# Метод совмещения результатов статического и динамического анализа для цикла разработки безопасного программного обеспечения

Мишечкин Максим Владимирович
mishmax@ispras.ru
Курмангалеев Шамиль Фаимович
kursh@ispras.ru

ИСП РАН

# Сложности для статического анализа

## Ошибки первого и второго рода из-за:

- использование виртуальных методов;
- использование вызовов функций по указателям на вычисляемый адрес;
- недостаточной точности построения карты памяти;
- …

## Необходимость ручной разметки предупреждений:

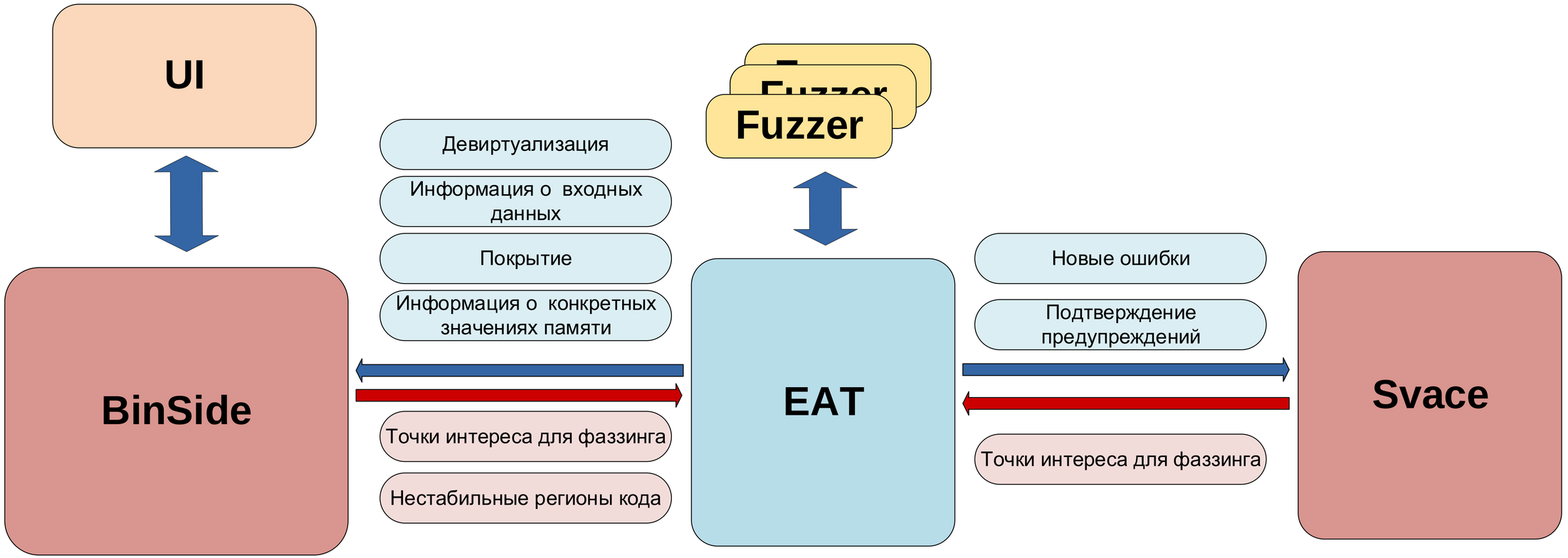
- разметка каждого предупреждения — это временные затраты;
- не полное понимание приоритета исправления найденных ошибок;
- нет гарантии, что человек правильно классифицирует ошибки;
- нет контекста на котором проявляется ошибка.

# Сложности для динамического анализа

- ограниченная эффективность выбора входных данных для мутации;
- нестабильные регионы кода, которые влияют на качество проводимых мутаций;
- ограниченное понимание влияния байт на покрытие;

