Тема: Разработка программного модуля для анализа программ на языках C и C++ на недекларированные возможности

Руководитель от кафедры: канд. техн. наук, доц. А. И. Кононова
Исполнитель ст. гр. ПИН-43 А. А. Уманский
Цель: Ускорение проведения сравнительного анализа статических и динамических трасс программ, написанных на C/C++
Задачи:

1. исследование предметной области;
2. сравнительный анализ существующих программных решений;
3. выбор языка и среды разработки;
4. разработка схемы данных ПМ АПНДВ;
5. разработка схемы алгоритма ПМ АПНДВ;
6. программирование ПМ АПНДВ;
7. отладка и тестирование ПМ АПНДВ;
8. разработка документации к ПМ АПНДВ;

Исследование предметной области

Таблица: До и после разработки ПМ АПНДВ

До разработки ПМ АПНДВ	После разработки ПМ АПНДВ
Проведение статического, динамического и сравнительного анализа проходило вручную	Проведение статического, динамического и сравнительного анализа проходит автоматически
Для проведения анализов нужно было вручную выбирать исследуемые файлы	Для проведения анализов, ПМ АПНДВ делает это автоматически
Динамический анализ включал в себя только вызовы функций	Динамический анализ включает в себя информацию о состоянии стека и регистров программы во время конкретного вызова

Обзор существующих решений

На сегодняшний день на рынке не существует решений аналогичных ПМ АПНДВ. Поэтому рассмотрим программы, которые можно использовать в качестве составных частей ПМ АПНДВ.

Таблица: Сравнительная таблица статических анализаторов

Свойства \ Название программы	Microsoft Application Inspector [1]	SCI Tools Understand [2]	GNU cflow [3]
Кросс-платформенность	Да	Да	Да
Открытость исходного кода	Да	Нет	Да
Препроцессирование кода C/C++	Нет	Да	Да
Представление препроцессорных директив как вызов функций	Нет	Нет	Да
Создание графа вызовов	Нет	Да	Да
Создание обратного графа вызовов	Нет	Да	Да
Бесплатность	Да	Нет	Да
Графический интерфейс	Нет	Есть	Нет

Обзор существующих решений

На сегодняшний день на рынке не существует решений аналогичных ПМ АПНДВ. Поэтому рассмотрим программы, которые можно использовать в качестве составных частей ПМ АПНДВ.

Таблица: Сравнительная таблица программ для динамического анализа

Свойства \ Название программы	GDB [4]	QEMU [5]
Кросс-платформенность	Да	Да
Открытость исходного кода	Да	Да
Возможность анализировать память	Да	Да
Возможность программно управлять	Да	Да
Возможность создавать собственные команды	Да	Нет
Возможность удаленной отладки	Да	Нет
Бесплатность	Да	Да
Графический интерфейс	Есть	Есть

Выбор языка программирования

Таблица: Сравнительная таблица языков программирования

Свойства \ Язык	Nim [6]	Python [7]	Perl [8]	C/C++
Сверхвысокоуровневость	Да	Да	Да	Нет
Компилируется в машинный код	Да	Нет	Нет	Да
Количество функции в стандартной библиотеке	5585	638	1338	1224
Портируемость	Есть	Есть	Есть	Есть, но неудобная
Встроенная генерация документации	Есть	Есть	Есть	Нет
Статическая типизация	Есть	Нет	Нет	Есть
Автоматическое управление памятью	Есть	Есть	Есть	Есть
Обобщенное программирование	Есть	Есть	Есть	Есть
Мета-программирование	Есть	Есть	Есть	Есть
Опыт использования	Есть	Есть	Нет	Есть

Выбор среды разработки

Для разработки на Nim существует несколько IDE и огромное количество текстовых редакторов, часть которых рассмотрим ниже:

Таблица: Сравнительная таблица IDE и редакторов кода

Свойства \ IDE/Редактор	Aporia [9]	Atom [10]	Sublime Text [11]	Visual Studio Code [12]	Vim [13]
Поддержка плагинов	Нет	Да	Да	Да	Да
Требователен к ресурсам	Нет	Да	Нет	Да	Нет
Имеет продвинутую систему редактирования текста	Нет	Нет	Нет	Нет	Да
Кросс-платформенность	Есть	Есть	Есть	Есть	Есть
Может работать без GUI	Нет	Нет	Нет	Нет	Да
Восстановление после сбоев	Нет	Есть	Есть	Есть	Есть
Возможность выделять ключевые слова с помощью регулярных выражений	Нет	Есть	Есть	Есть	Есть
Опыт использования	Нет	Нет	Есть	Есть	Есть

