«УТВЕРЖДАЮ»

Директор Федерального государственного бюджетного учреждения науки
Института динамики систем и теории управления имени В.М. Матросова СО РАН,
академик Бычков Игорь Вячеславович

«06» сентября 2017 г.

ЗАКЛЮЧЕНИЕ
Федерального государственного бюджетного учреждения науки
Института динамики систем и теории управления
имени В.М. Матросова Сибирского отделения Российской академии наук

Диссертация **«Методы декомпиляции объектного кода Delphi»** выполнена в Федеральном государственном бюджетном учреждении науки Институте динамики систем и теории управления имени В.М. Матросова Сибирского отделения Российской академии наук (ИДСТУ СО РАН). В период подготовки диссертации соискатель **Михайлов Андрей Анатольевич** работал в ИДСТУ СО РАН программистом, младшим научным сотрудником в лаборатории 4.1. Комплексных информационных систем. В 2011 г. Михайлов А.А. окончил Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Иркутский государственный университет», Институт математики экономики и информатики (ИМЭИ ИГУ), специальность – «Математическое обеспечение и администрирование информационных систем».

Сведения о сданных кандидатских экзаменах подтверждаются справкой об обучении № 15308-08-6525/06о от 06.09.2017, выданной Федеральным государственным бюджетным учреждением науки Институтом динамики систем и теории управления имени В.М. Матросова Сибирского отделения Российской академии наук.

Научный руководитель – к.т.н, доцент Хмельнов Алексей Евгеньевич, первый заместитель директора по информатизации ИДСТУ СО РАН.

По итогам обсуждения принято следующее заключение:

Диссертация А.А. Михайлова посвящена разработке методов и программных средств декомпиляции объектного кода Delphi.

Исследования по теме диссертационной работы проводились автором в период 2011 – 2017 гг. в рамках проекта СО РАН IV.38.2.3. «Новые методы, технологии и сервисы обработки пространственных и тематических данных, основанные на декларативных спецификациях и знаниях», а также научного проекта РФФИ № 15-37-20042 мол_а_вед.

Актуальность темы диссертации. Для разработки большинства сложных программных систем часто используются готовые компоненты, предоставляемые в виде скомпилированных модулей. Такой подход существенно сокращает время и стоимость создания программного обеспечения. С другой стороны, наличие сторонних модулей уменьшает надежность программного обеспечения и его информационную безопасность из-за возможного наличия уязвимостей, способствующих успешным атакам на информационную систему. Кроме того, сторонние компоненты могут содержать ошибки, устранение которых может быть затруднено из-за невозможности связаться с разработчиком, утраты разработчиком исходных кодов и т.д. В некоторых случаях может потребоваться доработка сторонних модулей, исходные тексты которых отсутствуют.

Среди объектных файлов особое место занимают файлы DCU, используемые компиляторами различных версий Delphi. С одной стороны, такие файлы технически можно отнести к объектным файлам, поскольку в дальнейшем с использованием редактора связей из них собирается загрузочный модуль. С другой стороны, файлы DCU содержат больше сведений, чем типичные объектные файлы. Файл DCU может полностью заменить исходный текст для той версии компилятора, при помощи которой он был создан. Этой особенностью активно пользуются разработчики программных модулей, которые часто распространяют их в формате DCU без предоставления исходных текстов, в особенности тогда, когда это делается на коммерческой основе. В том случае, когда разработчик прекращает развитие своих программных модулей, отсутствие исходных текстов не позволяет применить эти модули с новыми версиями компилятора. Также становится невозможным: исправить обнаруженные ошибки, проанализировать качество кода модуля, не говоря уже о его доработке. В связи с этим является актуальной задача разработки методов декомпиляции объектных файлов Delphi.

Основные результаты диссертации и их новизна:

1. Впервые разработан метод декомпиляции объектного кода Delphi, скомпилированного под платформу .NET, позволяющий восстанавливать программу на языке CIL в программу на языке Delphi, включающий следующие этапы: синтаксический анализ объектного кода Delphi, генерация управляющего графа, генерация промежуточного представления, структурирование графа потоков управления, анализ потоков данных, улучшение и генерации кода Delphi.
2. На основе предложенных методов реализован оригинальный декомпилятор объектных файлов Delphi, скомпилированных под платформу .NET.
3. Разработан оригинальный метод визуализации управляющего графа на плоскости. Основной особенностью разработанного метода визуализации является возможность использования изобразительных соглашений, принятых при проектировании блок-схем, что позволяет эффективнее выделять в графе узлы, соответствующие высокоуровневым операторам языков программирования.

Научная и практическая значимость результатов проведенного исследования.

Разработанные в рамках диссертационной работы методы и программное средство позволяют повысить эффективность анализа исполняемого кода за счет снижения трудозатрат, сокращения времени анализа, а также повышения наглядности представления результатов. Практическая значимость результатов связана с возможностью их применения для поддержки, анализа и изучения унаследованного программного обеспечения, имеющего в своем составе компоненты, представленные в виде скомпилированных модулей Delphi.

