

Трудности при интеграции SAST: разбираем и исправляем

PVS-Studio



Глеб Асламов
C# Developer

Уязвимости и SAST

Уязвимости и SAST

Трудности при интеграции и их решение

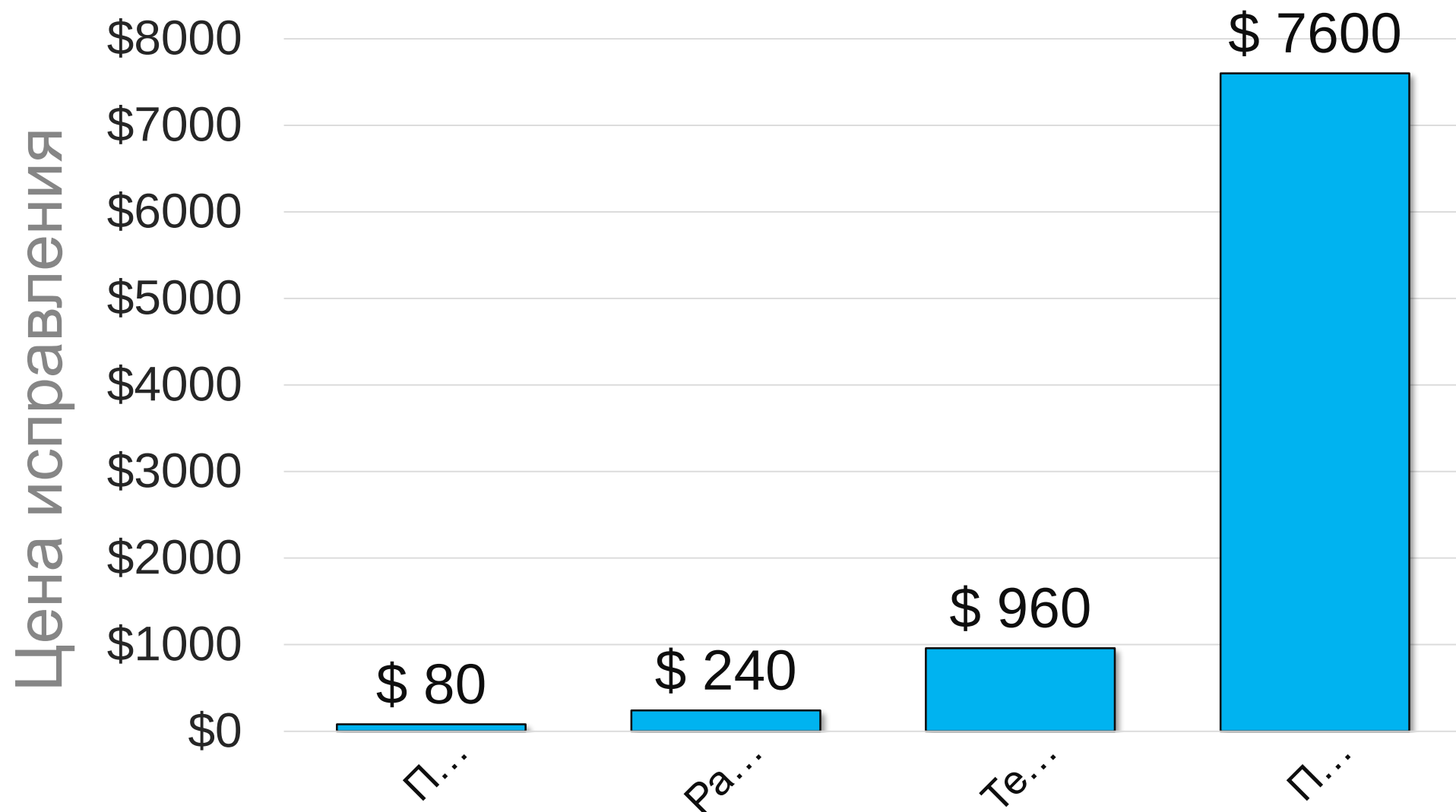
Уязвимости и SAST

Трудности при интеграции и их решение

Как быстро попробовать SAST инструмент

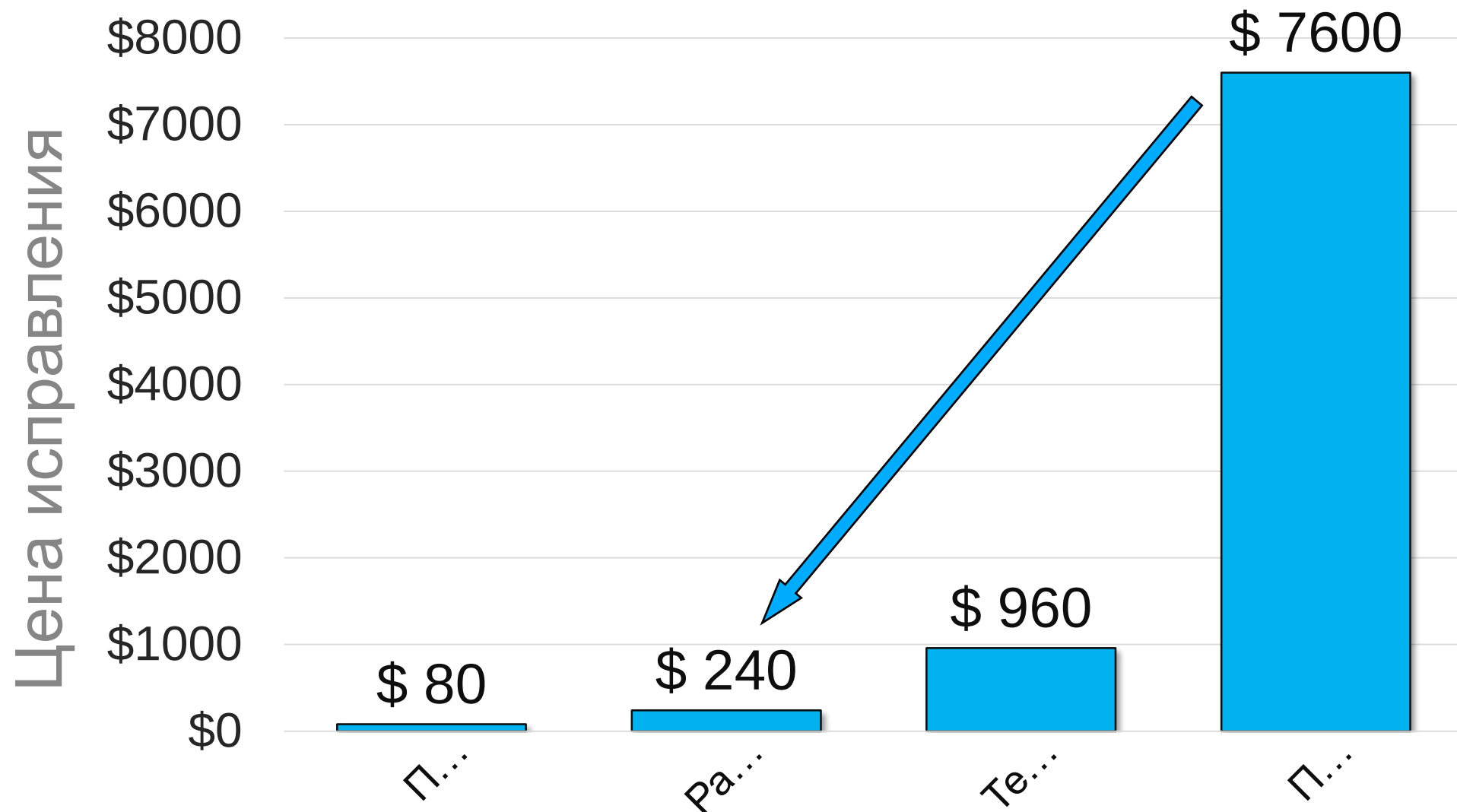
Почему уязвимости опасны?

Сколько стоит исправить уязвимость?



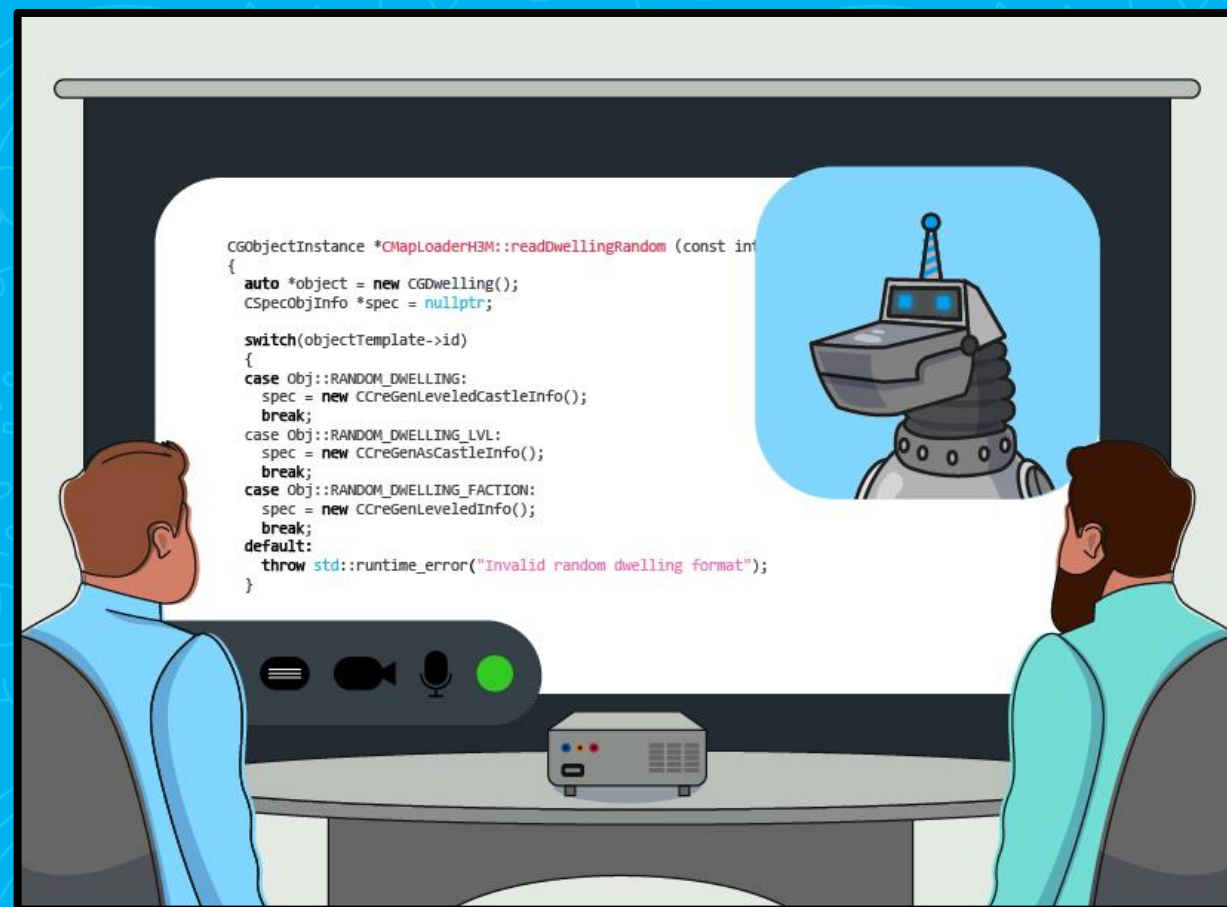
Источник - NIST: National Institute of Standards and Technology

Сколько стоит исправить уязвимость?