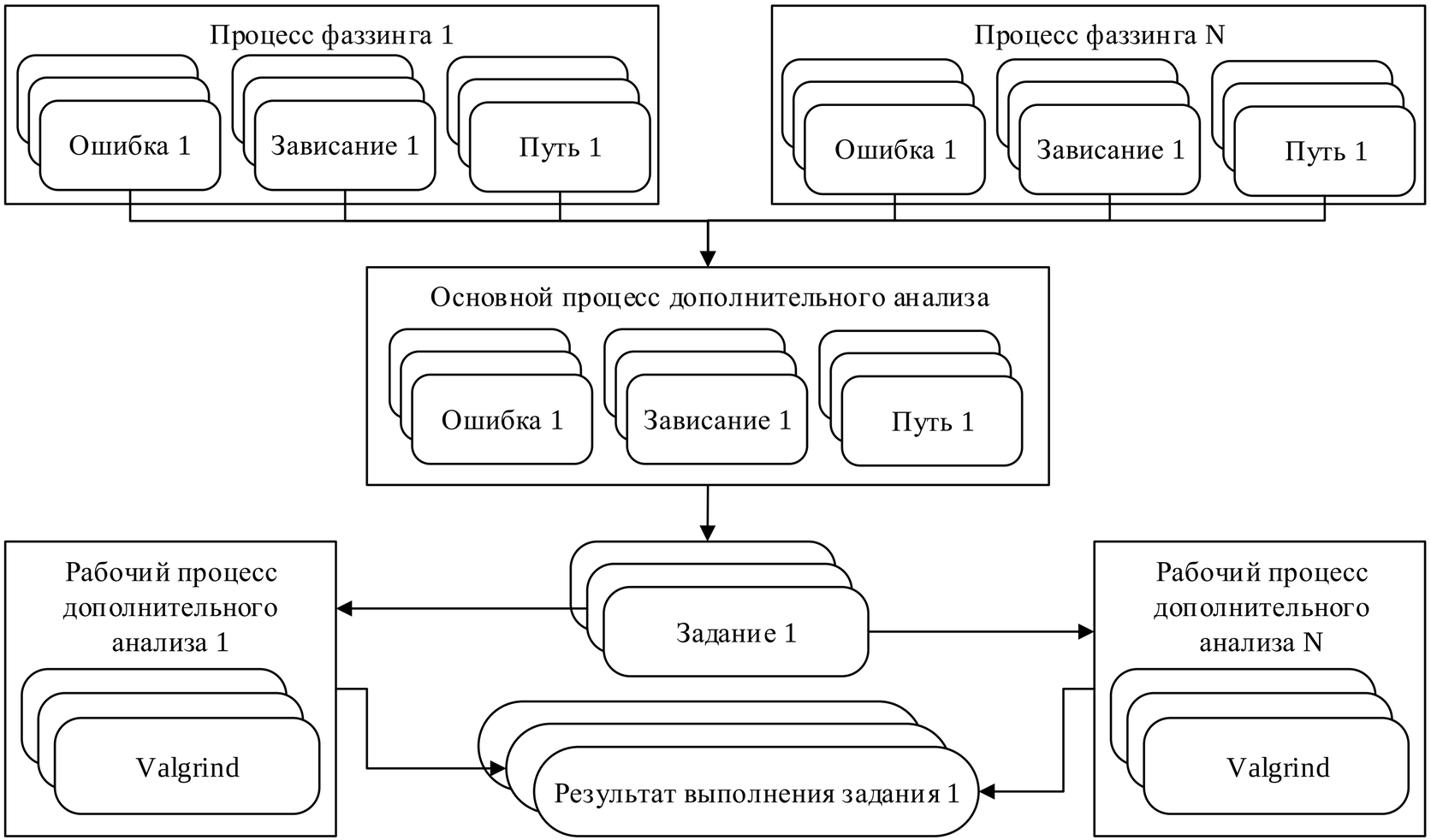
# Crusher

## Объединение статического и динамического анализа



# Crusher

## Модуль дополнительного анализа



# Crusher

## Интегрированные средства динамического анализа:

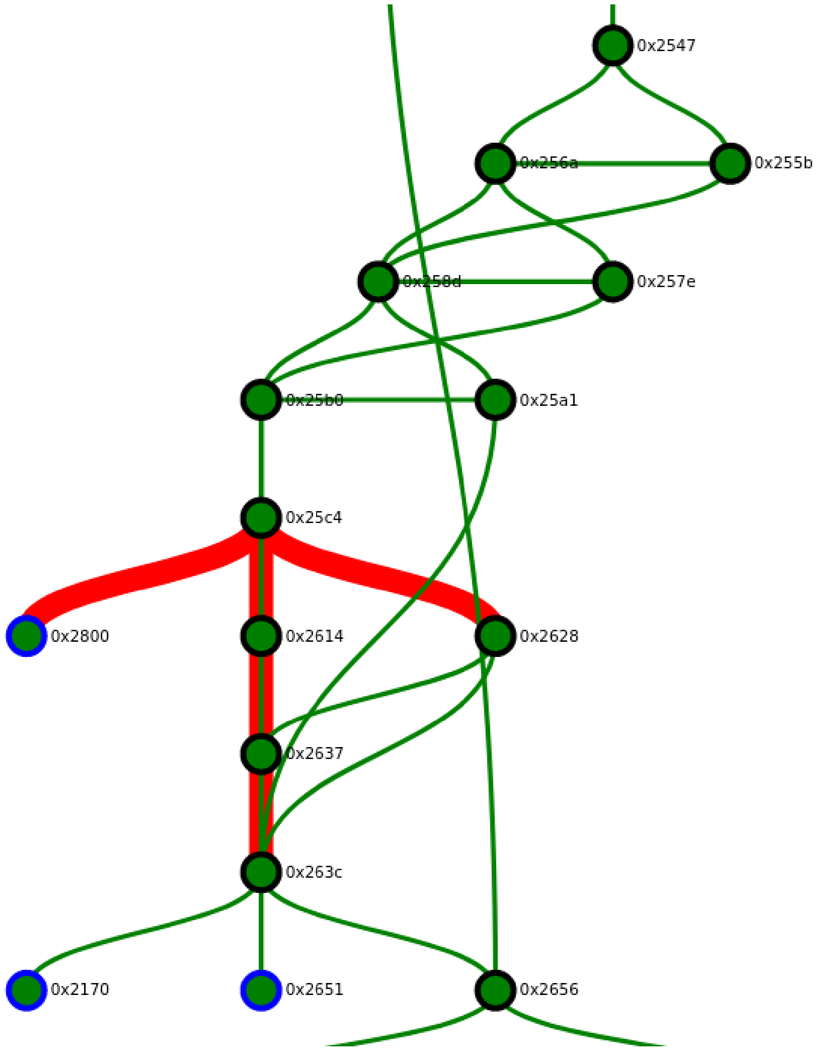
- Valgrind;
