О Т З Ы В

на автореферат кандидатской диссертации «Методы декомпиляции объектного кода Delphi», представленной Михайловым Андреем Анатольевичем на соискание учёной степени кандидата технических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей»

Представленная работа посвящена разработке методов декомпиляции и анализа объектного кода Delphi. Существует масса приложений, разработанных в среде Delphi. Многие предприятия в настоящее время стараются использовать C++, C#, Java и другие современные языки и системы. В этой связи становится актуальной задача декомпиляции программного кода, созданного с помощью среды Delphi, его анализа и создания программного средства, позволяющего изучать, анализировать и поддерживать унаследованное программное обеспечение, содержащее в своём составе скомпилированные модули Delphi.

Следует отметить практическую значимость проделанной работы. Предложенные методы использованы в созданном программном обеспечении – декомпиляторе объектных файлов Delphi, для которого имеется свидетельство о регистрации программ для ЭВМ. Применимость результатов исследования подтверждается актом внедрения.

Основные результаты работы апробированы на всероссийских и международных конференциях, а также опубликованы в периодических изданиях, в том числе рекомендованных ВАК и индексируемых в международных базах, что позволяет судить о высокой квалификации автора в исследуемой области.

По результатам ознакомления с авторефератом диссертации сформулированы следующие замечания:

1. На стр. 7 содержится утверждение о том, что «задача декомпиляции становится не проще задачи трансляции». Трансляция в широком смысле – это перевод программы с одного формального языка (например, языка программирования высокого уровня) на другой (чаще всего машинный код). При этом в некоторых источниках рассматриваемые задачи декомпиляции сами по себе рассматриваются как задачи обратной трансляции, т.е. подмножество трансляции. В узком смысле под трансляцией обычно понимают перевод ассемблерного кода в машинный код. В любом случае, обратная задача является заведомо более сложной, чем прямая ввиду утраты значительной части информации, содержащейся в исходном коде.

2. Ценная информация для повышения качества восстановления исходного кода программы может быть получена при исследовании компилятора, с помощью которого выполнялась генерация объектного кода. В результате такого исследования могут быть выявлены некоторые характерные для компилятора шаблоны, на основании которых код восстанавливается более точно (их можно рассматривать как некие вспомогательные эвристики на этапе оптимизации). Исходя из автореферата, данный вопрос в рассматриваемой работе не затронут, предлагаемые методы основываются только на анализе управляющего графа.

3. На стр. 14 автореферата указано, что четвертая глава диссертации посвящена описанию применения методов декомпиляции в задаче визуализации управляющего графа. Также утверждается, что задача декомпиляции кода для целевой платформы x86 не всегда выполнима. Из текста автореферата неочевидно, для чего, исходя из заявленной темы, требуется решать задачу визуализации управляющего графа, и как предложенный алгоритм раскладки графа применяется в созданном декомпиляторе. Кроме того, в качестве научной новизны работы заявлен только метод декомпиляции кода CIL (машинного кода виртуальной машины .NET). Вместе с тем упоминаются сложности с декомпиляцией машинного кода x86. Полезно было более подробно рассказать о результатах, полученных для x86, если такая задача решалась в рамках данного исследования.

К сожалению, объем автореферата не позволяет увидеть конкретные результаты декомпиляции реального кода. Кроме того, с учётом высокой практической значимости работы интерес представляли бы сведения о планах реализации её результатов в виде доступного широкому кругу пользователей программного продукта (поскольку сама по себе регистрация некоторых модулей ещё не означает последующей их коммерциализации).

Перечисленные замечания не снижают теоретической и высокой практической ценности представленной работы, выполненной на актуальную тему и содержащей научную новизну.

Считаем, что диссертация Михайлова Андрея Анатольевича соответствует паспорту специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей» и требованиям, предъявляемым к кандидатским диссертациям, а её автор заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.11 – «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

ФГБОУ ВО «Иркутский национальный исследовательский технический университет»: 664074, г. Иркутск, ул. Лермонтова, 83; http://www.istu.edu

_____ Дорофеев Андрей Сергеевич, к.т.н., доцент, заведующий кафедрой вычислительной техники

тел.: (3952)40-51-63, e-mail: dorbaik@istu.edu

_____ Ипполитов Александр Александрович, к.т.н., доцент кафедры вычислительной техники

тел.: (3952)40-51-07, e-mail: ippolitow@mail.ru

Подпись Дорофеев, Ипполитов
ЗАВЕРЯЮ
Общий отдел ФГБОУ ВО «ИРНИТУ»