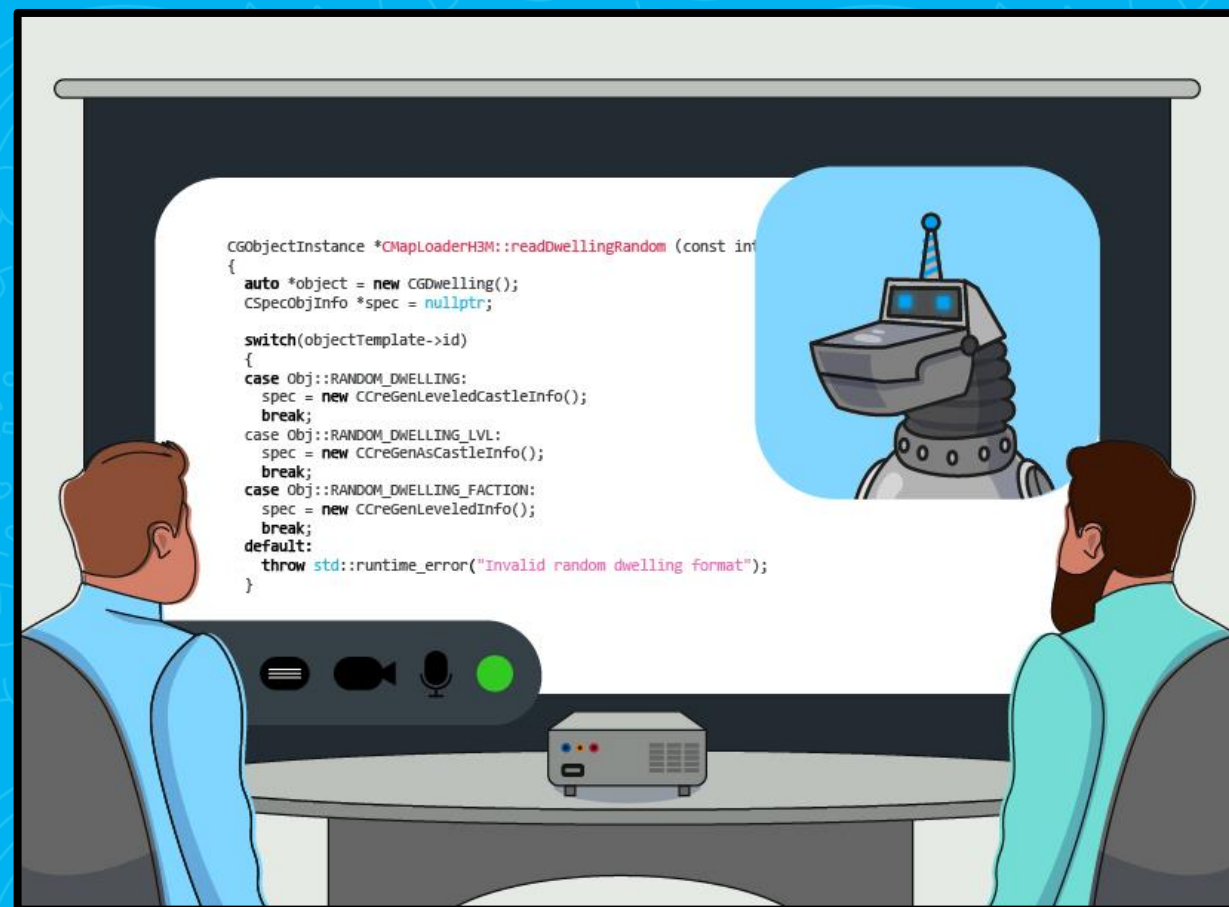
Источник - NIST: National Institute of Standards and Technology

Как искать уязвимости?



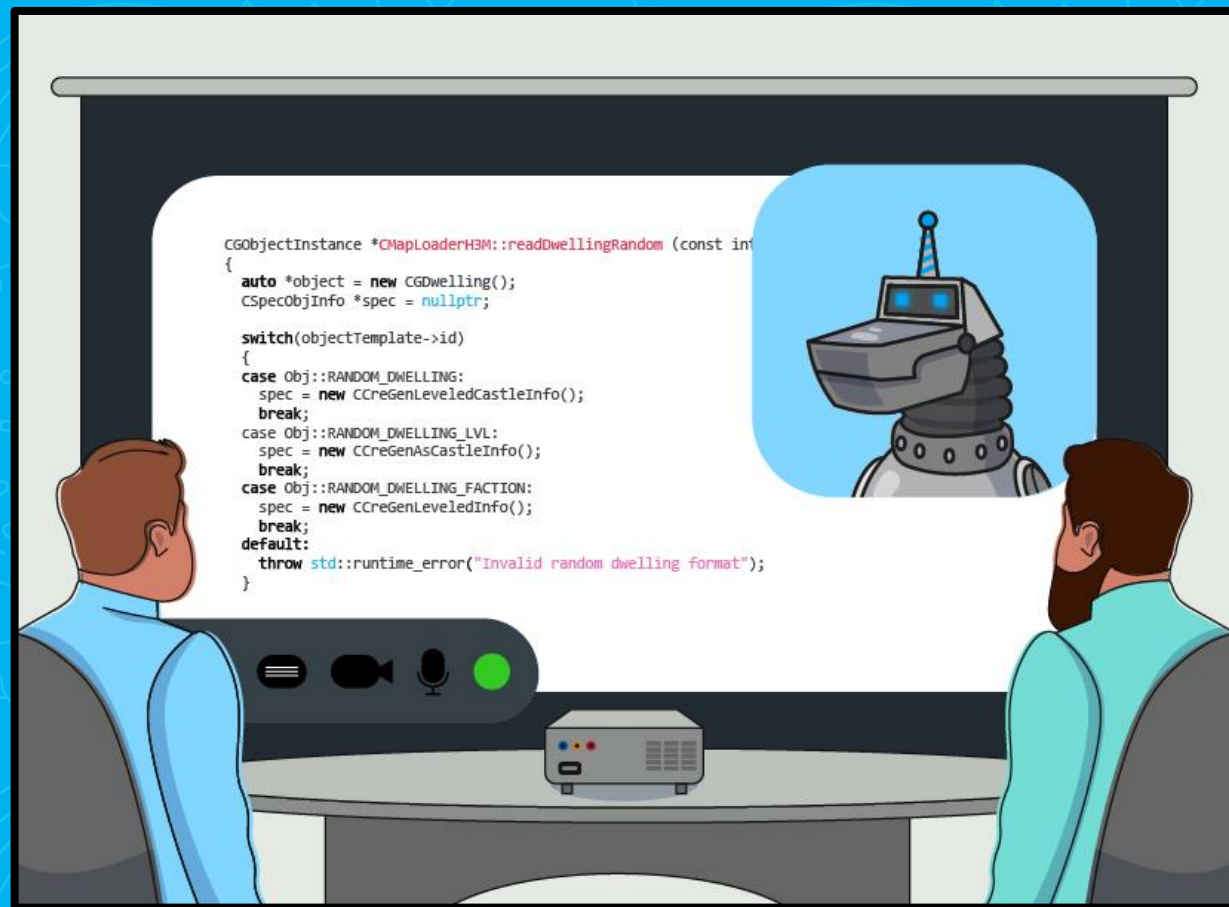
Как искать уязвимости?

- Часто ошибки == уязвимости



Как искать уязвимости?

- Часто уязвимости == ошибки
- Помогут найти тесты и анализаторы



Что такое SAST?

Жизнь без SAST

Сделать	В процессе	Сделано
Баг	Баг	Баг
Фича	Эпик	Баг
Баг	Баг	Баг



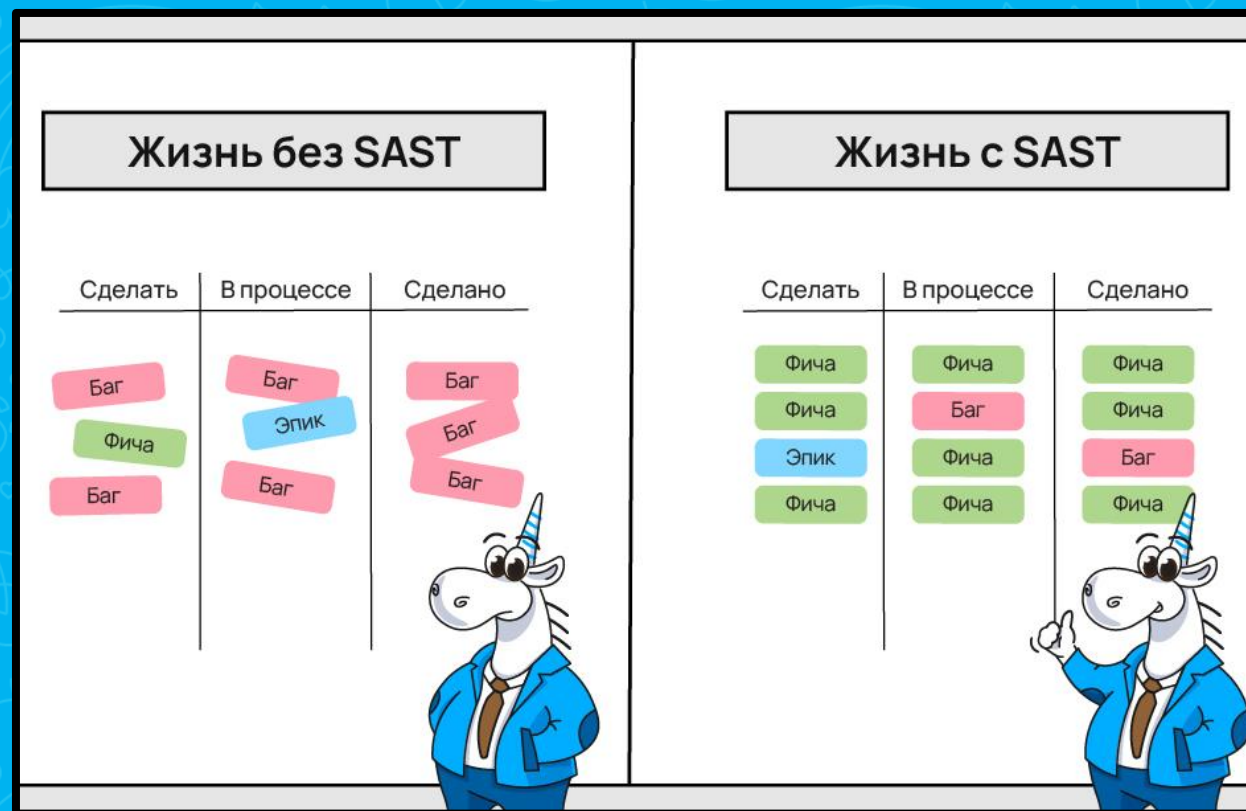
Жизнь с SAST

Сделать	В процессе	Сделано
Фича	Фича	Фича
Фича	Баг	Фича
Эпик	Фича	Баг
Фича	Фича	Фича



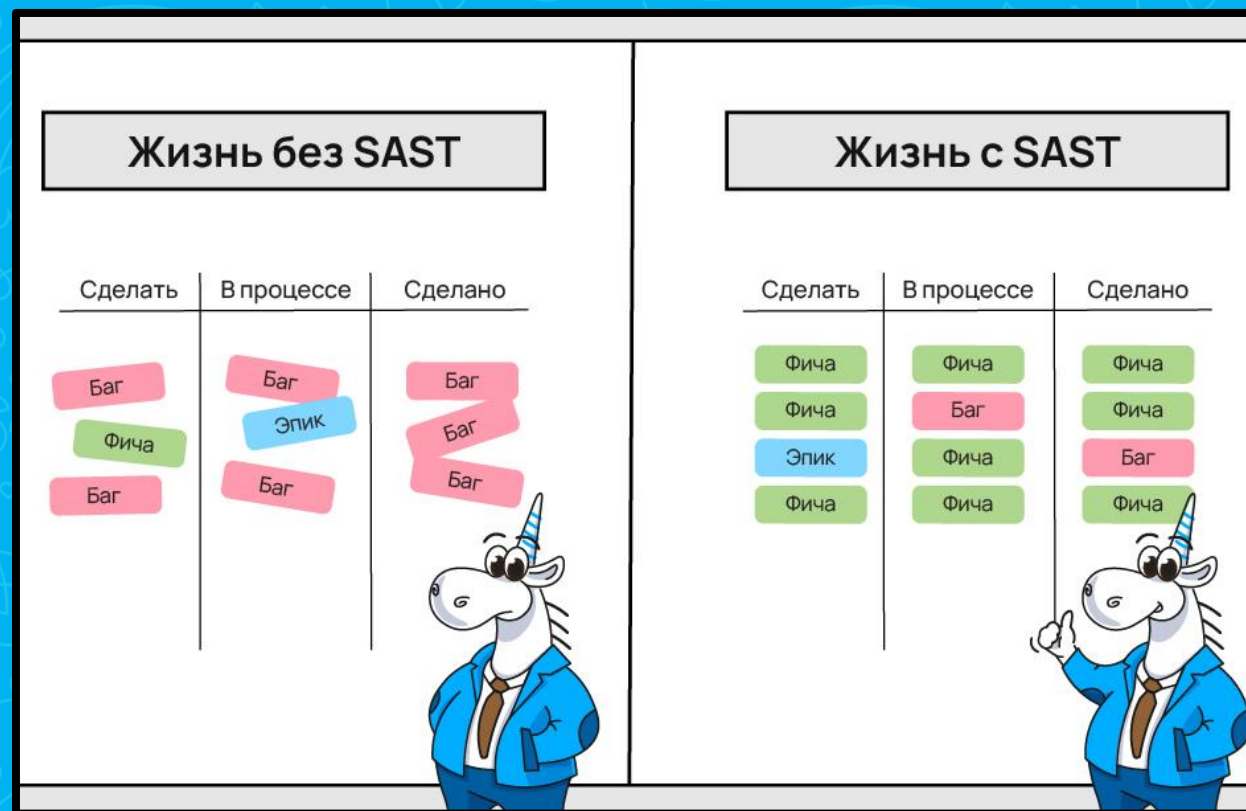
Что такое SAST?