- Средства оценки критичности (exploitable, casr);
- DrMemory;
- QASan.

## Результаты расширенного анализа:

- Отчеты аварийных завершений для Svace;
- Подтверждение Svace Warnings;
- Lighthouse покрытие;
- Трассы для инструмента BinSide.

# Crusher

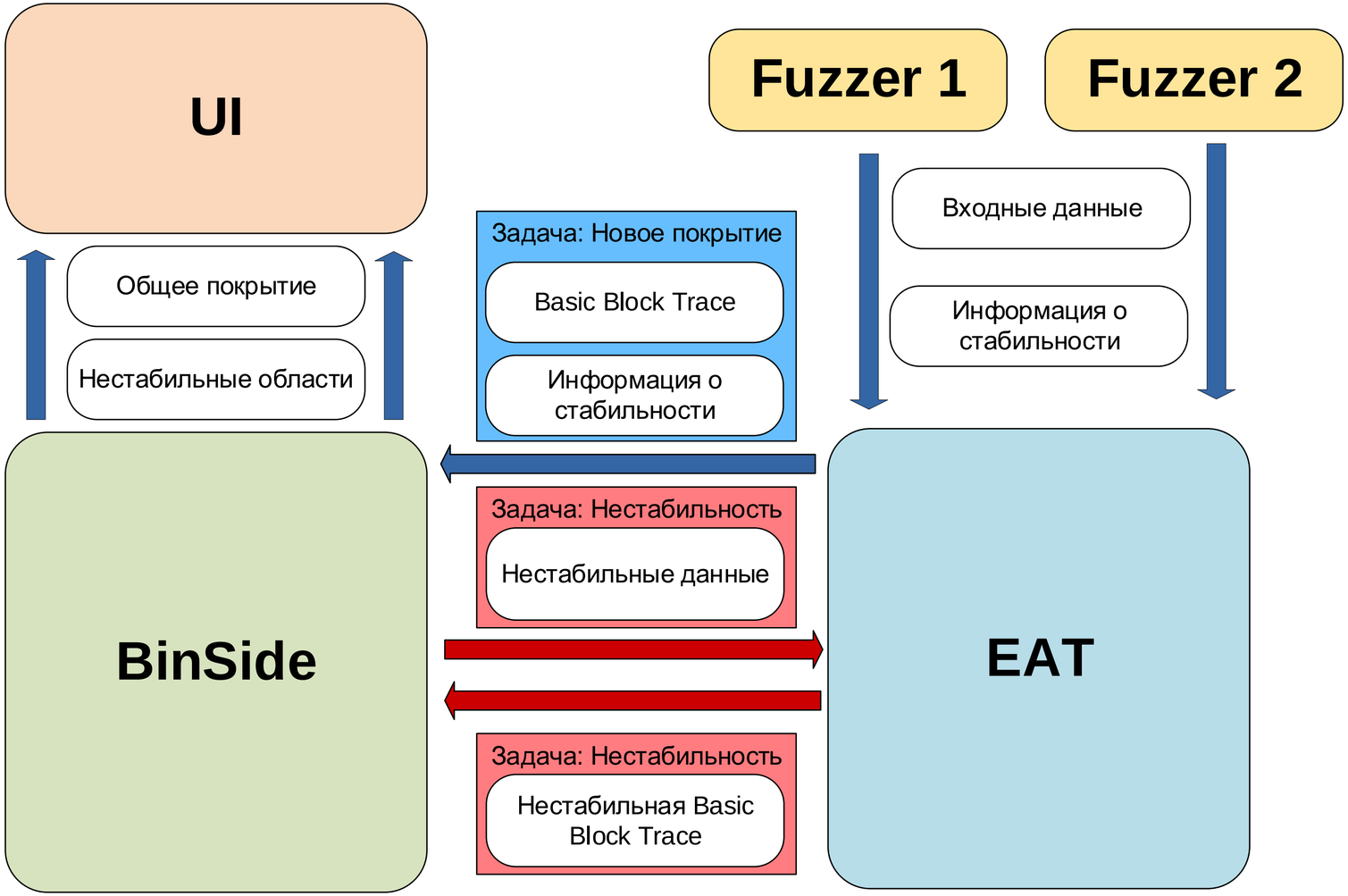
## Локализация нестабильного поведения в ПО




```
37          if (data[4] == 'f') {
38              i++;
39               int rand_number = dist(e);
40              if (rand_number % 2 == 0) {
41                i++;
42              } else {
43                i--;
44              }
45          }
```