Схема данных

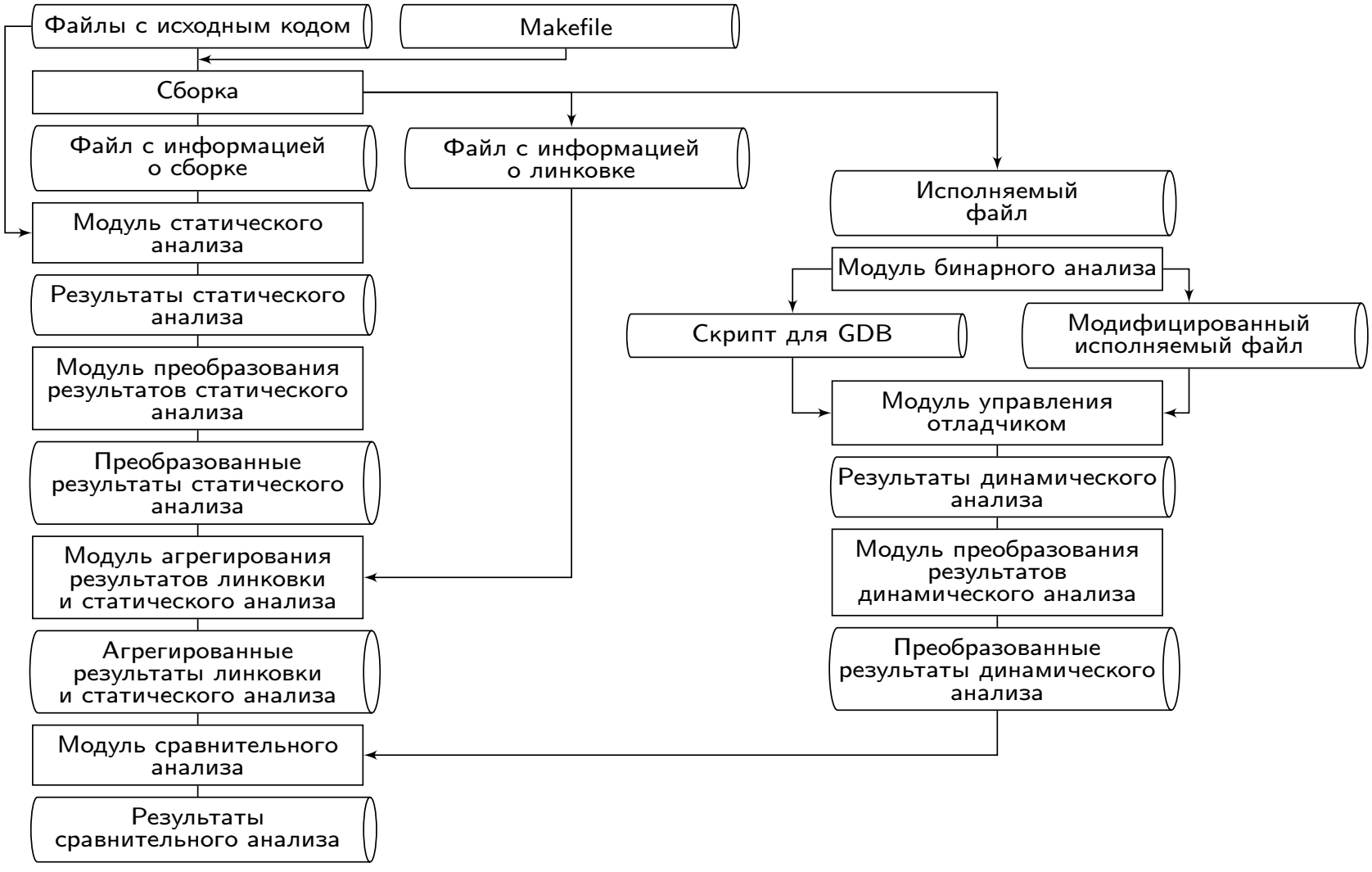

Схема алгоритма

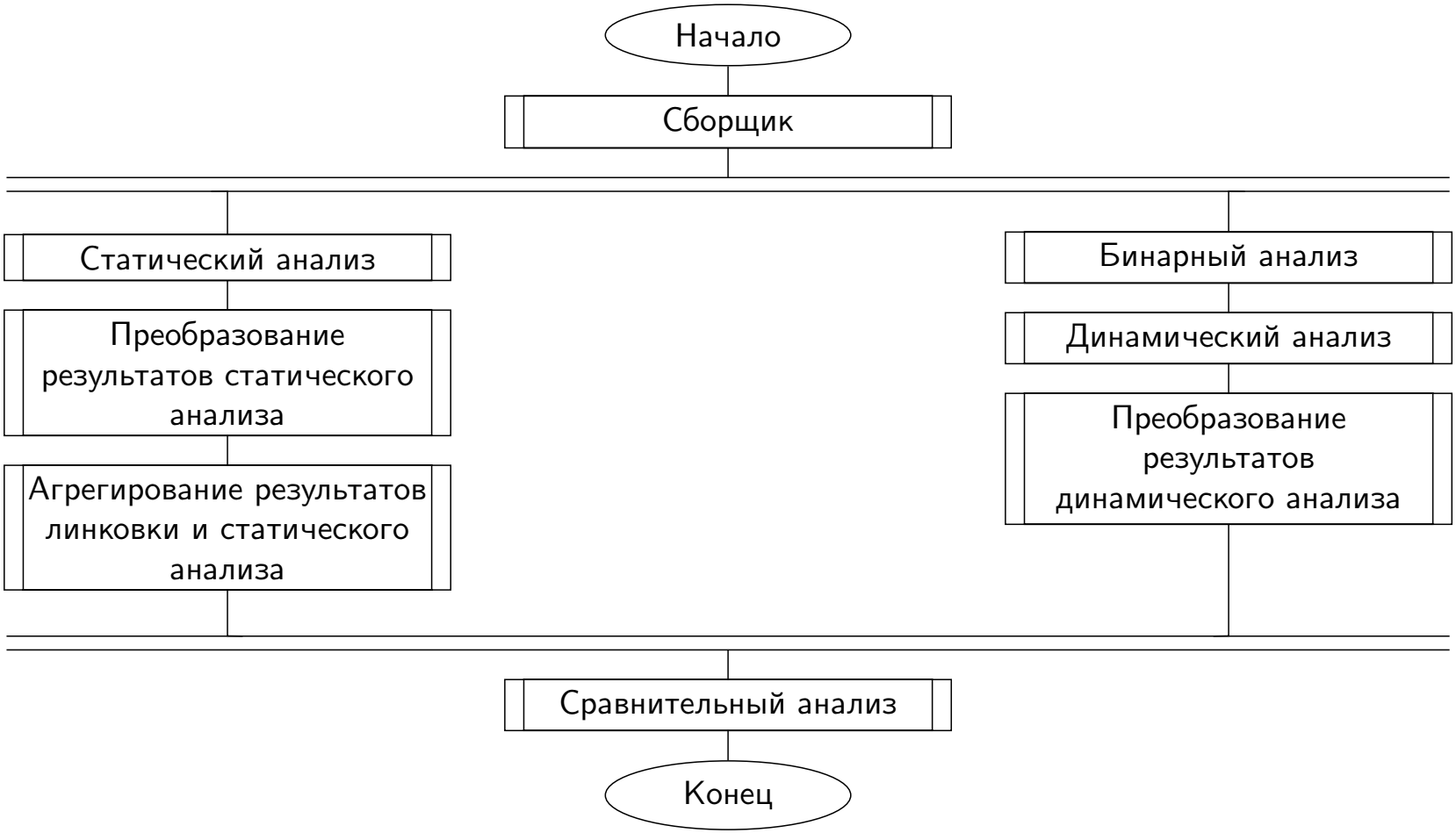

					СХЕМА АЛГОРИТМА ПМ АПНДВ		
					Программный модуль «анализа программ на языках C и C++ на недекларированные возможности»	Лит.	Масса / Масштаб
Изм	Лист	№ докум.	Подпись	Дата			1 / 1 : 1
Разраб.						Лис 6	Листов 11
Провер.							
Т. Контр.						НИУ «МИЭТ»	
Реценз.							
Н. Контр.							
Утверд.							

Ползовательский интерфейс

Пользователь будет управлять ПМ АПНДВ с помощью консольного интерфейса.

Апробация

ПМ АПНДВ готовится к внедрению на предпириятии ООО Фирма «Анкад»

Результаты работы

1. исследована предметная область;
2. проведен сравнительный анализ существующих программных решений;
3. выборан язык и среда разработки;
4. разработана схема данных ПМ АПНДВ;
5. разработана схема алгоритма ПМ АПНДВ;
6. запрограммирован ПМ АПНДВ;
7. проведена отладка и тестирование ПМ АПНДВ;
8. разработана документации к ПМ АПНДВ;

Ссылки I