- Статический анализ, но про уязвимости



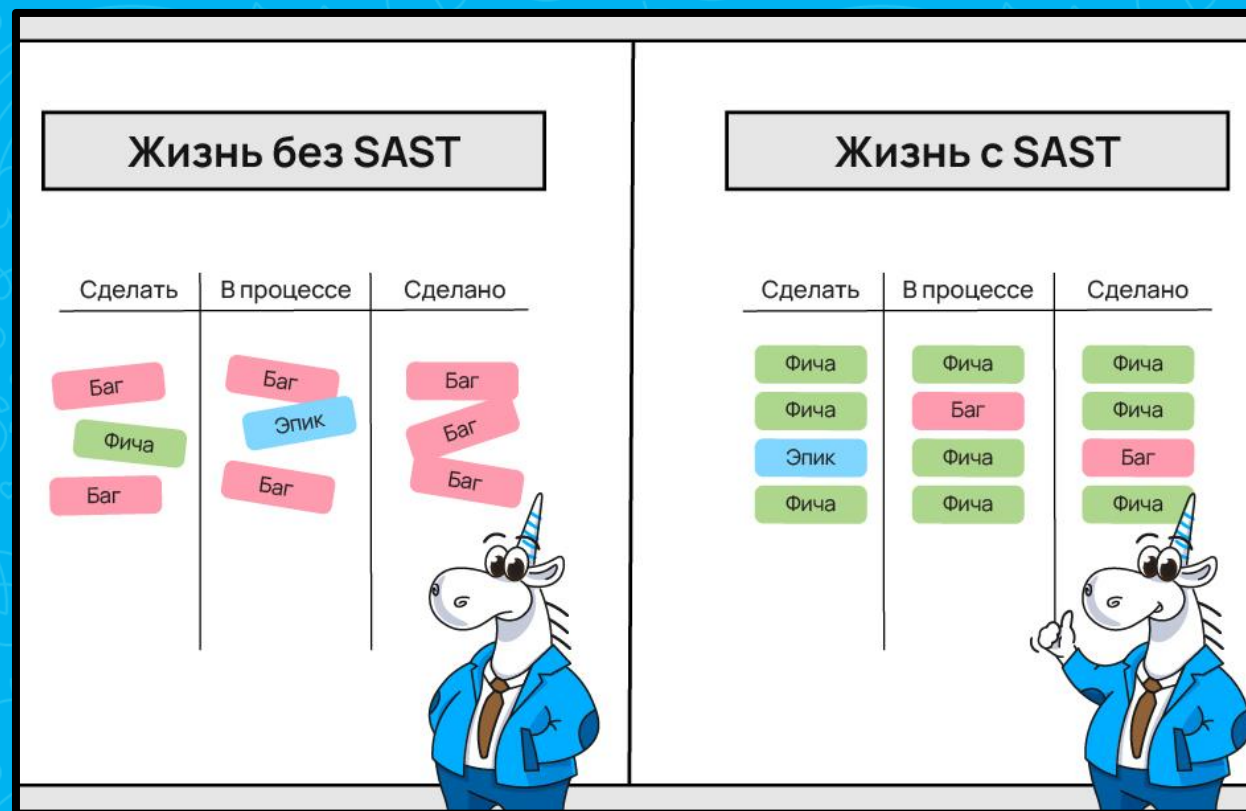
Что такое SAST?

- Статический анализ, но про уязвимости
- Нужен только код



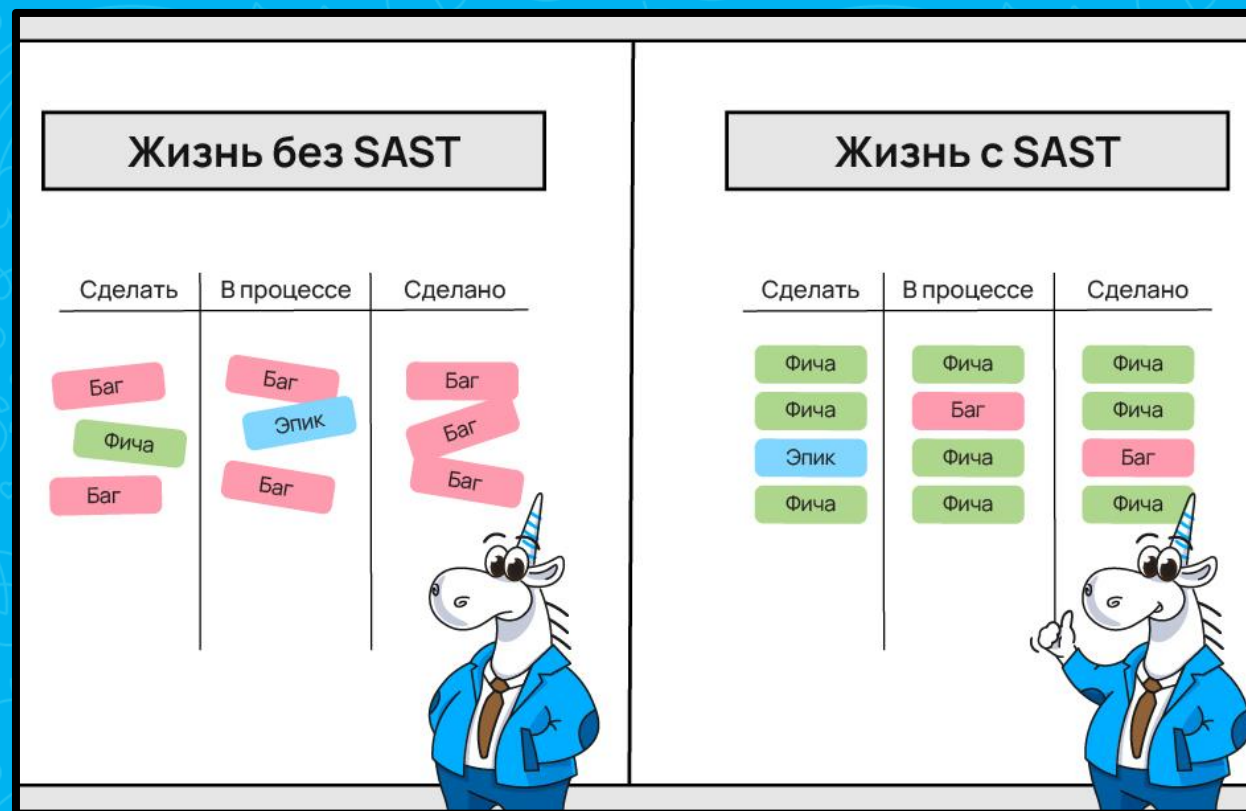
Что такое SAST?

- Статический анализ, но про уязвимости
- Нужен только код
- Полное покрытие



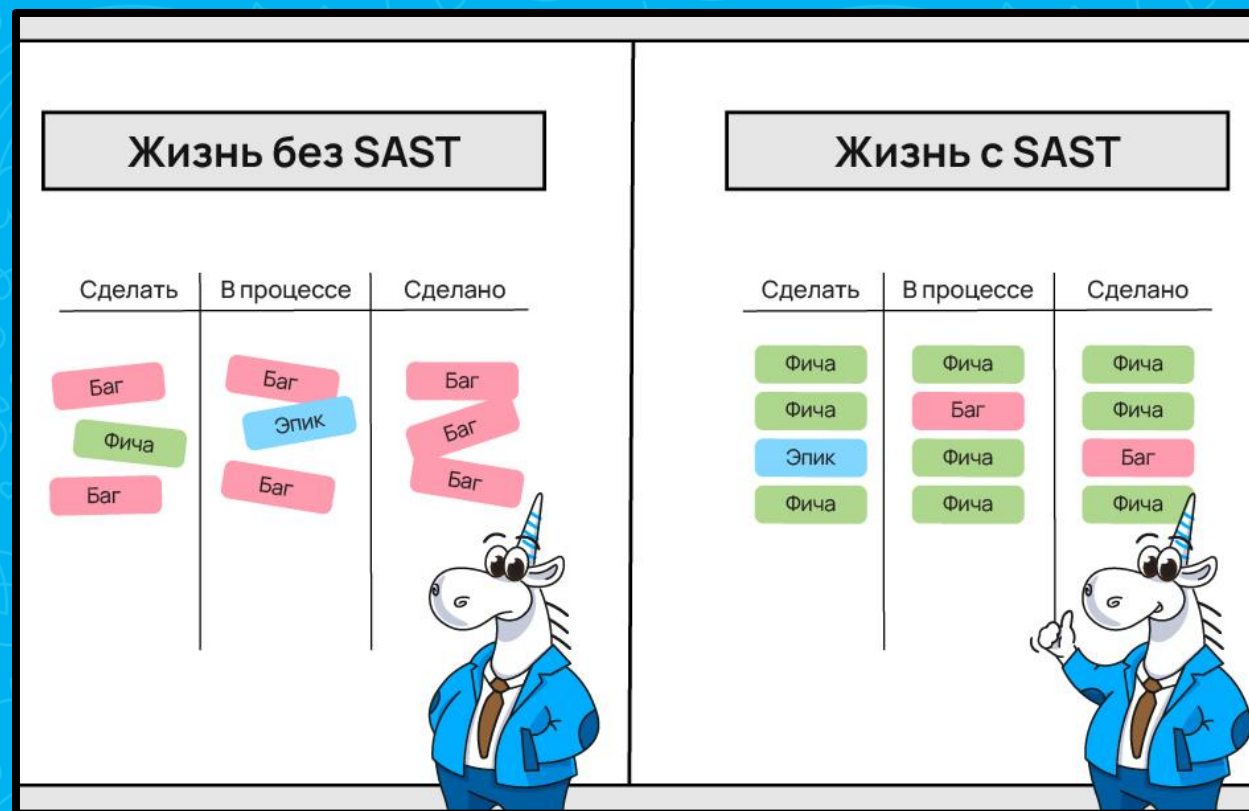
Что такое SAST?

