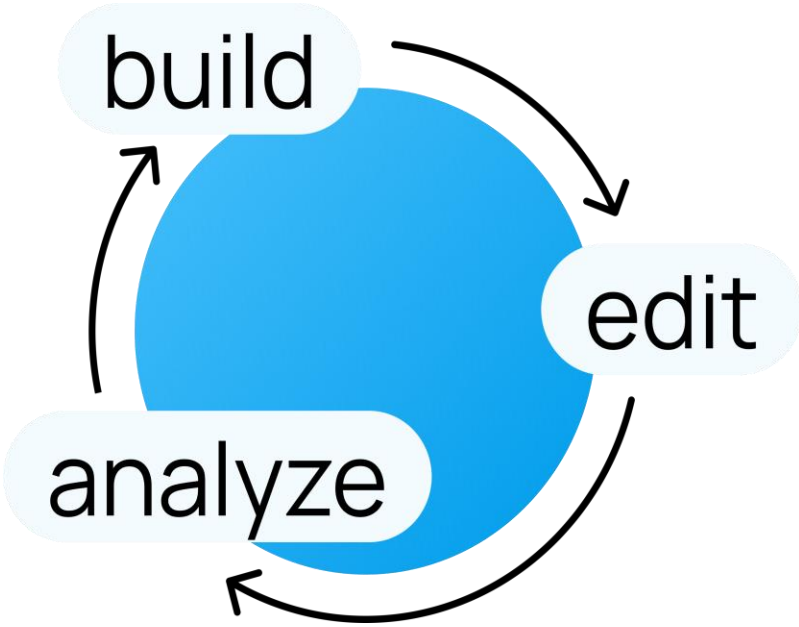
Quality gate	Задаёт условия приёмки

Quality gate и loop engineering

Quality gate	Задаёт условия приёмки
Loop engineering	Организует изменения и повторные проверки

