Десятая независимая научно-практическая конференция
«Разработка ПО 2014»

23 - 25 октября, Москва

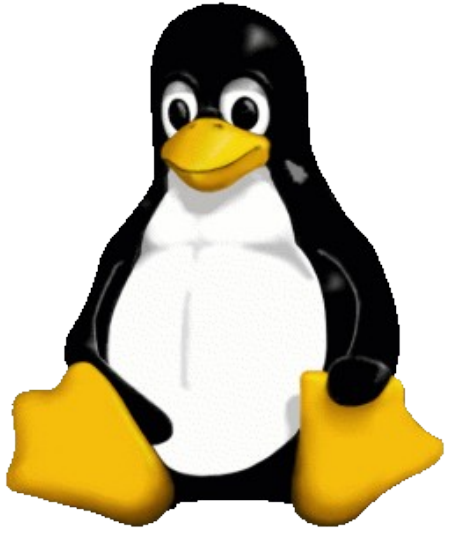

# Статическая верификация модулей ядра Linux: текущие достижения и перспективы

Евгений Новиков

ISP RAS
LinuxTesting.org

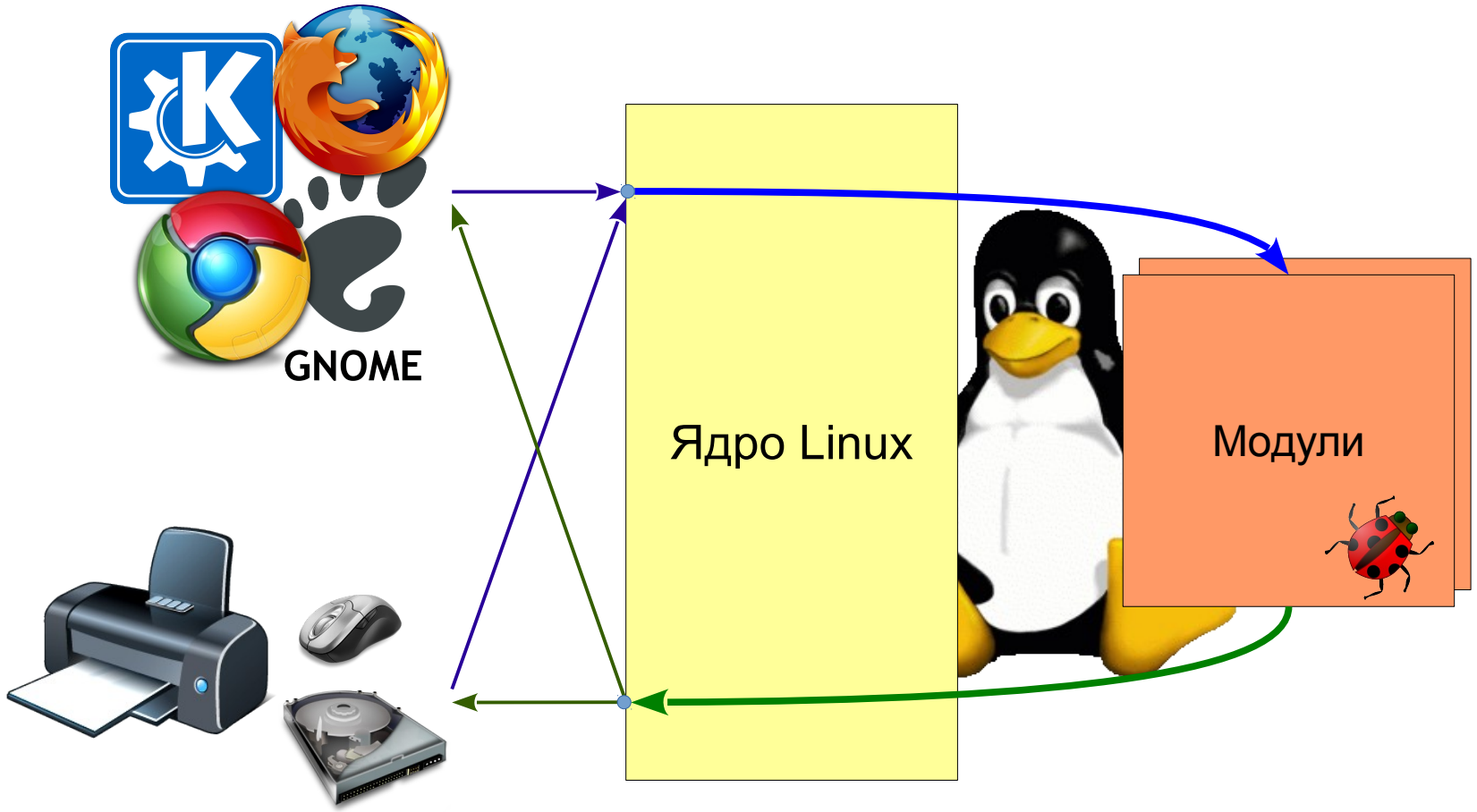
# Тестирование vs. статический анализ

| Тестирование | Статический анализ |
|---|---|
| Программа выполняется на определенных входных данных | Исходный код программы проверяется без ее реального выполнения |
| Проверка различных требований | Проверка ограниченного набора свойств |
| Отсутствие ложных сообщений об ошибках | Ложных сообщений об ошибках может быть достаточно много |
| Для хорошего покрытия требуются достаточно большие трудозатраты | Анализ обеспечивает хорошее покрытие, но может быть достаточно много пропусков ошибок |