- Статический анализ, но про уязвимости
- Нужен только код
- Полное покрытие
- Раннее обнаружение ошибок и уязвимостей



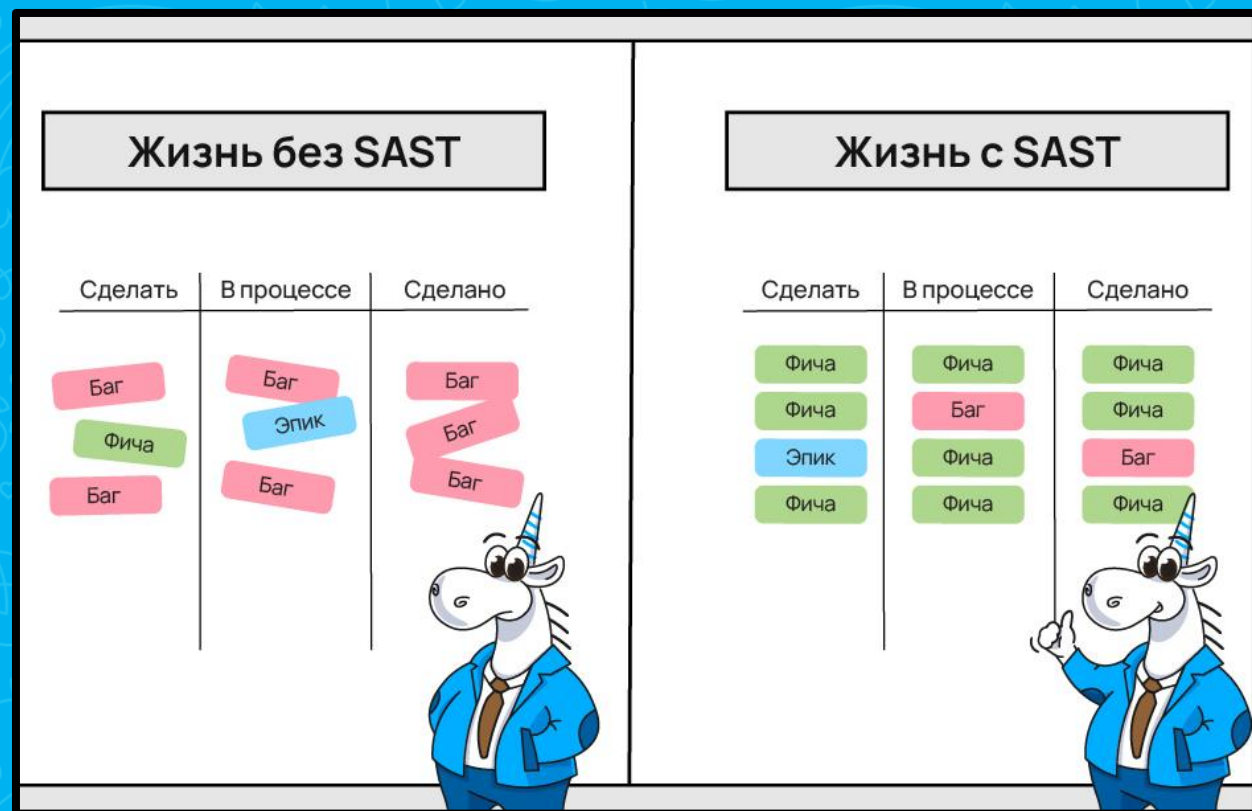
Что такое SAST?

- Статический анализ, но про уязвимости
- Нужен только код
- Полное покрытие
- Раннее обнаружение ошибок и уязвимостей
- Исправление до этапа тестирования



Что такое SAST?

- Статический анализ, но про уязвимости
- Нужен только код
- Полное покрытие
- Раннее обнаружение ошибок и уязвимостей
- Исправление до этапа тестирования
- PVS-Studio – это SAST инструмент



Пример CWE в проекте FastReport

```
ParagraphFormat paragraphFormat;
```

```
....
```

```
public ParagraphFormat ParagraphFormat  
{  
    get { return paragraphFormat; }  
    set { ParagraphFormat = value; }  
}
```



Пример CWE в проекте FastReport

ParagraphFormat paragraphFormat; Поле 

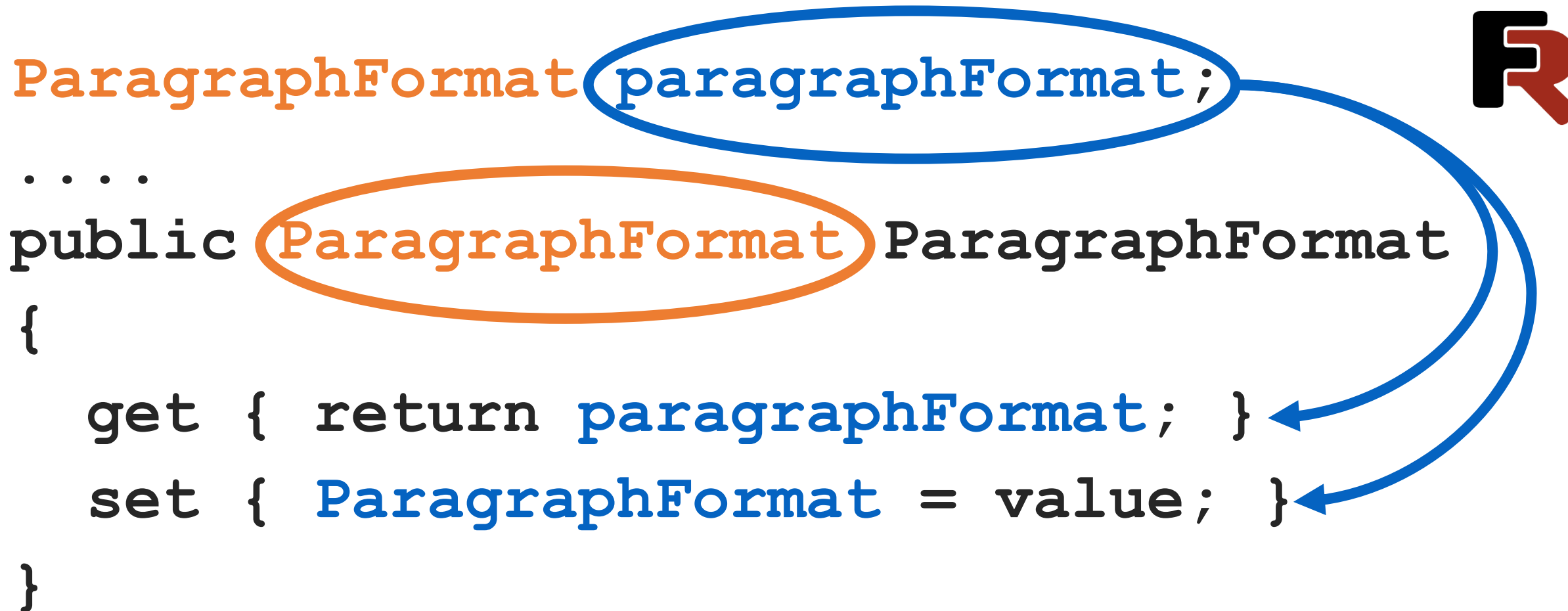
```
....  
public ParagraphFormat ParagraphFormat  
{  
    get { return paragraphFormat; }  
    set { ParagraphFormat = value; }  
}
```

Пример CWE в проекте FastReport

```
ParagraphFormat paragraphFormat; Поле   
...  
public ParagraphFormat ParagraphFormat  
{  
    СВОЙСТВО  
    get { return paragraphFormat; }  
    set { ParagraphFormat = value; }  
}
```

Пример CWE в проекте FastReport

```
ParagraphFormat paragraphFormat;  
....  
public ParagraphFormat ParagraphFormat  
{  
    get { return paragraphFormat; }  
    set { ParagraphFormat = value; }  
}
```



Пример CWE в проекте FastReport

```
ParagraphFormat paragraphFormat;
```



```
....
```

```
public ParagraphFormat  
{  
    get { return paragraphFormat; }  
    set { ParagraphFormat = value; }  
}
```

Пример CWE в проекте FastReport

```
ParagraphFormat paragraphFormat;
```

```
....
```

```
public ParagraphFormat ParagraphFormat  
{  
    get { return paragraphFormat; }  
    set { ParagraphFormat = value; }  
}
```



Пример CWE в проекте FastReport



```
static void Main(string[] args)
{
    TextObject textObj = new TextObject();
    textObj.ParagraphFormat = null;

    Console.WriteLine("Ok");
}
```

Пример CWE в проекте FastReport



```
static void Main(string[] args)
```

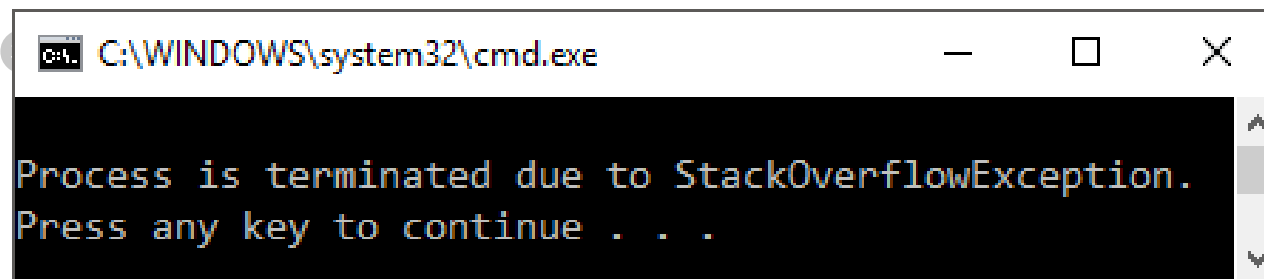
```
{
```

```
    TextObj
```

```
    textObj
```

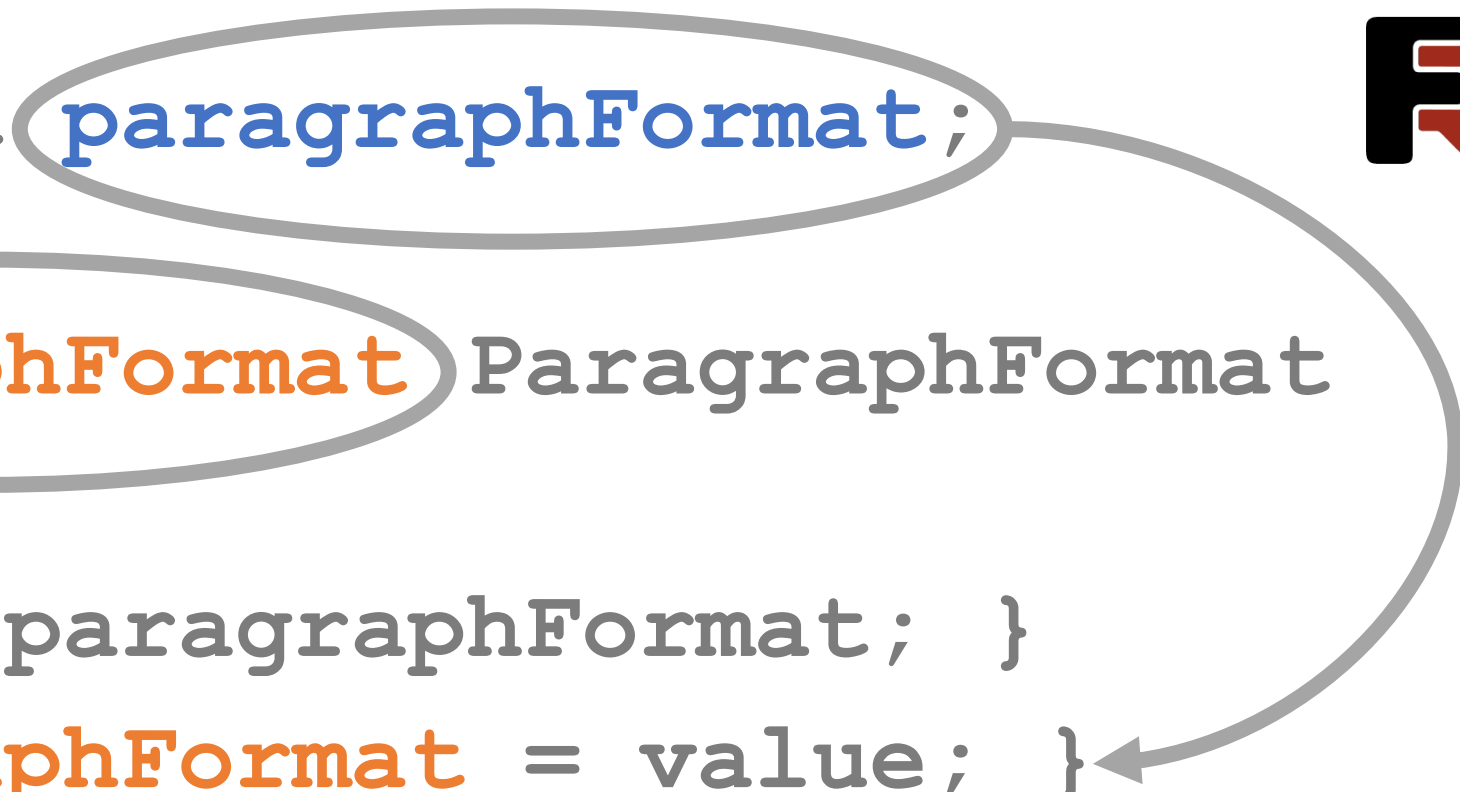
```
    Console.WriteLine("Ok");
```

```
}
```



Пример CWE в проекте FastReport

```
ParagraphFormat paragraphFormat;  
....  
public ParagraphFormat ParagraphFormat  
{  
    get { return paragraphFormat; }  
    set { ParagraphFormat = value; }
```



Предупреждение PVS-Studio: V3010 [CWE-674]

Possible infinite recursion inside 'ParagraphFormat' property.

