

СВЕДЕНИЯ О РЕЗУЛЬТАТАХ ПУБЛИЧНОЙ ЗАЩИТЫ ДИССЕРТАЦИИ

Диссертационный совет Д 212.267.12, созданный на базе федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский Томский государственный университет», извещает о результатах состоявшейся 31 мая 2017 года публичной защиты диссертации Ермакова Антона Дмитриевича «Автоматные методы и алгоритмы синтеза тестов для программного обеспечения с использованием подходов формальной верификации» по специальности 05.13.01 – Системный анализ, управление и обработка информации (в отраслях информатики, вычислительной техники и автоматизации) на соискание ученой степени кандидата технических наук.

На заседании присутствовали 16 из 21 члена диссертационного совета, в том числе 7 докторов наук по специальности 05.13.01 – Системный анализ, управление и обработка информации (в отраслях информатики, вычислительной техники и автоматизации), технические науки:

№№	Фамилия, инициалы	Ученая степень	Специальность, отрасль науки в совете
1.	Горцев А.М., председатель	доктор технических наук	05.13.01, технические науки
2.	Назаров А.А., заместитель председателя	доктор технических наук	05.13.01, технические науки
3.	Тарасенко П.Ф., ученый секретарь	кандидат физико- математических наук	05.13.01, физико-математические науки
4.	Дмитренко А.Г.	доктор физико- математических наук	05.13.01, физико-математические науки
5.	Дмитриев Ю.Г.	доктор физико- математических наук	05.13.01, физико-математические науки
6.	Евтушенко Н.В.	доктор технических наук	05.13.01, технические науки
7.	Китаева А.В.	доктор физико- математических наук	05.13.01, физико-математические науки

8.	Конев В.В.	доктор физико-математических наук	05.13.01, физико-математические науки
9.	Кошкин Г.М.	доктор физико-математических наук	05.13.01, физико-математические науки
10.	Матросова А.Ю.	доктор технических наук	05.13.01, технические науки
11.	Моисеева С.П.	доктор физико-математических наук	05.13.01, физико-математические науки
12.	Рожкова С.В.	доктор физико-математических наук	05.13.01, физико-математические науки
13.	Смагин В.И.	доктор технических наук	05.13.01, технические науки
14.	Спицын В.Г.	доктор технических наук	05.13.01, технические науки
15.	Удод В.А.	доктор технических наук	05.13.01, технические науки
16.	Шумилов Б.М.	доктор физико-математических наук	05.13.01, физико-математические науки

Заседание провёл председатель диссертационного совета доктор технических наук, профессор Горцев Александр Михайлович.

По результатам защиты диссертации тайным голосованием (результаты голосования: за присуждение ученой степени – 16, против – нет, недействительных бюллетеней – нет) диссертационный совет принял решение присудить А.Д. Ермакову ученую степень кандидата технических наук.

Заключение диссертационного совета Д 212.267.12
на базе федерального государственного автономного образовательного
учреждения высшего образования
«Национальный исследовательский Томский государственный университет»
Министерства образования и науки Российской Федерации
по диссертации на соискание ученой степени кандидата наук
аттестационное дело № _____

решение диссертационного совета от 31.05.2017, № 202

О присуждении **Ермакову Антону Дмитриевичу**, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация **«Автоматные методы и алгоритмы синтеза тестов для программного обеспечения с использованием подходов формальной верификации»** по специальности **05.13.01 – Системный анализ, управление и обработка информации** (в отраслях информатики, вычислительной техники и автоматизации) принята к защите 22.03.2017, протокол № 196, диссертационным советом **Д 212.267.12** на базе федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский Томский государственный университет» Министерства образования и науки Российской Федерации (634050, г. Томск, пр. Ленина, 36, приказ о создании диссертационного совета № 105/нк от 11.04.2012 г.).

Соискатель **Ермаков Антон Дмитриевич**, 1989 года рождения.

В 2012 г. соискатель окончил федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Национальный исследовательский Томский государственный университет».

В 2016 году соискатель очно окончил аспирантуру федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский Томский государственный университет».

Работает в должности инженера-исследователя лаборатории компьютерных наук федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский Томский государственный университет» Министерства образования и науки Российской Федерации.