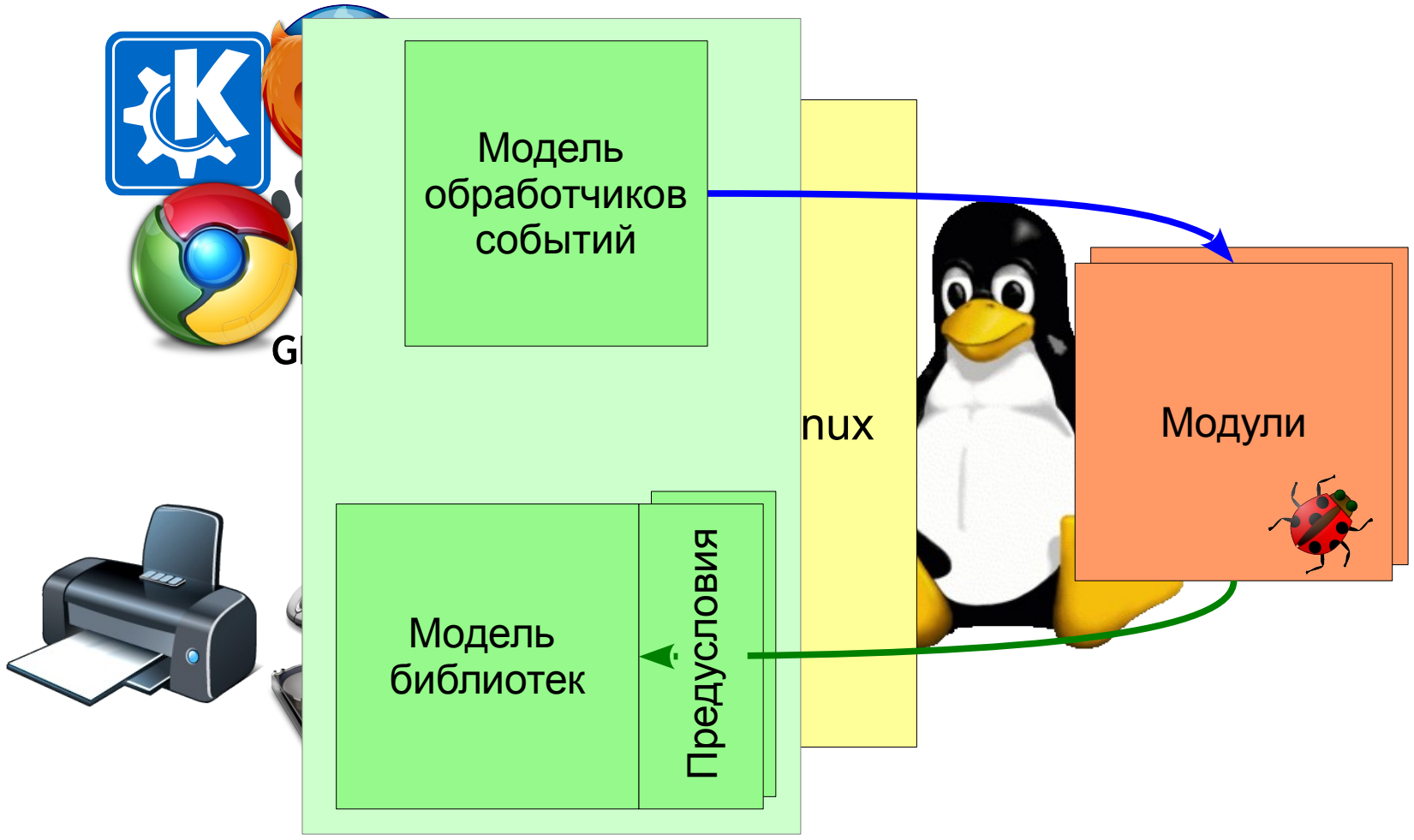



CRAY
XE6

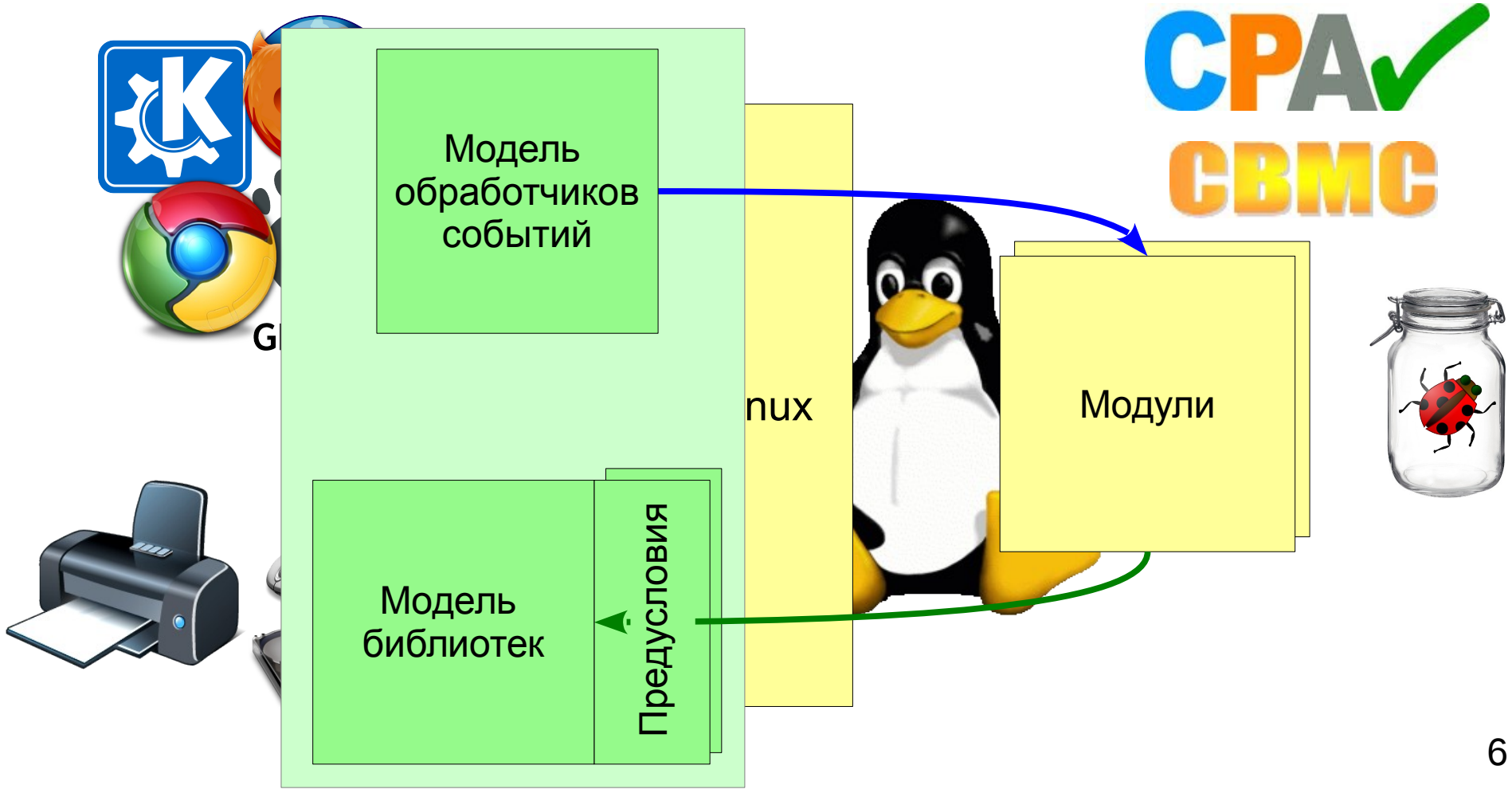
# Схема устройства и работы ядра Linux