Управляемый цикл исправления

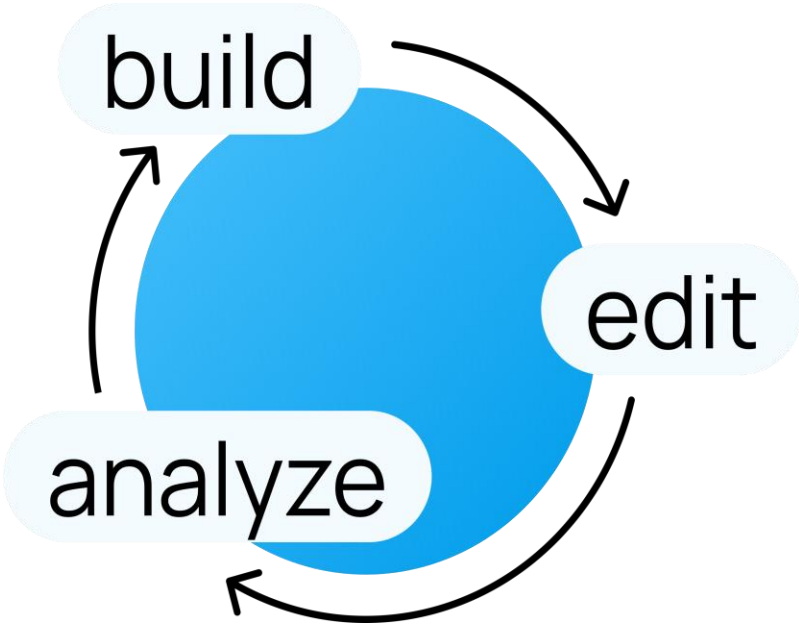
1. Задача и исходная версия



Управляемый цикл исправления

1. Задача и исходная версия

2. Изменение кода агентом

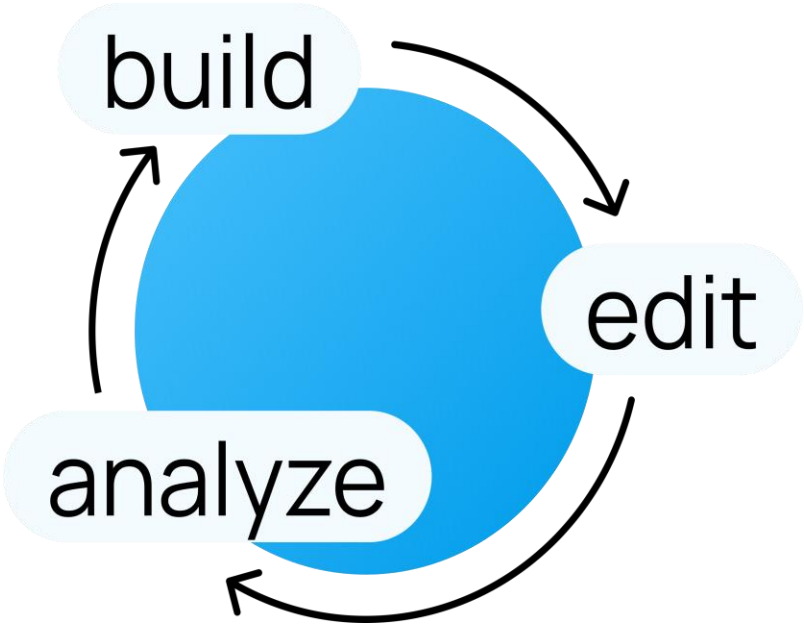


Управляемый цикл исправления

1. Задача и исходная версия

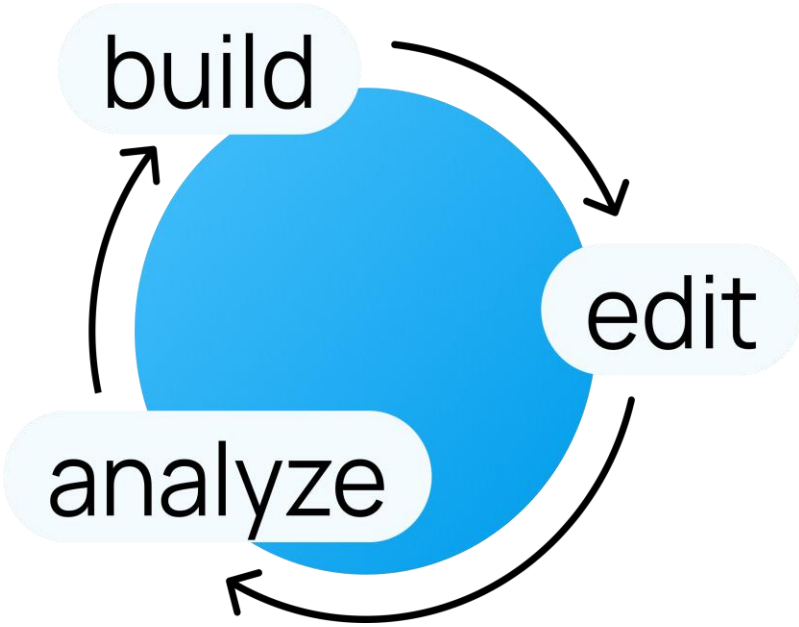
2. Изменение кода агентом

3. Сборка, тесты и анализ



Управляемый цикл исправления

1. Задача и исходная версия
2. Изменение кода агентом
3. **Сборка, тесты и анализ**
4. Разбор и новая попытка



Что именно принимает quality gate

Свежесть — Проверки относятся к текущему состоянию кода

Что именно принимает quality gate

Свежесть	Проверки относятся к текущему состоянию кода
Полнота	Известно, какие файлы и языки проверены

Что именно принимает quality gate

Свежесть	Проверки относятся к текущему состоянию кода
Полнота	Известно, какие файлы и языки проверены
Политика	Замечания разобраны по правилам команды

Что именно принимает quality gate

Свежесть	Проверки относятся к текущему состоянию кода
Полнота	Известно, какие файлы и языки проверены
Политика	Замечания разобраны по правилам команды
Независимость	Агент не меняет критерии успеха ради прохождения

Что именно принимает quality gate

Свежесть	Проверки относятся к текущему состоянию кода
Полнота	Известно, какие файлы и языки проверены
Политика	Замечания разобраны по правилам команды
Независимость	Агент не меняет критерии успеха ради прохождения

Зелёный статус подтверждает заданные проверки. Он не доказывает отсутствие всех уязвимостей.

У цикла есть условия остановки

Продолжаем

Есть конкретное замечание
Понятен следующий шаг
Есть новая информация
Остался бюджет попыток

У цикла есть условия остановки

Продолжаем

Есть конкретное замечание
Понятен следующий шаг
Есть новая информация
Остался бюджет попыток

Передаём инженеру

Повторяется тот же сбой
Неясно нужное поведение
Нужны права или исключение
Исчерпан лимит времени

При замене модели

Сохраняются

Сборка, тесты, анализ
Правила и история результатов

При замене модели

Сохраняются	Сборка, тесты, анализ Правила и история результатов
Проверяем заново	Работу новой модели с теми же инструментами

Инструменты в цикле

Агент проходит инженерный процесс
с привычными инструментами и проверками

Привычные инструменты в цикле

Компилятор — Собирает проект и сообщает об ошибках сборки

Привычные инструменты в цикле

Компилятор	Собирает проект и сообщает об ошибках сборки
Тесты	Проверяют ожидаемое поведение и помогают заметить регрессии