# Crusher

## Локализация нестабильного поведения в ПО

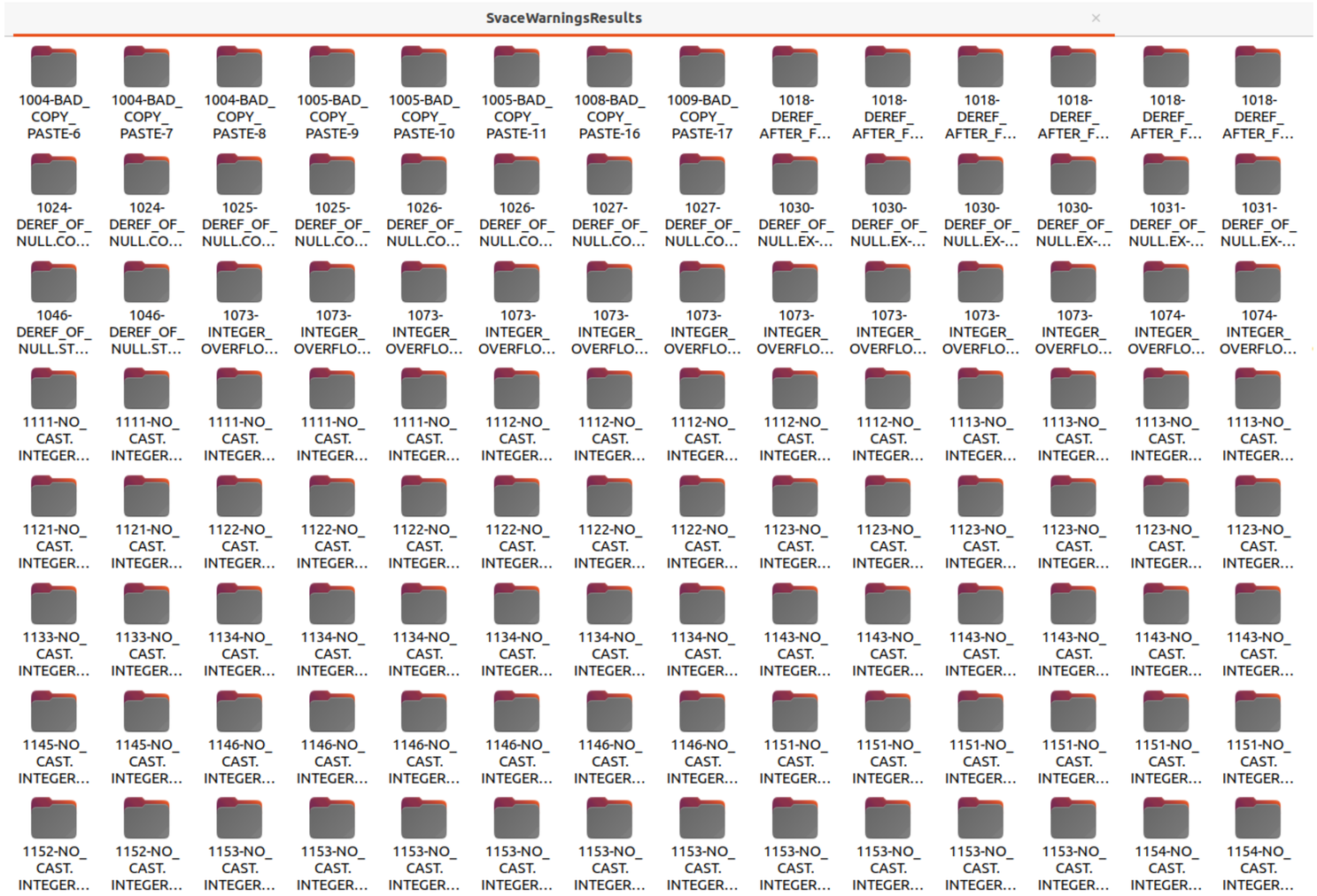


# Crusher

## Подтверждение предупреждений