Материалы диссертации могут быть использованы при разработке спецкурсов для студентов математиков, а также при написании курсовых и дипломных работ, магистерских диссертаций.

Созданное программное обеспечение зарегистрировано в Федеральной службе по интеллектуальной собственности, патентам и товарным знакам № 2014617137, № 2016612670.

Достоверность результатов проведенного исследования обеспечена:

- обоснованным использованием методов и технологий декомпиляции информационных систем и визуализации управляющих графов, опубликованных в открытой печати;
- согласованностью с результатами исследований других авторов, представленных в печатных изданиях;
- работоспособностью разработанного декомпилятора и модуля визуализации графов, адекватностью полученных данных в результате их тестирования и сравнения с аналогичными средствами.

Полнота изложения результатов диссертации в печатных работах, опубликованных соискателем, подтверждается следующим перечнем работ:

Статьи в журналах, из списка рекомендованных ВАК РФ для опубликования основных научных результатов диссертации на соискание учёной степени кандидата и доктора наук:

1. Михайлов А. А. Анализ графа потоков управления в задаче декомпиляции подпрограмм объектных файлов dcuil // Вестник Новосибирского государственного университета. Серия: Информационные технологии. 2014. Т. 12, № 2. С. 74–79.
2. Михайлов А. А. Промежуточное представление подпрограмм в задаче декомпиляции объектных файлов dcuil // Вестник Бурятского государственного университета. 2014. № 9-3. С. 32–38.
3. Хмельнов А. Е., Бычков И. В., Михайлов А. А. Декларативный язык FlexT—инструмент анализа и документирования бинарных форматов данных // Труды института системного программирования РАН. 2016. Т. 28, № 5. С. 239–268.

Статьи в журналах из перечня WOS:

4. Mikhailov A., Hmelnov A., Cherkashin E. et al. Control flow graph visualization in compiled software engineering // Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2016 39th International Convention on / IEEE. 2016. P. 1313–1317.

Статьи в других изданиях:

5. Михайлов А. А. Анализ объектных файлов Delphi с использованием спецификации семантики машинных команд // Прикладная дискретная математика. 2012. Т. 5. С. 108–110.
6. Михайлов А. А. Анализ потоков данных подпрограмм в объектных файлах dcu // Материалы конференции. Малые Винеровские чтения 2013. 2013. С. 23 – 28.
7. Михайлов А. А. Анализ потоков данных подпрограмм в объектных файлах DCU // Тезисы конференции. ЛЯПУНОВСКИЕ ЧТЕНИЯ — 2012. 2012. С. 24.
8. Михайлов А. А. Анализ потоков данных подпрограмм объектных файлов Delphi // Труды XVIII Байкальской Всероссийской конференции "Информационные и математические технологии в науке и управлении". Т. 2. 2013. С. 151 – 156.
9. Михайлов А. А. Алгоритм анализа потоков данных подпрограмм объектных файлов DCU // Тезисы II Российско-Монгольской конференции молодых ученых — 2013. 2013. С. 43.
10. Михайлов А. А. Визуализация управляющего графа // Тезисы доклада III Российско-монгольской конференции молодых ученых по математическому моделированию, вычислительно-информационным технологиям и управлению Иркутск (Россия) - Ханх (Монголия). 2015. С. 59.
11. Михайлов А. А., Хмельнов А. Е. Анализ программного кода в объектных файлах Delphi, скомпилированных под платформу .NET // Труды конференции Языки программирования и компиляторы – 2017. 2017. С. 202 – 204.
12. Михайлов А. А. Анализ программного кода объектных файлов Delphi с использованием спецификации семантики машинных команд. 2012. URL:http://conf.nsc.ru/ym2012/ru/reportview/139230 (дата обращения: 2015-01-19).
13. Hmelnov A. E., Mikhaylov A. A., Burlakov A. S. Delphi .NET object file decompiler // In Proc. of the 5th International Workshop on Computer Science and Engineering — Russia, Moscow: Bauman Moscow State Technical University. 2015. P. 202 – 208.
14. Burlakov A. S., Mikhaylov A. A. The Computer Architecture and Hardware Descriptive Language // In Proc. of the 5th International Workshop on Computer Science and Engineering — Russia, Moscow: Bauman Moscow State Technical University. 2015. P. 148 – 154.

Свидетельства о регистрации программ для ЭВМ:

15. Михайлов А. А., Хмельнов А. Е. DCUIL2PAS - декомпилятор объектных модулей Delphi, скомпилированных по платформу .NET (файлов *.DCUIL). Свидетельство о

государственной регистрации программ для ЭВМ № 2014617137 М.: Федеральная служба по интеллектуальной собственности, патентам и товарным знакам.