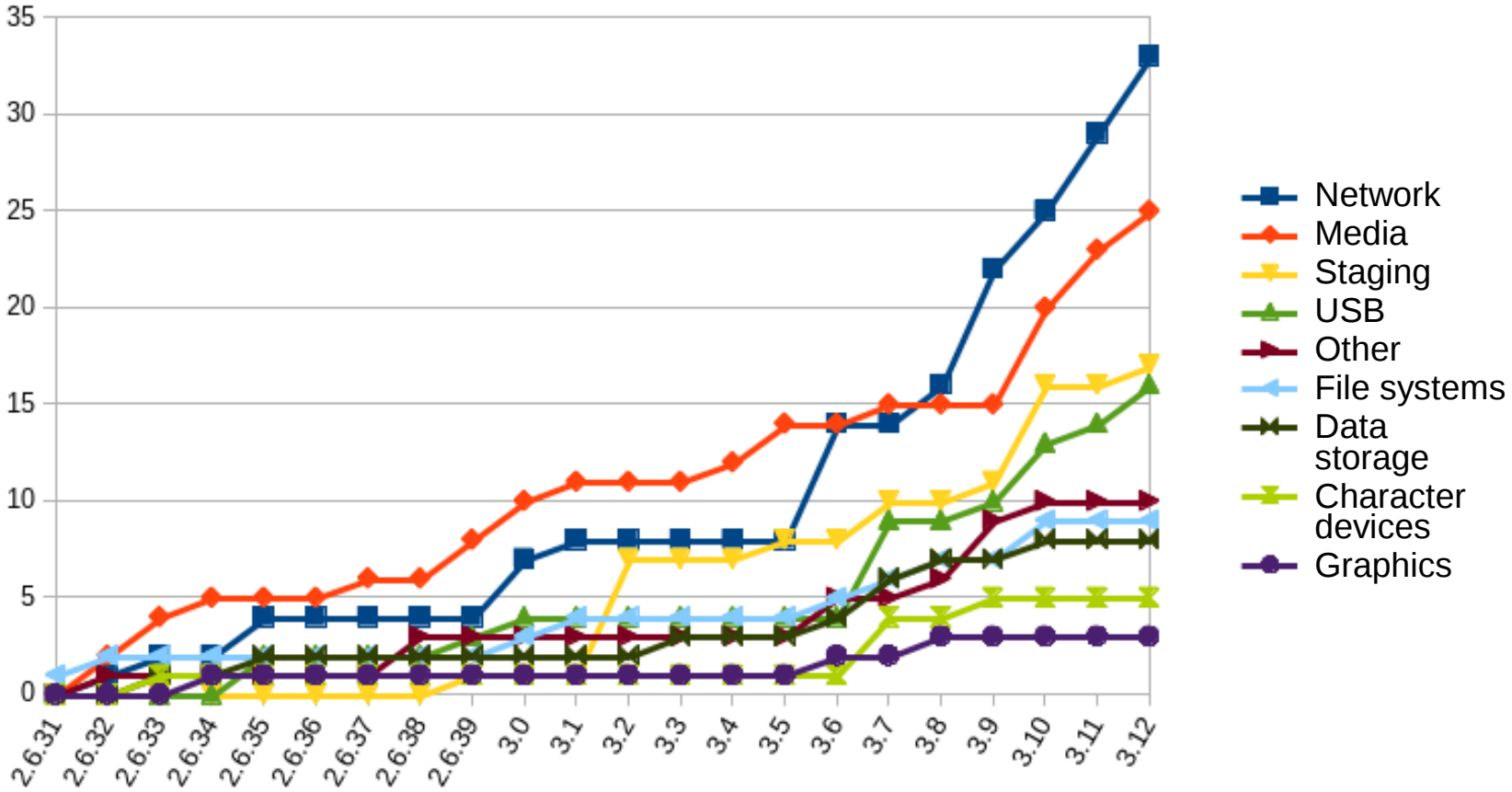
# Моделирование окружения



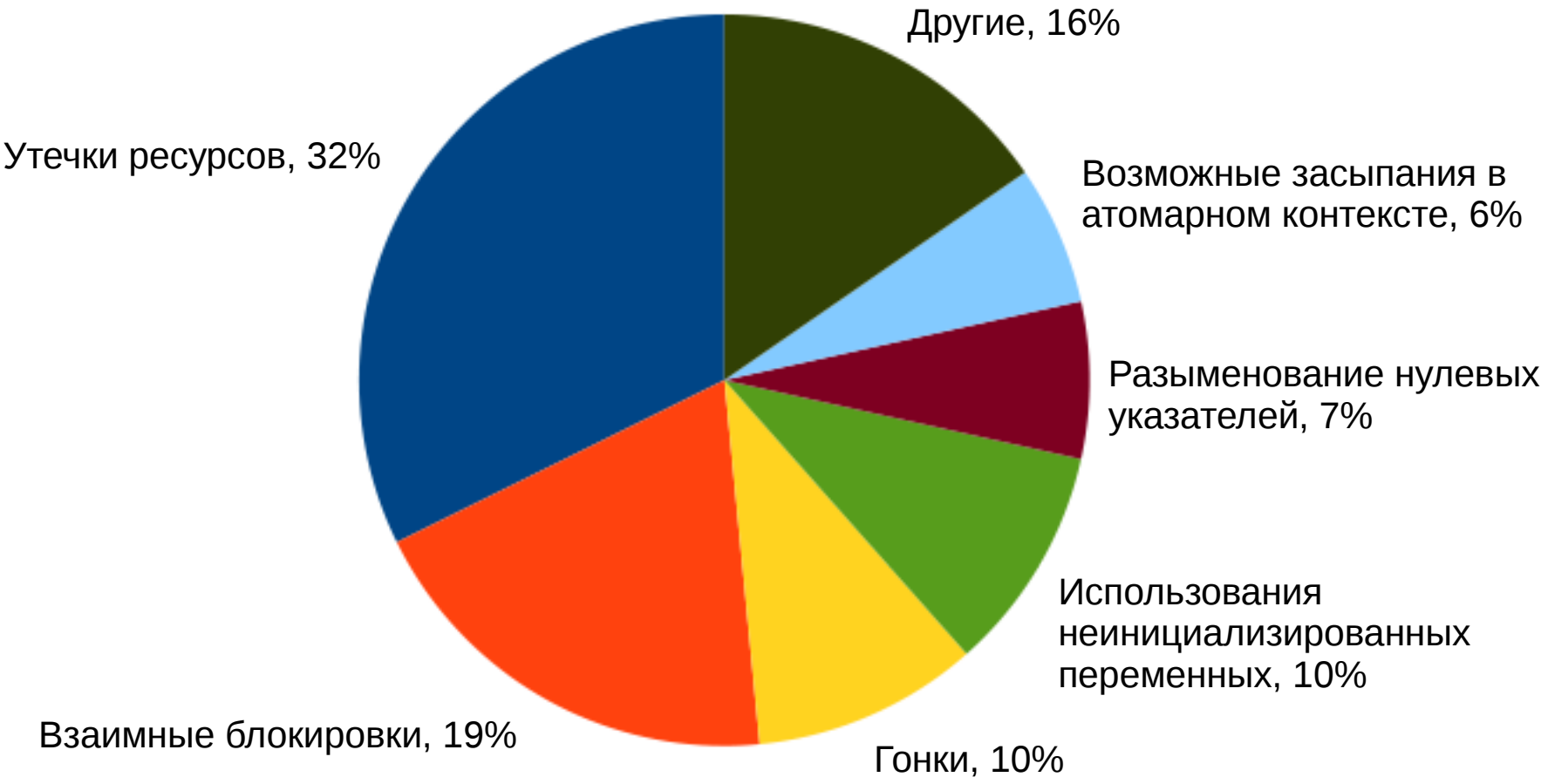
# Статическая верификация модулей



# Распределение выявленных ошибок



# Последствия выявленных ошибок



# Причины ложных сообщений об ошибках

| Выявленные ошибки  | Ложные сообщения об ошибках | | |
|---|---|---|---|
| | Неточная модель обработчиков событий | Неточная модель библиотек | Проблемы в инструменте верификации |
| 17% | 58% | 15% | 10% |