Svace

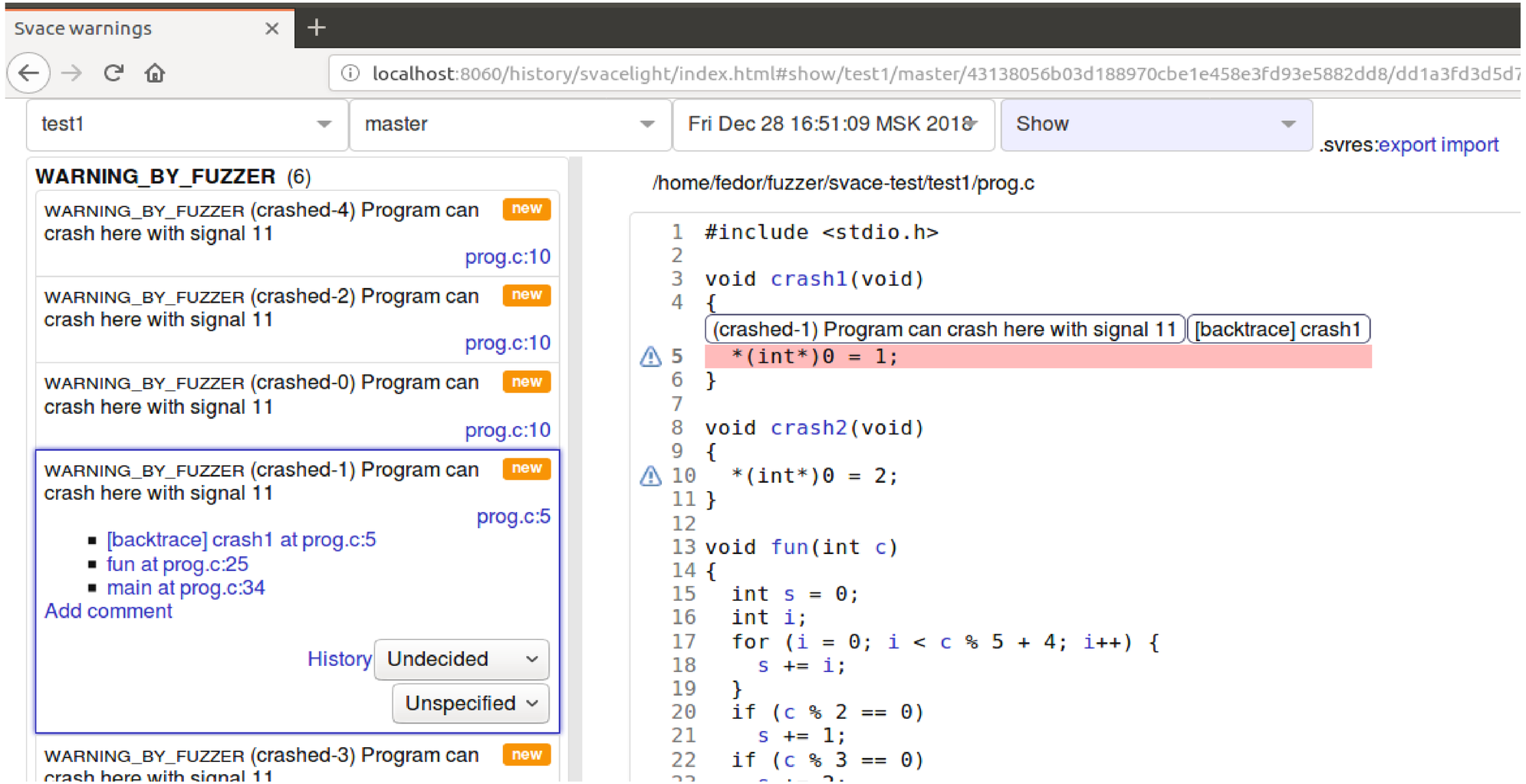
# Crusher

## Подтверждение предупреждений Svace (результаты NGINX)



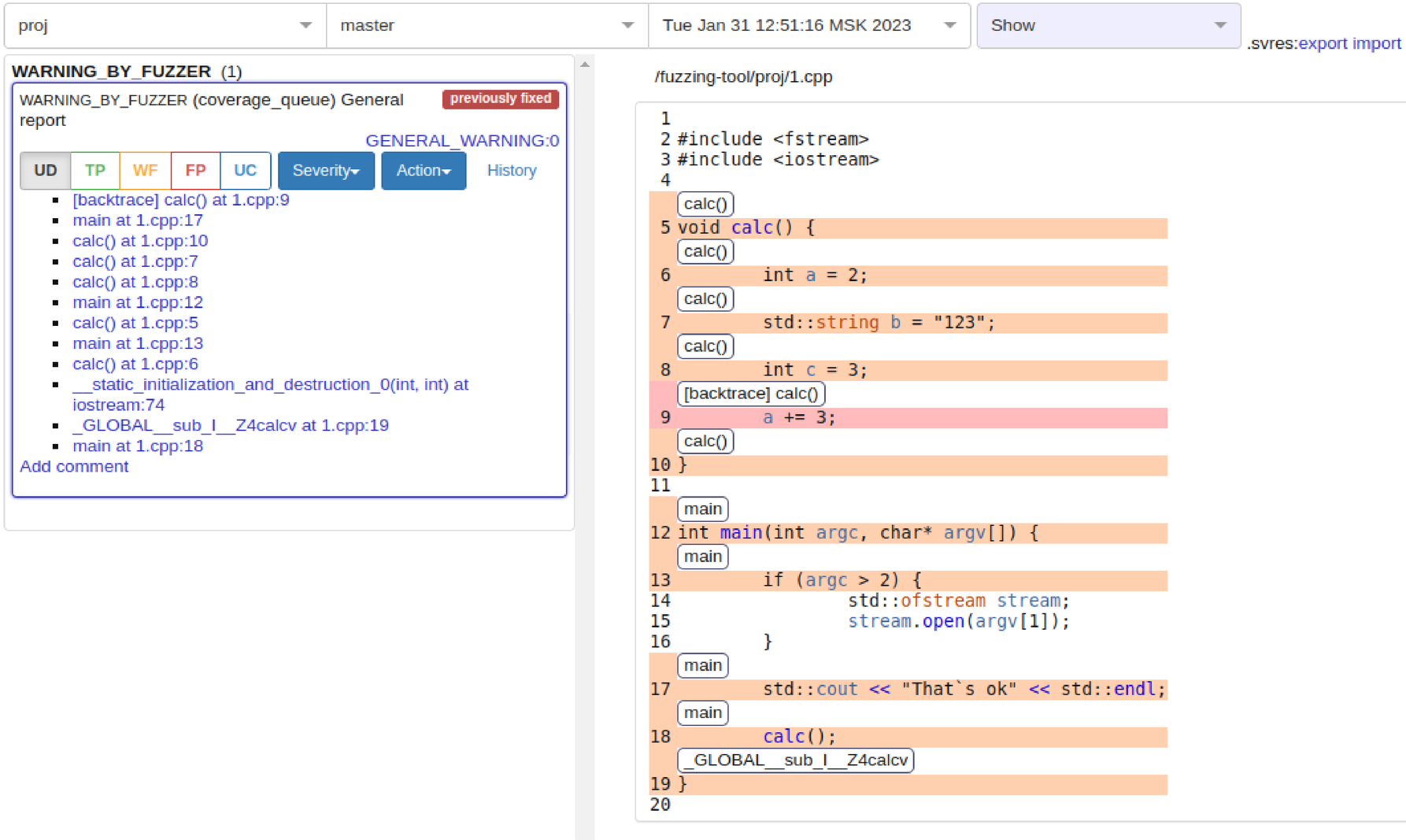