Разбираем проблемы при интеграции в legacy проект

PVS-Studio



Fails: 0



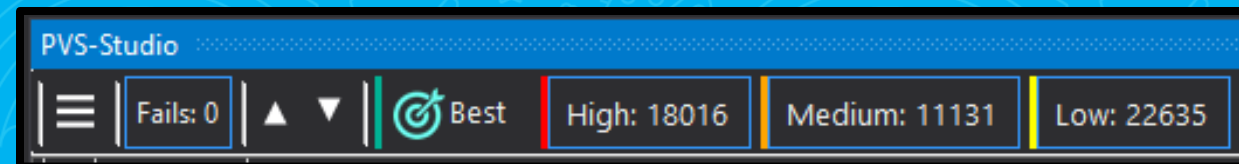
Best

High: 18016

Medium: 11131

Low: 22635

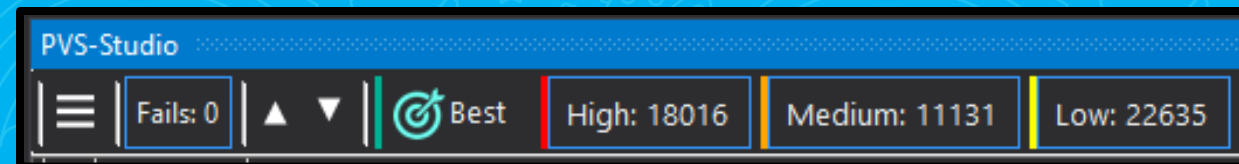
Опасность первого раза



Опасность первого раза

- Много срабатываний ==

нормально

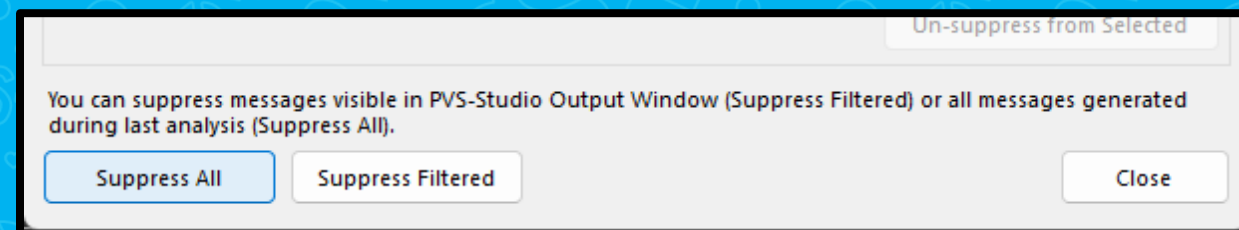
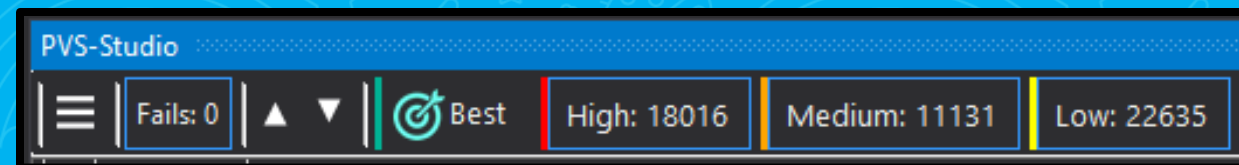


Опасность первого раза

- Много срабатываний ==

нормально

- **Используем массовое подавление**



Опасность первого раза

- Много срабатываний ==

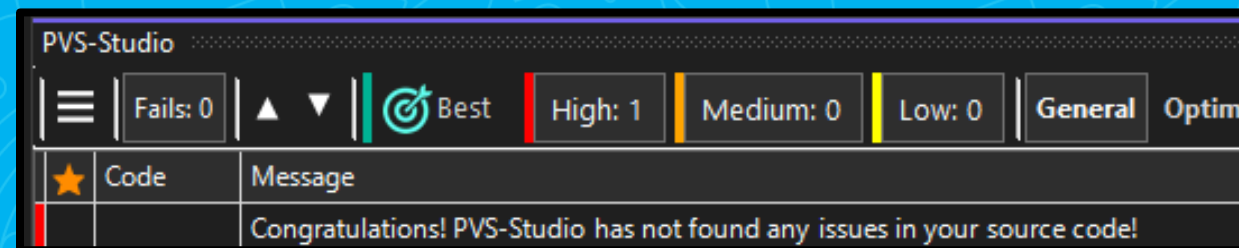
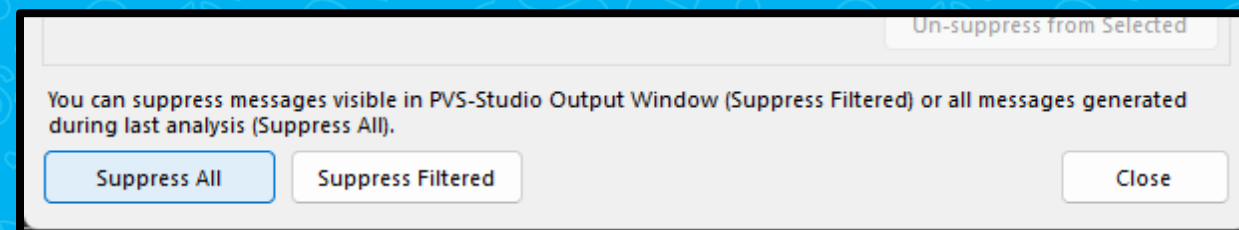
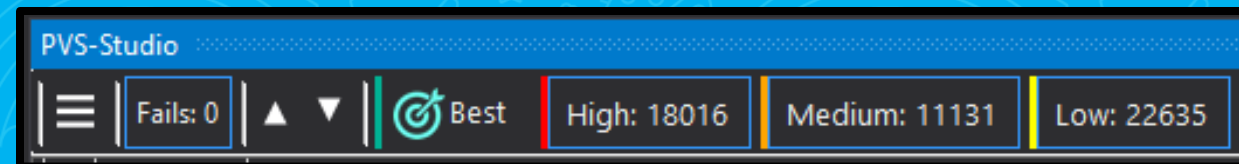
нормально

- **Используем массовое**

подавление

- Периодически возвращаемся и

чиним



Опасность первого раза

- Много срабатываний ==

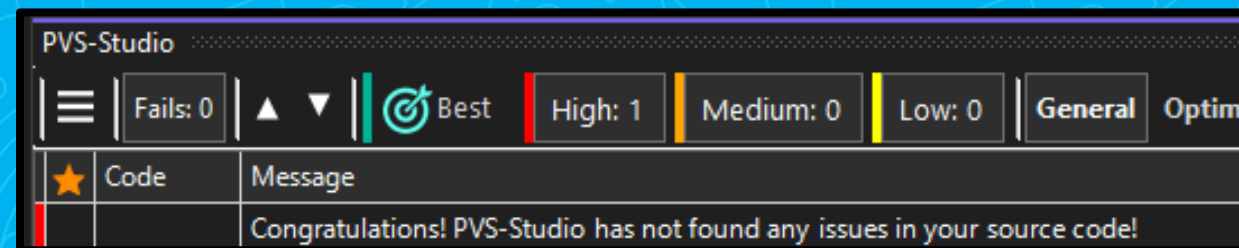
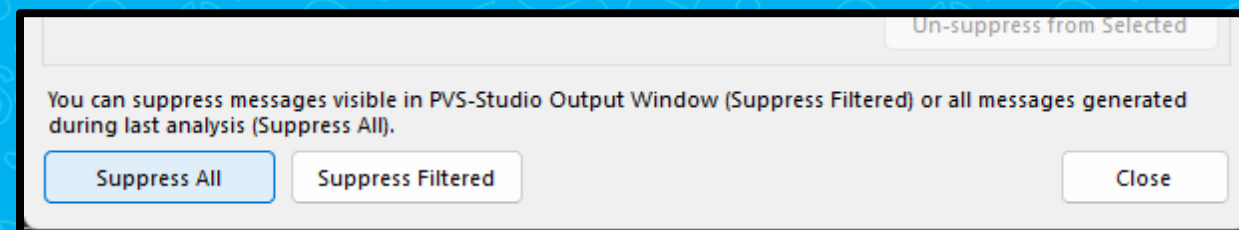
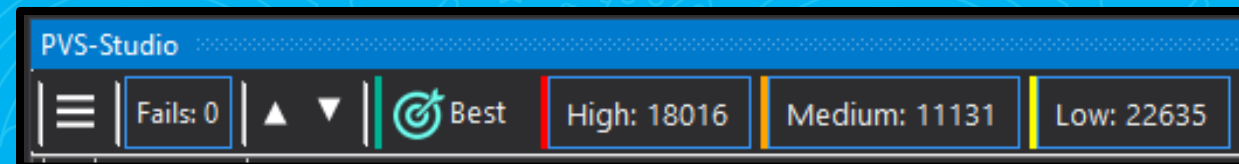
нормально