16. Михайлов А. А., Хмельнов А. Е. Модуль структурной раскладки графов потоков управления на плоскости для программы визуализации графов Visual Graph. 2016. Свидетельство о государственной регистрации программ для ЭВМ № 2014617137 М.: Федеральная служба по интеллектуальной собственности, патентам и товарным знакам.

Личный вклад автора. Все выносимые на защиту научные результаты получены соискателем лично. В основных научных работах по теме диссертации, опубликованных в соавторстве, лично соискателем разработаны: в [2, 5, 6, 8, 9, 12] – методы декомпиляции объектного кода Delphi, скомпилированного под платформу .NET; [3, 13, 14] – программная реализация декомпилятора объектных файлов Delphi, скомпилированных под платформу .NET; [1, 4, 7, 10, 11] – метод визуализации управляющего графа на плоскости.

Ценность научных работ соискателя и их апробация подтверждена:

- Использованием результатов диссертационной работы в учебном процессе на кафедре «Информационных технологий» ИМЭИ ИГУ в рамках специального курса «Языки и системы программирования» для студентов 2-3 курсов дневного отделения.
- Дипломом I степени в конкурсе молодых ученых ИДСТУ СО РАН в номинации «Профессиональные достижения в области информационных технологий» на конференции «Ляпуновские чтения 2015».
- Дипломом II степени в конкурсе прикладных работ молодых ученых ИДСТУ СО РАН.
- Участием в конференциях: «Ляпуновские чтения 2012, 2013, 2014, 2015» (Иркутск, 2012, 2013, 2014, 2015 гг.); XIII Всероссийская конференция молодых ученых по математическому моделированию и информационным технологиям (Новосибирск, 2012 г.); «Малые Винеровские чтения 2013» (Иркутск, 2013 г.); XVIII Байкальская Всероссийская конференция «Информационные и математические технологии в науке и управлении». (Иркутск, 2013 г.); II Российско-Монгольская конференция молодых ученых (п. Ханх, Монголия, 2013 г.); III Российско-монгольская конференция молодых ученых по математическому моделированию, вычислительно-информационным технологиям и управлению Иркутск (Россия) – Ханх (Монголия) (п. Ханх, Монголия, 2015 г.); 5th International Workshop on Computer Science and Engineering – Russia, Moscow: Bauman Moscow State Technical University (Москва, 2015 г.); The 39th International ICT Convention – MIPRO 2016 (г. Опатия, Хорватия, 2016 г.)
- Отдельные результаты диссертационного исследования были получены в рамках программы фундаментальных исследований СО РАН проект IV.38.2.3. «Новые методы, технологии и сервисы обработки пространственных и тематических данных, основанные на декларативных спецификациях и знаниях» (2013-2015 гг.), а также научного проекта РФФИ № 15-37-20042 мол_а_вед. Основные результаты диссертации и её отдельные положения, а также результаты конкретных прикладных исследований и разработок обсуждались на научных семинарах ИДСТУ СО РАН, ИСИ СО РАН, ИСП РАН.

Соответствие паспорту специальности. В соответствии с формулой специальности 05.13.11 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей диссертационная работа Михайлова А.А. охватывает решение задач повышения эффективности процессов анализа, сопровождения и создания программ и программных систем, в частности, унаследованного программного обеспечения, имеющего в своем составе компоненты, представленные в виде скомпилированных модулей Delphi.

Отраженные в диссертации положения соответствуют пунктам 1, 2, 7 и 10 области исследований специальности 05.13.11:

- Модели, методы и алгоритмы проектирования и анализа программ и программных систем, их эквивалентных преобразований, верификации и тестирования.
- Языки программирования и системы программирования, семантика программ.
- Человеко-машинные интерфейсы; модели, методы, алгоритмы и программные средства машинной графики, визуализации, обработки изображений, систем виртуальной реальности, мультимедийного общения.
- Оценка качества, стандартизация и сопровождение программных систем.

Диссертационное исследование Михайлова А.А. «Методы декомпиляции объектного кода Delphi» является самостоятельной научно-квалификационной работой. Работа соответствует всем требованиям ВАК РФ, предъявляемым к кандидатским диссертациям, не содержит заимствованного материала без ссылок на автора и (или) источник заимствования.

Диссертационная работа Михайлова А.А. «Методы декомпиляции объектного кода Delphi» рекомендуется к защите на соискание ученой степени кандидата технических наук по специальности 05.13.11 «Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей».

Заключение принято на заседании Семинара ИДСТУ СО РАН по вычислительным технологиям. На заседании присутствовало 17 чел. Результаты голосования: «за» – 17 чел., «против» – нет, «воздержались» – нет (протокол №1 от 28 июня 2017 г.).

Председатель семинара,
д.т.н, профессор — Г.А. Опарин

Секретарь семинара,
к.т.н — А.П. Новопашин