# Crusher

## Svace отчеты аварийных завершений



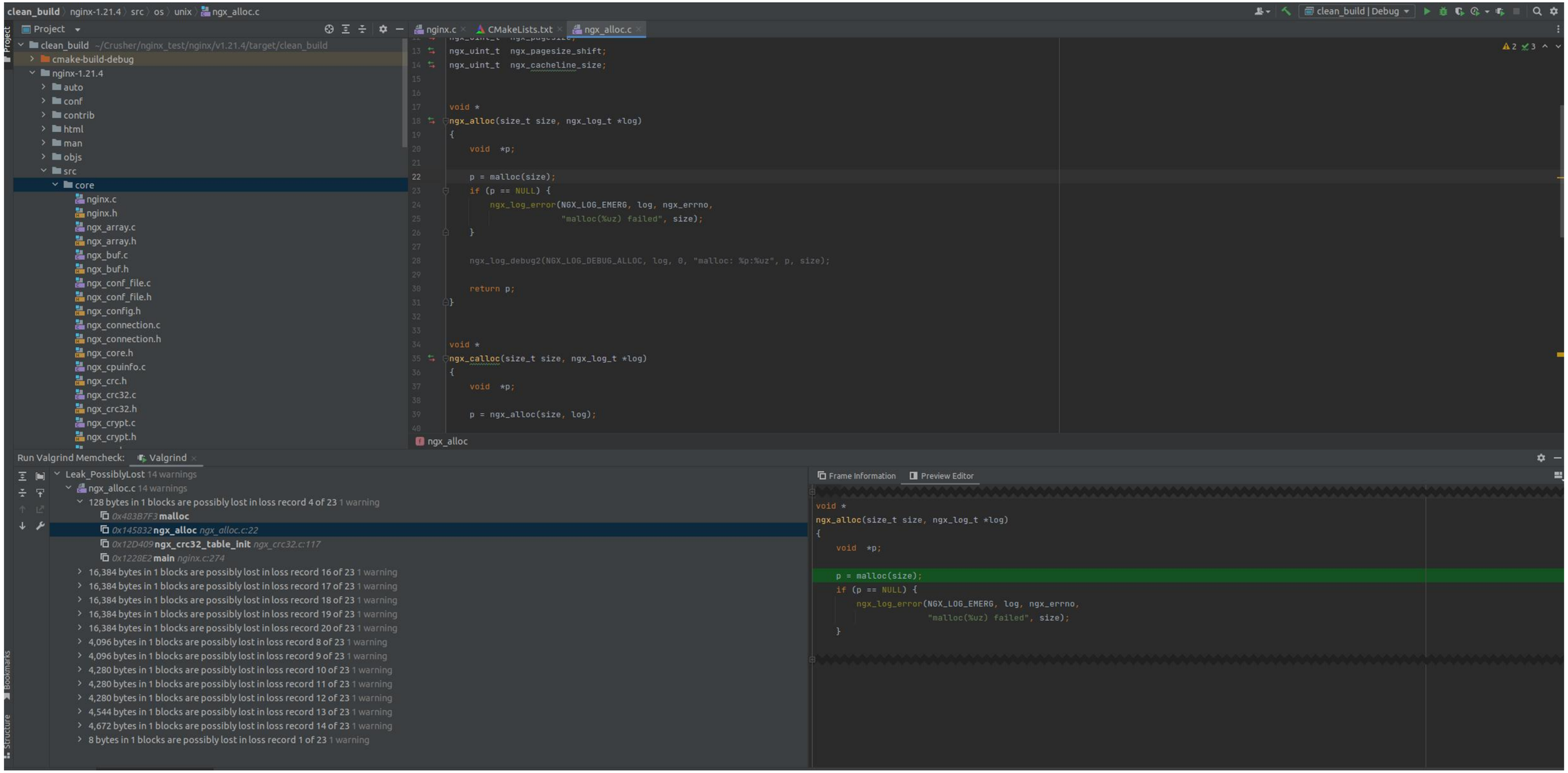
# Crusher

## Svace покрытие