- **Используем массовое**

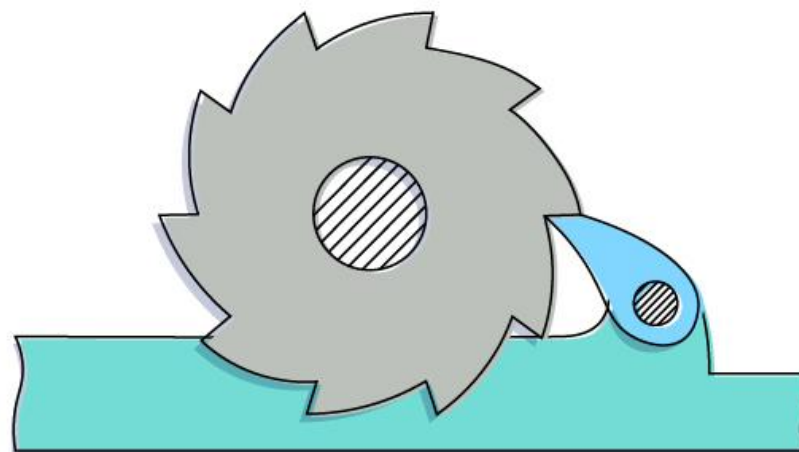
подавление

- Периодически возвращаемся и

чиним

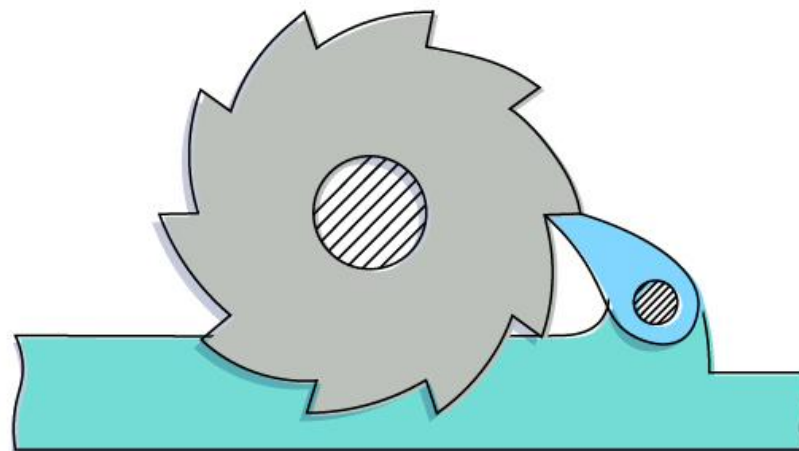


Принцип Храповика



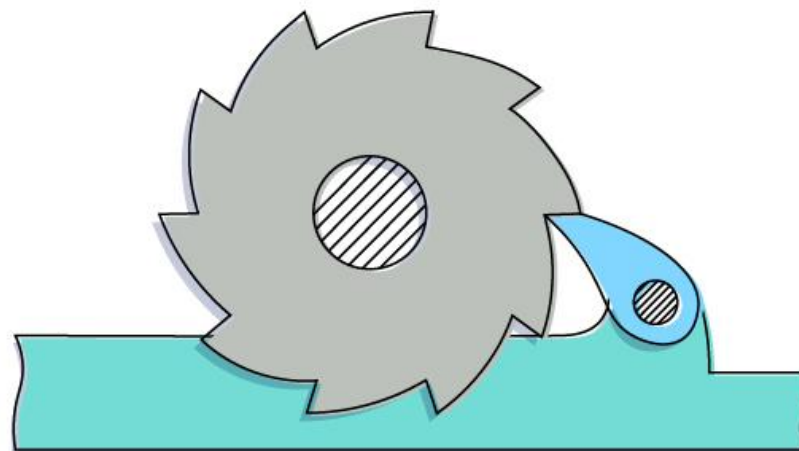
Принцип Храповика

- Выполняем анализ



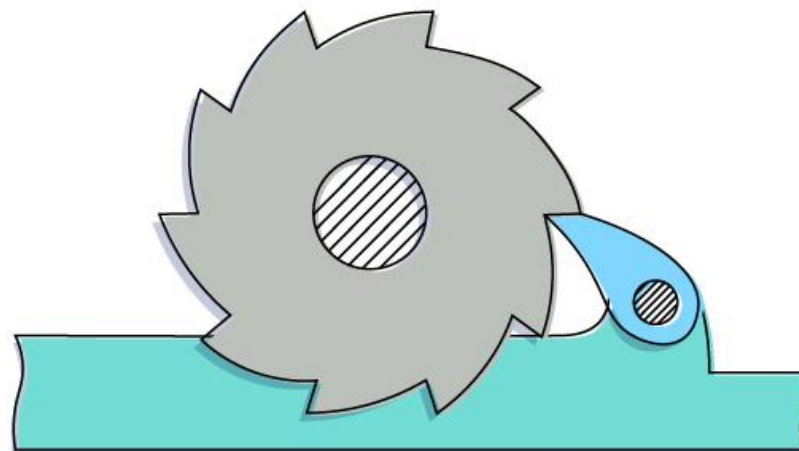
Принцип Храповика

- Выполняем анализ
- **Заносим в систему контроля версий и устанавливаем порог вхождения**

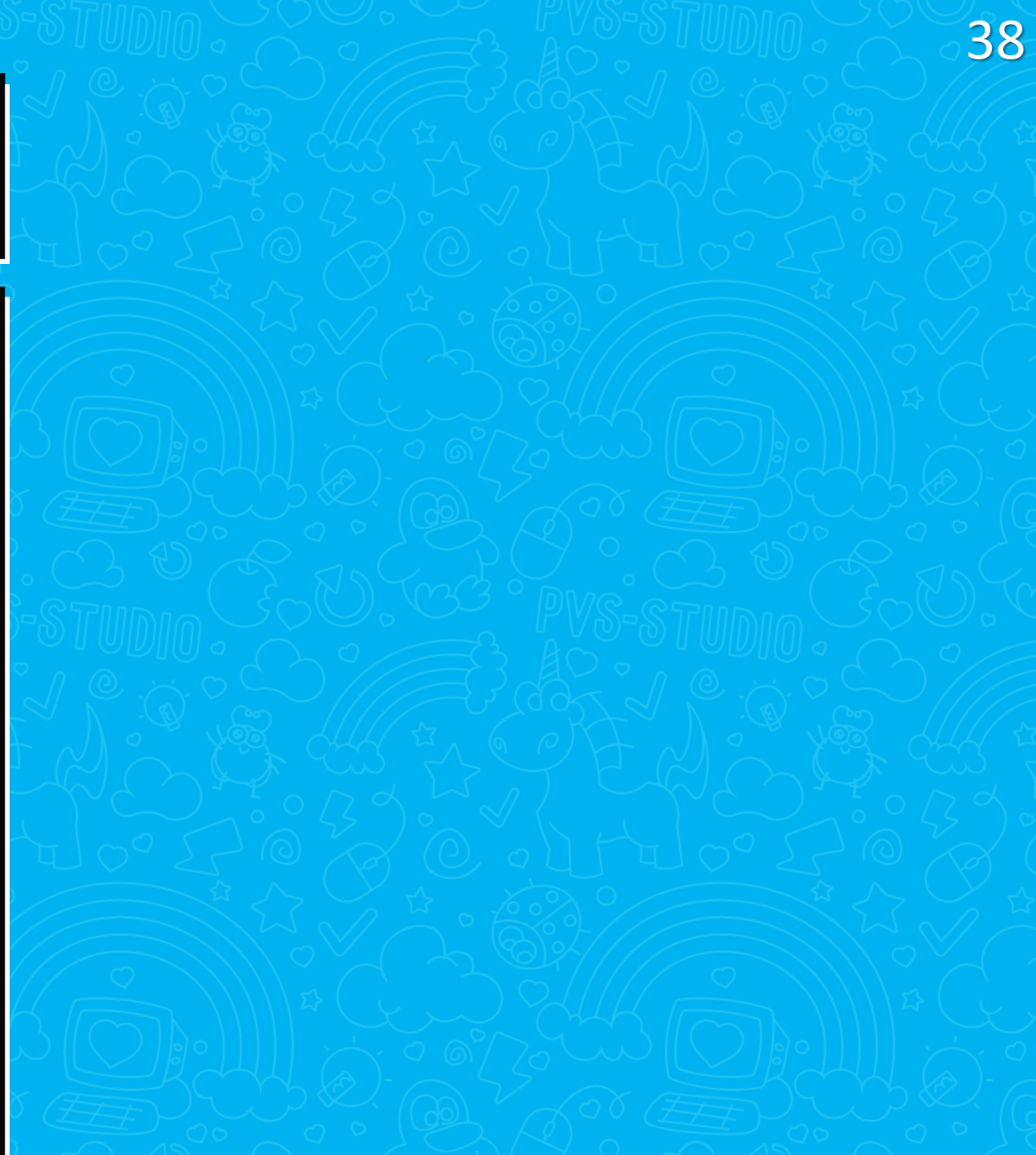


Принцип Храповика

- Выполняем анализ
- **Заносим в систему контроля версий и устанавливаем порог вхождения**
- Исправляем!



Ложные срабатывания

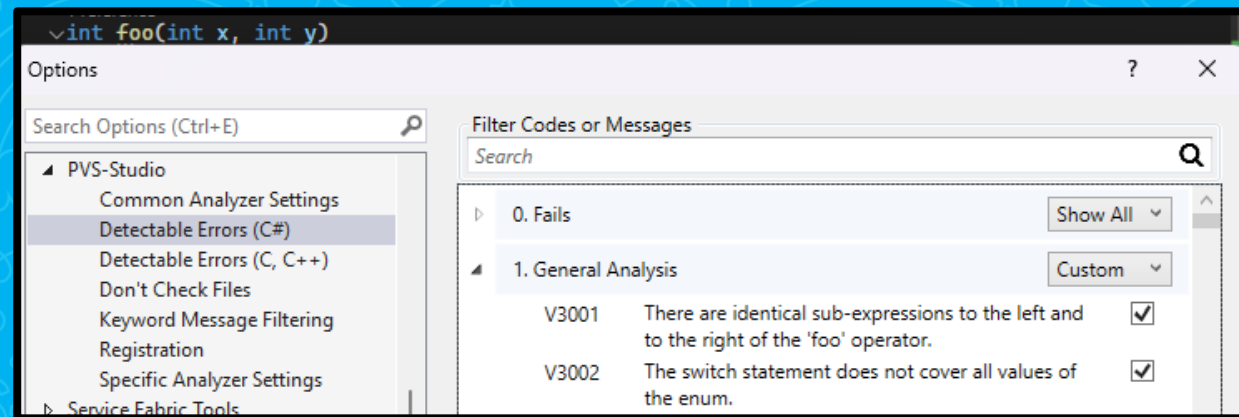


Ложные срабатывания

- Особенность технологии

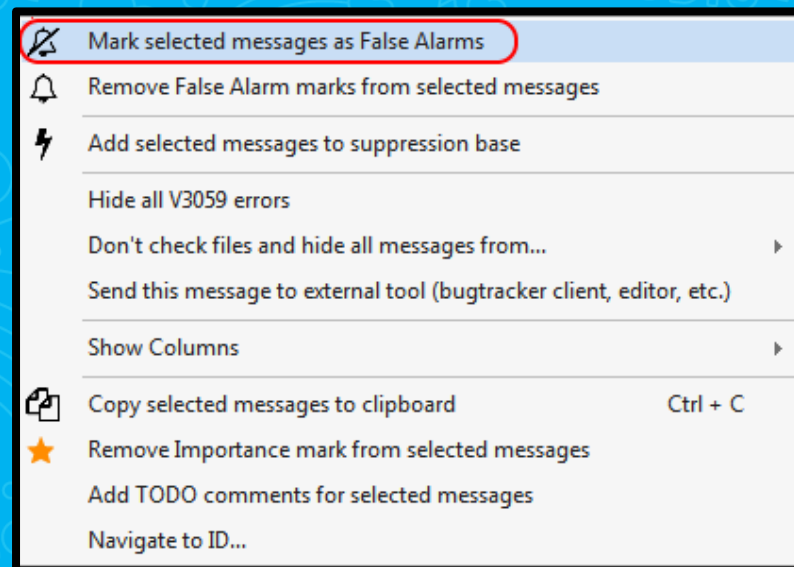
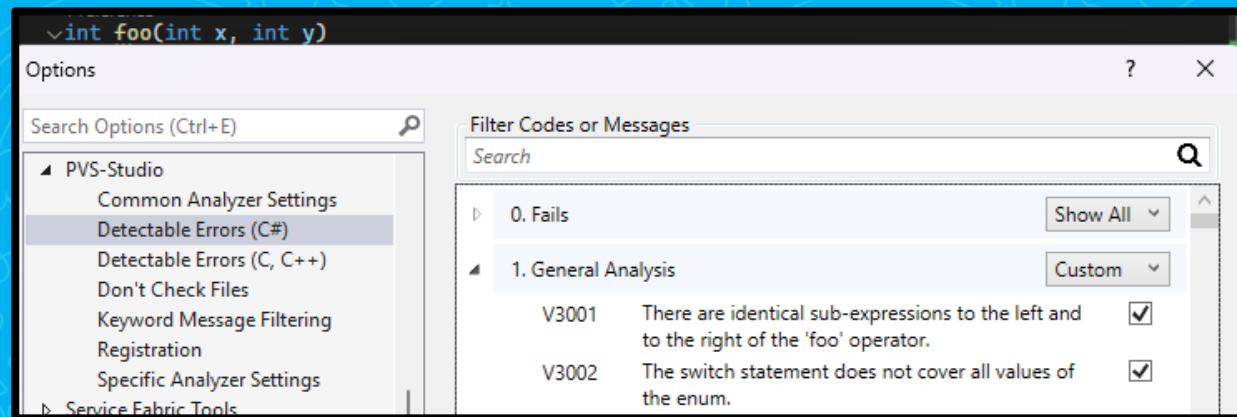
Ложные срабатывания