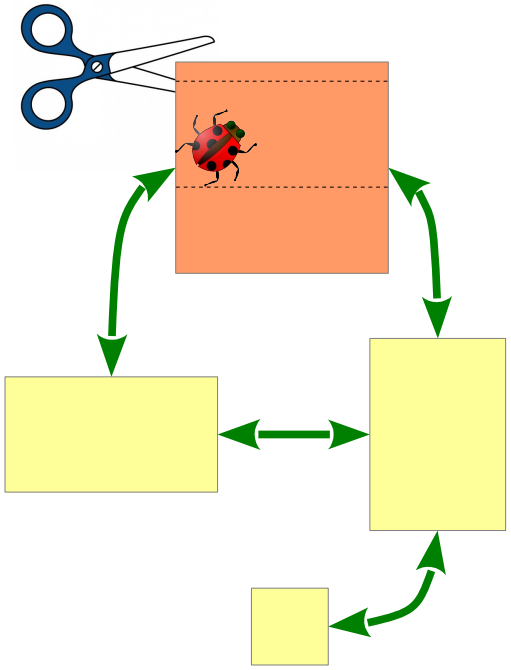
# Обнаружение/пропуск ошибок

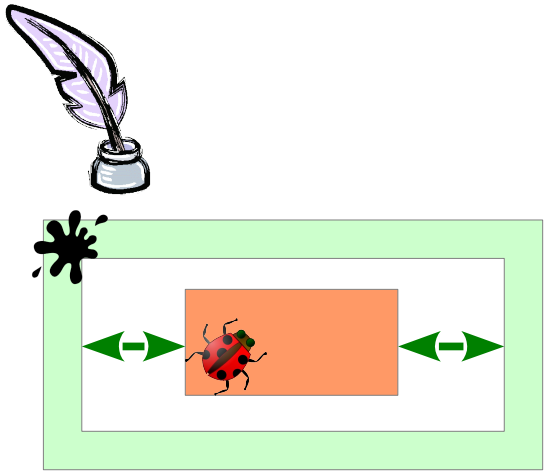
| Выявленные ошибки  | Пропуск ошибок | | |
|---|---|---|---|
| | Неточная модель обработчиков событий | Неточная модель библиотек | Проблемы в инструменте верификации |
| 49% | 21% | 15% | 15% |

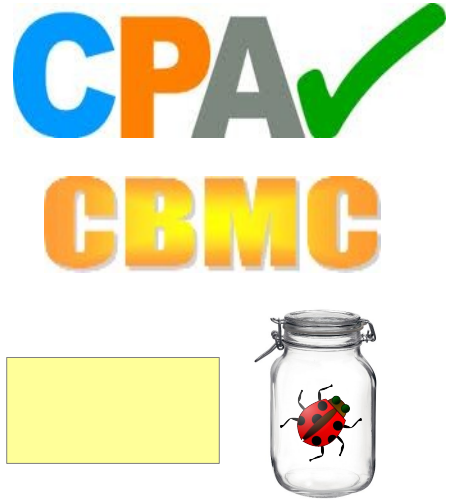
# Дальнейшие планы

- Разработка более точной модели окружения
- Использование более точных, быстрых и потребляющих меньшее количество памяти инструментов верификации
- Выявление и формализация новых правил корректного использования библиотек ядра
- Интеграция инструментов статической верификации в стандартный процесс разработки модулей ядра Linux

# Применение к другим программам







# Инструменты статической верификации

| Название инструмента | Организация-разработчик |
|---|---|
| BLAST 2.7.2 | ISP RAS, Russia |
| CBMC | University of Oxford, UK |
| CPAchecker | University of Passau, Germany |
| CPAlien | Brno University of Technology, Czech Republic |
| Cseq-Lazy, Cseq-MU | University of Southampton, UK |
| ESBMC 1.22 | University of Southampton, UK / Federal University of Amazonas, Brazil |
| FrankenBit | SEI, USA / University College Dublin, Ireland |
| LLBMC | Karlsruhe Institute of Technology, Germany |
| Predator | Brno University of Technology, Czech Republic |
| Symbiotic 2 | Masaryk University at Brno, Czech Republic |
| Threader | TU Munich, Germany |
| UFO | University of Toronto, Canada / SEI, USA |
| Ultimate Automizer / Kojak | University of Freiburg, Germany |