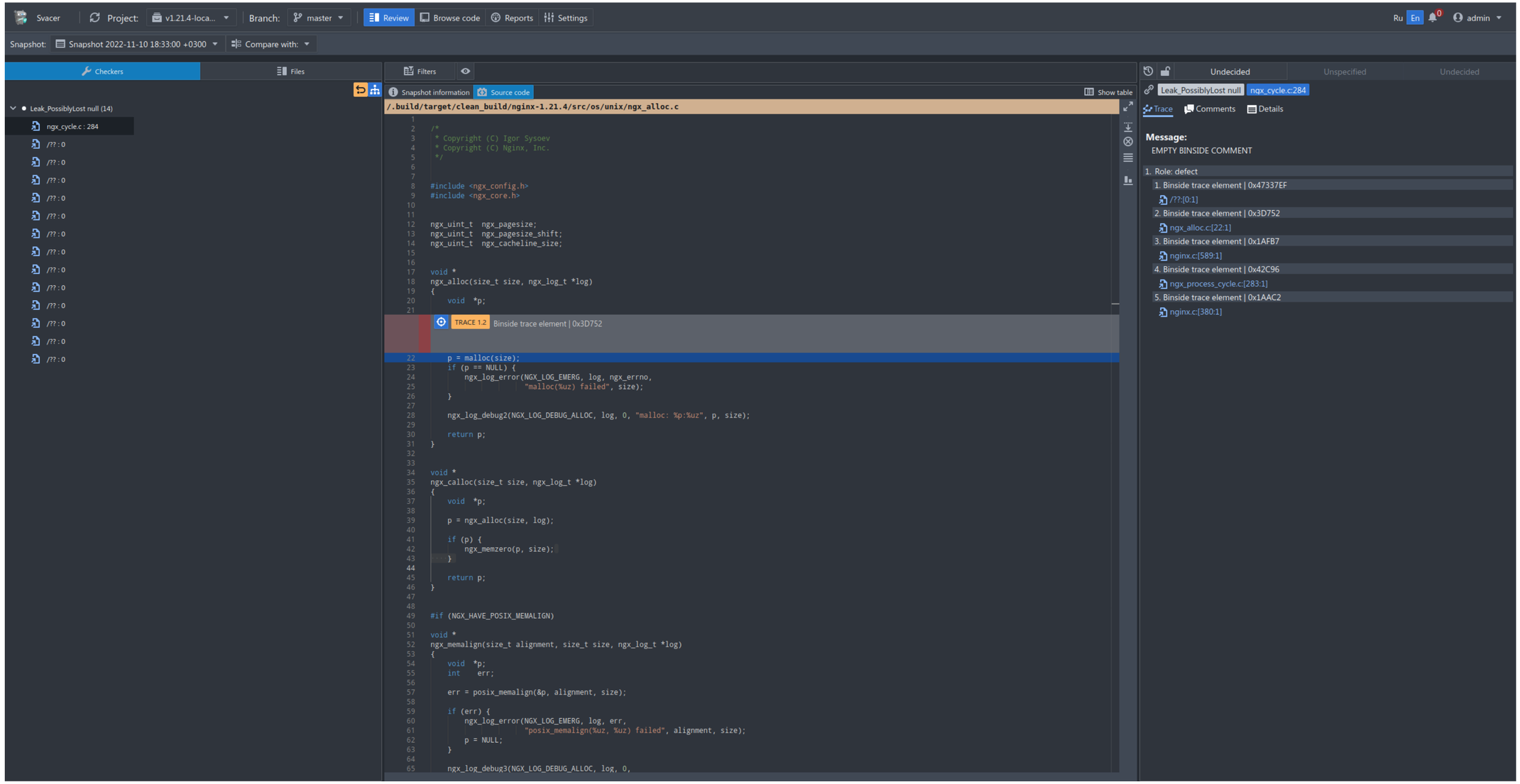
# Crusher

## Valgrind отчеты Clion



# Crusher

## Valgrind отчеты Svace



# Спасибо за просмотр

ИСП РАН