- Особенность технологии
- Настраиваем анализатор под проект

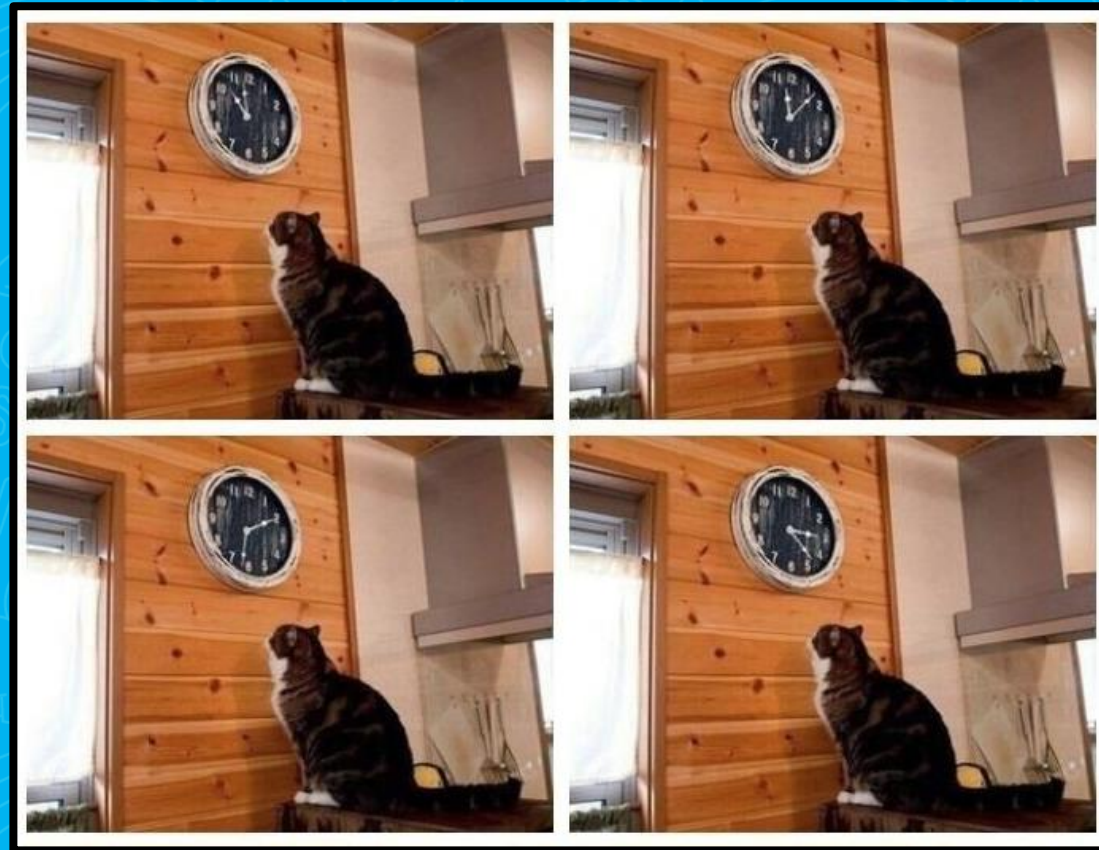


Ложные срабатывания

- Особенность технологии
- Настраиваем анализатор под проект

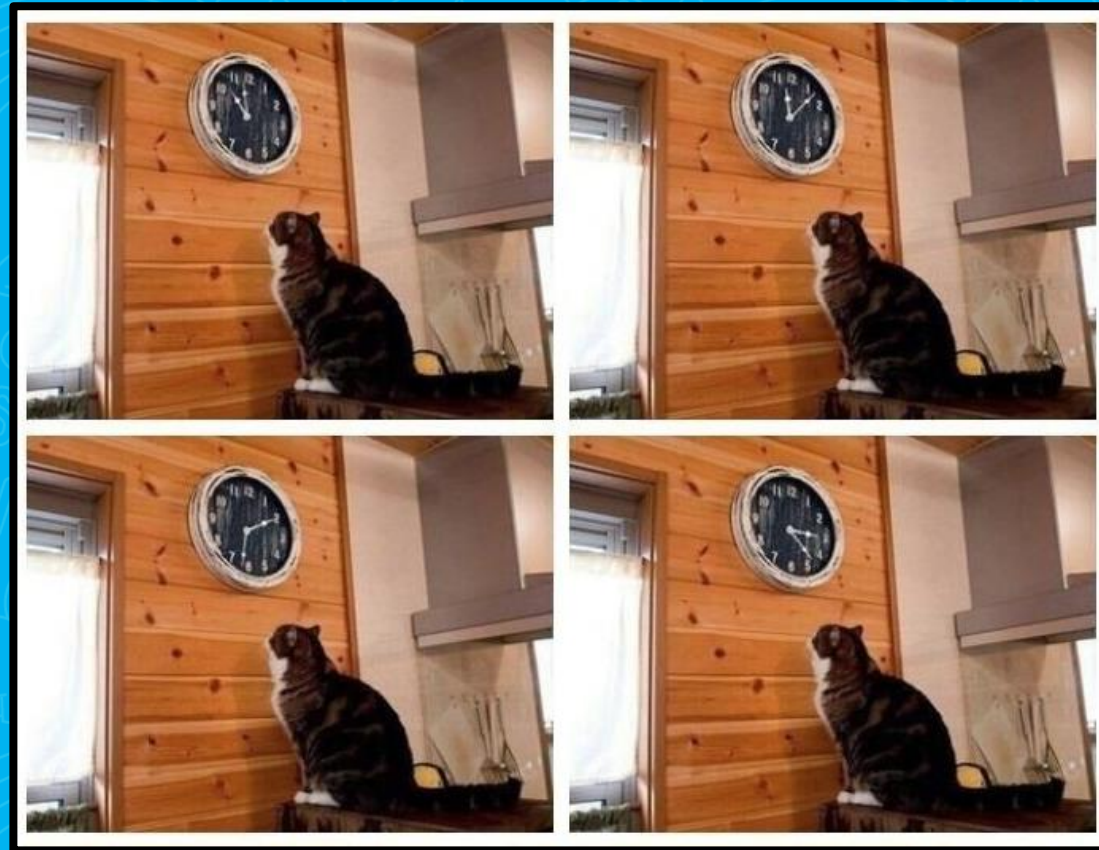


Долго время анализа



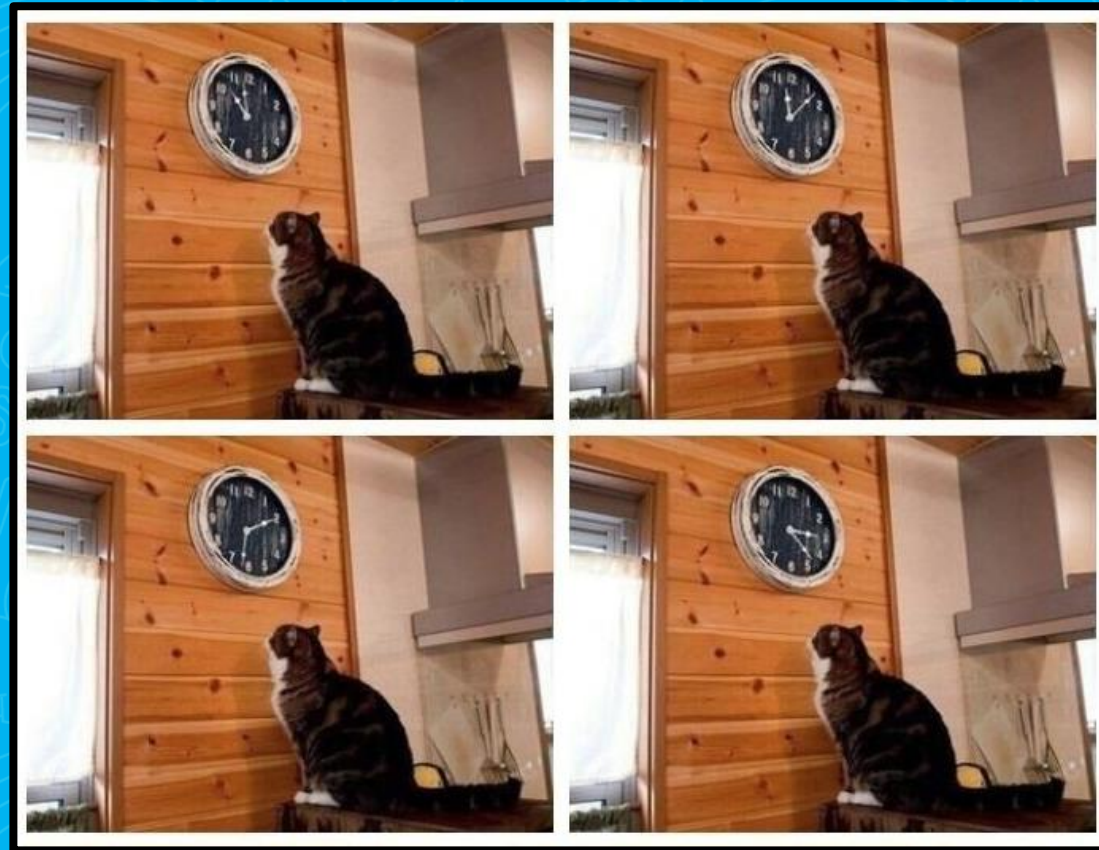
Долго время анализа

- Больше проект == больше время



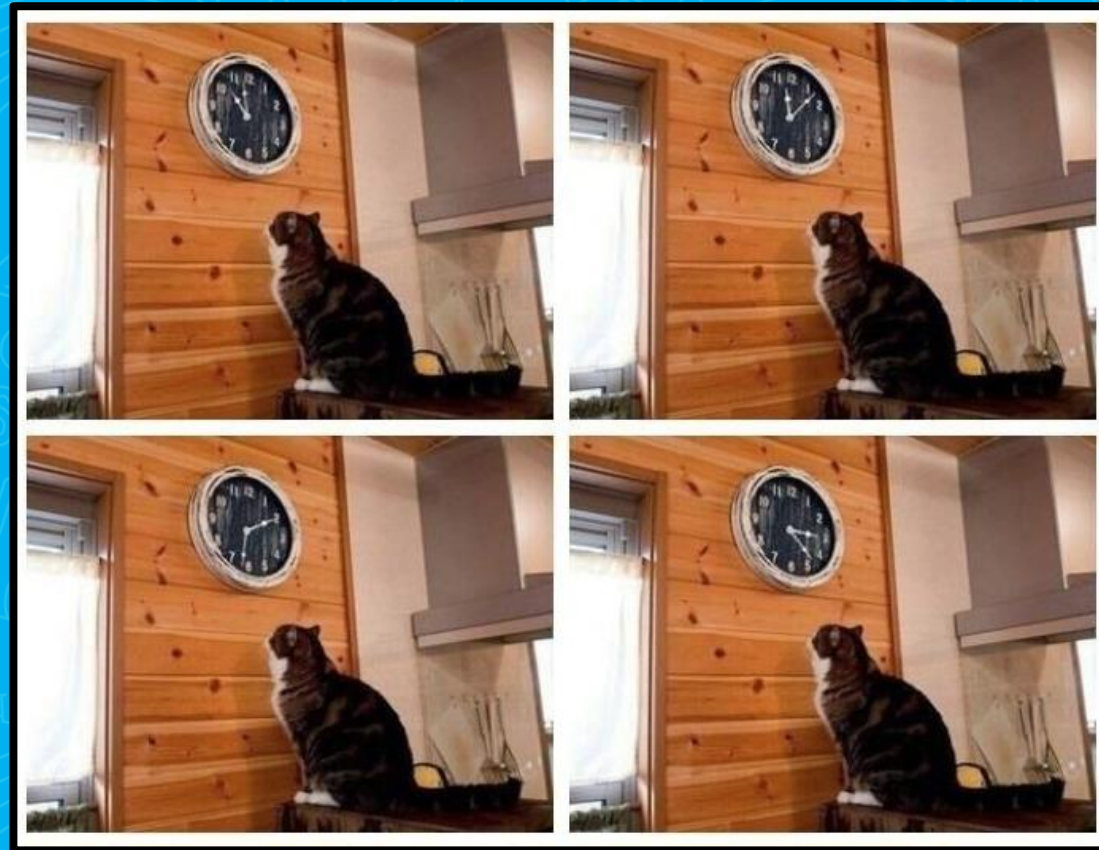
Долго время анализа

- Больше проект == больше время
- **Инкрементальный анализ**

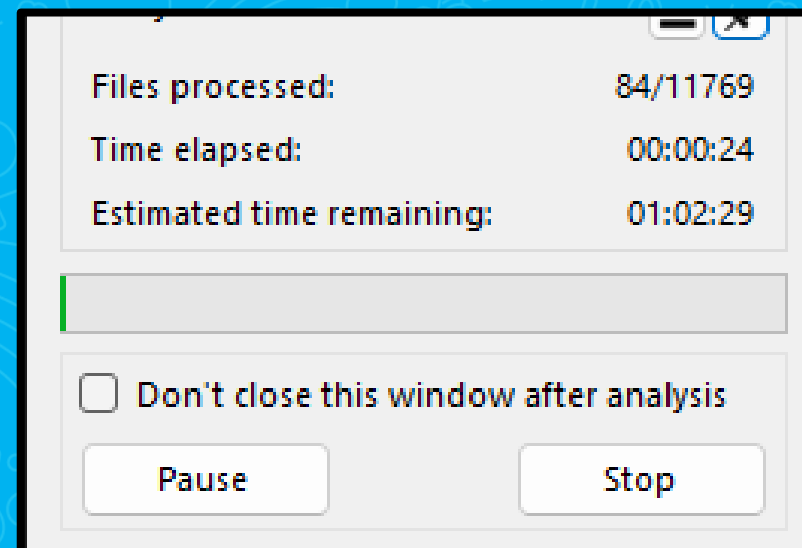
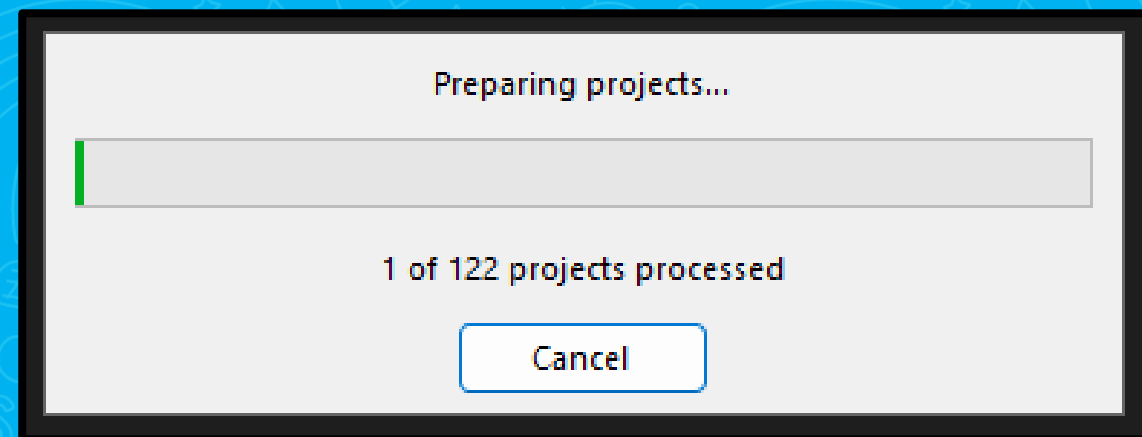