Привычные инструменты в цикле

Компилятор	Собирает проект и сообщает об ошибках сборки
Тесты	Проверяют ожидаемое поведение и помогают заметить регрессии
Стат-Анализ	Находит ошибки и потенциальные уязвимости в исходном коде

Привычные инструменты в цикле

Компилятор	Собирает проект и сообщает об ошибках сборки
Тесты	Проверяют ожидаемое поведение и помогают заметить регрессии
Стат-Анализ	Находит ошибки и потенциальные уязвимости в исходном коде
Агент	Разбирает обратную связь и готовит следующую правку

Опыт инженера для агента

Контекст — Требования, устройство проекта и принятые в команде решения

Опыт инженера для агента

Контекст	Требования, устройство проекта и принятые в команде решения
Skills	Когда и как применять инструменты, что делать с их результатами

Опыт инженера для агента

Контекст	Требования, устройство проекта и принятые в команде решения
Skills	Когда и как применять инструменты, что делать с их результатами
Практика	Проверять работу на задачах и уточнять инструкции

Тот же путь, что у инженера

Разобраться — Прочитать задачу, код и требования безопасности

Тот же путь, что у инженера

Разобраться	Прочитать задачу, код и требования безопасности
Изменить	Подготовить правку и необходимые тесты

Тот же путь, что у инженера

Разобраться	Прочитать задачу, код и требования безопасности
Изменить	Подготовить правку и необходимые тесты
Проверить	Выполнить сборку, тесты и анализ, разобрать замечания

Тот же путь, что у инженера

Разобраться	Прочитать задачу, код и требования безопасности
Изменить	Подготовить правку и необходимые тесты
Проверить	Выполнить сборку, тесты и анализ, разобрать замечания
Предъявить	Показать diff и результаты для ревью и приёмки

PVS-Studio: ответ для агента

```
pvs_check(files: ["/repo/src/net/session.cpp"])
PVS-Studio: 1 warning in change
scope: files (1)
setup: C/C++: CMake target
```

Условный пример формата, не результат нового прогона

PVS-Studio: ответ для агента

```
pvs_check(files: ["/repo/src/net/session.cpp"])
PVS-Studio: 1 warning in change
scope: files (1)
setup: C/C++: CMake target

src/net/session.cpp:88  V595 [L1]
Указатель использован до проверки на nullptr
```

Условный пример формата, не результат нового прогона

PVS-Studio: ответ для агента

```
pvs_check(files: ["/repo/src/net/session.cpp"])
PVS-Studio: 1 warning in change
scope: files (1)
setup: C/C++: CMake target

src/net/session.cpp:88  V595 [L1]
Указатель использован до проверки на nullptr

Not listed: 12 outside the change
Full report: .PVS-Studio/agent/last.json
```

Условный пример формата, не результат нового прогона

«Нет замечаний» и «не проверено»

Результат можно оценить

Анализ завершился
Область проверки известна
Нужный код вошёл в анализ
Остаток замечаний объяснён

«Нет замечаний» и «не проверено»

Результат можно оценить	Нужна отдельная реакция
Анализ завершился	nothing was analyzed
Область проверки известна	project is not ready
Нужный код вошёл в анализ	analysis failed / did not run
Остаток замечаний объяснён	NOT analyzed: ‹язык›

Роли агентов и стоимость контекста

Обычный сценарий

Код запускает проверку
Модель разбирает отчёт
Она же готовит исправление
Инструменты проверяют итог

Роли агентов и стоимость контекста

Обычный сценарий

Код запускает проверку
Модель разбирает отчёт
Она же готовит исправление
Инструменты проверяют итог

Разделение по необходимости

Отдельный контекст ревью
Группы независимых замечаний
Модели по сложности задач
Оценка качества и затрат

Четыре вывода

1. ИИ в РФ

Широкое использование
не означает автономный допуск

Четыре вывода

1. ИИ в РФ — Широкое использование не означает автономный допуск

2. Безопасность — Контроль сохраняется при ошибке или отказе модели

Четыре вывода

1. ИИ в РФ	Широкое использование не означает автономный допуск
2. Безопасность	Контроль сохраняется при ошибке или отказе модели
3. Loop engineering	Привычные проверки и явные правила для агента

Четыре вывода

1. ИИ в РФ	Широкое использование не означает автономный допуск
2. Безопасность	Контроль сохраняется при ошибке или отказе модели
3. Loop engineering	Привычные проверки и явные правила для агента
4. Инструменты	Контекст, skills и инструменты для полного инженерного цикла

Q&A

Всё!

Глеб Асламов, PVS-Studio

Сделай свой проект
чистым и безопасным
вместе с PVS-Studio
по промокоду

QUALITY_GENAI

PVS-Studio