Microsoft. — Application Inspector [Текст]. /. — Microsoft. — 2019. — URL: https://github.com/microsoft/ApplicationInspector.

scitools. — Features [Текст]. /. — scitools. — URL: https://scitools.com/features/.

Позняков, С. — GNU cflow [Текст]. /. — С. Позняков. — URL: https://www.gnu.org/software/cflow/.

Free Software Foundation, I. — GNU Debugger [Текст]. /. — I. Free Software Foundation. — URL: https://www.gnu.org/software/gdb/.

Bellard, F. — QEMU [Текст]. /. — F. Bellard. — URL: https://www.qemu.org/.

Rumpf, A. — Nim [Текст]. /. — A. Rumpf. — URL: https://nim-lang.org/.

Rossum, G. van. — python [Текст]. /. — G. van Rossum. — URL: https://www.python.org/.

Ссылки II

Wall, L. — Perl [Текст]. /. — L. Wall. — URL: https://www.perl.org/.

Aporia. — [Текст]. — URL: https://github.com/nim-lang/Aporia/.

Atom. — [Текст]. — URL: https://atom.io/.

Sublime Text. — [Текст]. — URL: https://www.sublimetext.com/.

Visual Studio Code. — [Текст]. — URL: https://code.visualstudio.com/.

Vim. — [Текст]. — URL: https://www.vim.org/.