Долго время анализа

- Больше проект == больше время
- **Инкрементальный анализ**
- Проверяйте только **изменённый код**

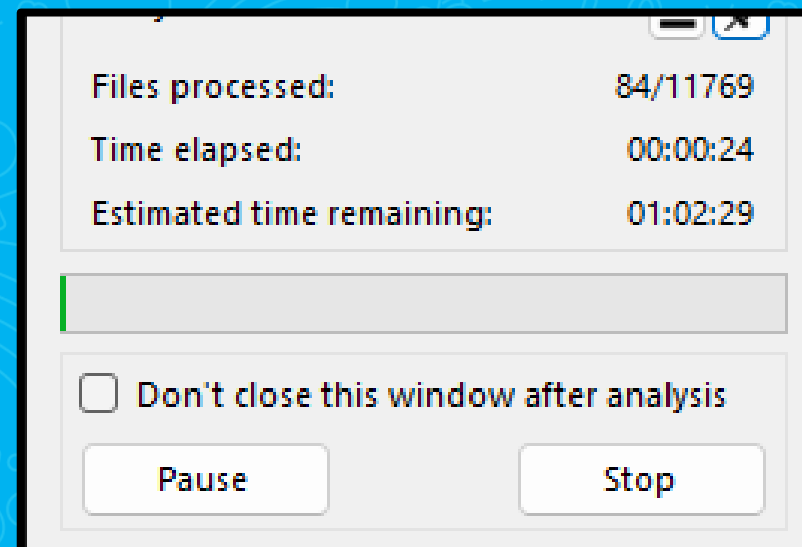
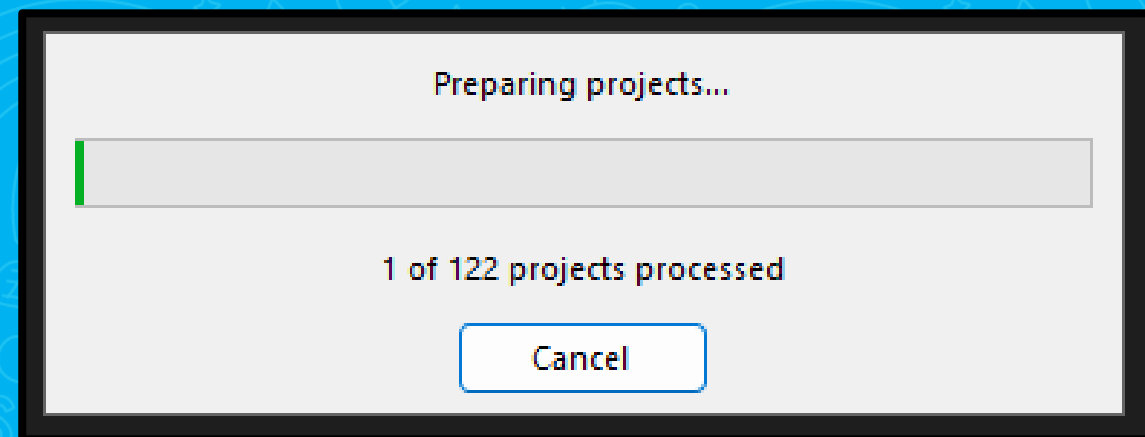


«Избыточный» анализ



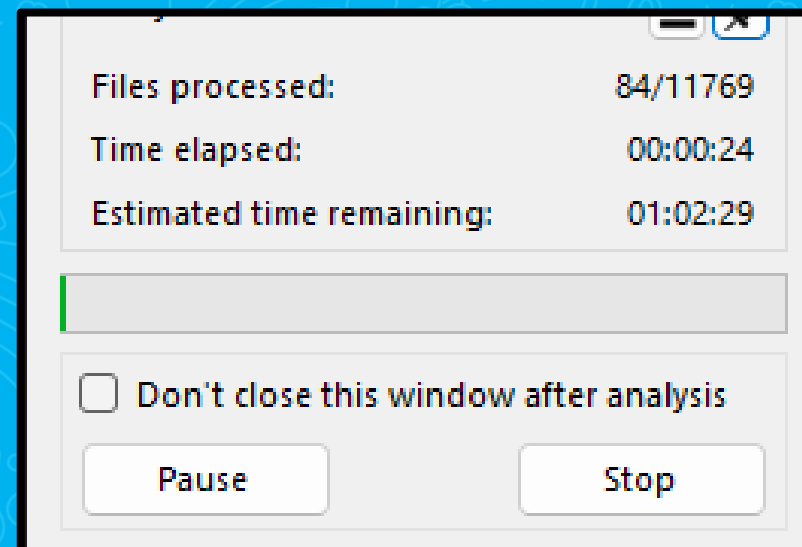
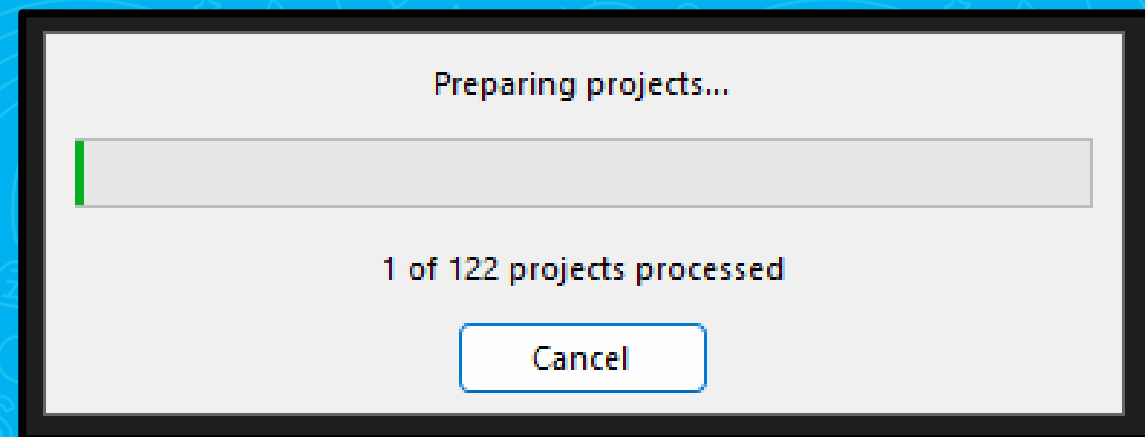
«Избыточный» анализ

- Лишние файлы, внешние библиотеки



«Избыточный» анализ

- Лишние файлы, внешние библиотеки
- **Возвращаемся к настройке!**

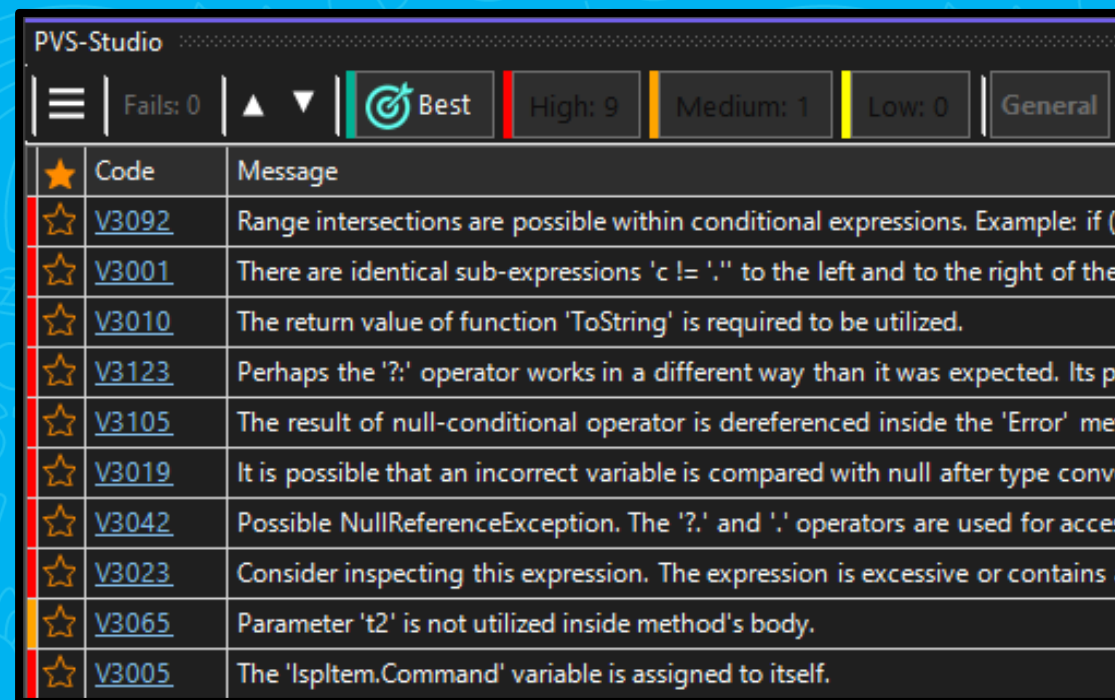


Не хватает диагностик

- Анализатор не идеален
- Но все решаемо!
- Пишем в поддержку

Как быстро попробовать?

- Написать проект самому?
- Взять опен-сурс?
- Использовать на целевом?
- Попробовать TOP 10!



The screenshot shows the PVS-Studio application window. At the top, there's a header bar with the title 'PVS-Studio'. Below it, a toolbar contains a menu icon, 'Fails: 0', a list of icons (a triangle, a circle with a dot, and a target icon), and a status bar showing 'Best', 'High: 9', 'Medium: 1', 'Low: 0', and a 'General' tab. The main area displays a table of 10 error messages, each with a star icon in the first column, a code in the second, and a message in the third.

★	Code	Message
★	V3092	Range intersections are possible within conditional expressions. Example: if (
★	V3001	There are identical sub-expressions 'c != '.' to the left and to the right of the
★	V3010	The return value of function 'ToString' is required to be utilized.
★	V3123	Perhaps the '?' operator works in a different way than it was expected. Its p
★	V3105	The result of null-conditional operator is dereferenced inside the 'Error' met
★	V3019	It is possible that an incorrect variable is compared with null after type conve
★	V3042	Possible NullReferenceException. The '?' and '.' operators are used for acces
★	V3023	Consider inspecting this expression. The expression is excessive or contains a
★	V3065	Parameter 't2' is not utilized inside method's body.
★	V3005	The 'Ispltem.Command' variable is assigned to itself.

**Устранение неисправностей при
работе PVS-Studio**



**Советы по повышению скорости
работы PVS-Studio**





Задавайте
вопросы

Q&A

Глеб Асламов
C# Developer & DevRel