Диссертация выполнена на кафедре информационных технологий в исследовании дискретных структур федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский Томский государственный университет» Министерства образования и науки Российской Федерации.

Научный руководитель – доктор технических наук, **Евтушенко Нина Владимировна**, федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Томский государственный университет», лаборатория компьютерных наук, заведующий лабораторией; по совместительству – кафедра информационных технологий в исследовании дискретных структур, профессор, (на момент назначения научным руководителем – кафедра информационных технологий в исследовании дискретных структур, заведующий кафедрой).

Официальные оппоненты:

Шалыто Анатолий Абрамович, доктор технических наук, профессор, федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», кафедра технологий программирования, заведующий кафедрой

Медведев Юрий Геннадьевич, кандидат технических наук, Федеральное государственное бюджетное учреждение науки Институт вычислительной математики и математической геофизики Сибирского отделения Российской академии наук, лаборатория синтеза параллельных программ, старший научный сотрудник

дали положительные отзывы на диссертацию.

Ведущая организация – Федеральное государственное бюджетное учреждение науки **Санкт-Петербургский институт информатики и автоматизации Российской академии наук**, г. Санкт-Петербург, в своем положительном отзыве, подписанном **Барановым Сергеем Николаевичем** (доктор физико-математических наук, профессор, лаборатория информационно-вычислительных систем и технологий программирования, главный научный сотрудник) и **Осиповым Василием**

Юрьевичем (доктор технических наук, профессор, лаборатория информационно-вычислительных систем и технологий программирования, заведующий лабораторией), указала, что диссертационная работа посвящена актуальной задаче синтеза входных данных для проверки правильности функционирования программного обеспечения, гарантирующей достаточную полноту тестового покрытия. А.Д. Ермаковым использованы модели с конечным числом переходов – так называемые автоматные модели – для построения проверяющих тестов для исследуемого программного обеспечения; предложены методы и алгоритмы для повышения качества тестирования программного обеспечения с использованием таких моделей; исследованы неклассические автоматные модели, такие как расширенный и недетерминированный автоматы и автоматные сети, в рамках которых предложены усовершенствования для известных подходов к синтезу тестов с гарантированной полнотой покрытия операторов и ветвлений, которые оказываются вполне работоспособными для определенного класса приложений сравнительно небольшого размера; предложено новое решение для построения адаптивной проверяющей последовательности относительно редукции (глава 3), в котором вместо разделяющей последовательности используется адаптивный различающий тестовый пример; разработаны: алгоритм повышения полноты тестов, построенных по расширенному автомату, используя инструментарий для мутационного тестирования, алгоритм локализации ошибочных компонентов в автоматной сети, описывающей поведение программного обеспечения, метод построения адаптивных проверяющих последовательностей для неинициальных недетерминированных автоматов, программная реализация алгоритмов поиска уязвимостей типа «переполнение буфера» в программном коде на языках C/C++. Предложенные методы и алгоритмы повышения качества тестирования можно классифицировать как новые научно обоснованные технические решения и разработки, имеющие существенное значение для развития подходов к тестированию программного обеспечения. Работа открывает новые перспективы для дальнейших научных исследований в области анализа дискретных систем, поведение которых может быть недетерминированным. Предложенные А.Д. Ермаковым методы и алгоритмы повышения качества тестирования могут быть классифицированы как новые научно

обоснованные технические решения и разработки, имеющие существенное значение для развития подходов к тестированию программного обеспечения и могут быть использованы при тестировании программного обеспечения, специфицируемого расширенным автоматом, для тестирования программных реализаций телекоммуникационных протоколов, а также программ управляющих систем. Разработанный автором ППП для поиска уязвимостей в программном обеспечении на основе верификатора *Java Path Finder* может быть использован для проверки безопасности программного обеспечения.

Соискатель имеет 13 опубликованных работ, в том числе по теме диссертации – 12 работ, опубликованных в рецензируемых научных изданиях – 4, в зарубежных научных изданиях, индексируемых Web of Science и Scopus – 3, в научном журнале – 1, в сборниках материалов международных и всероссийских научных конференций – 4. Общий объем работ – 6,6 п.л., авторский вклад – 3,79 п.л.

В диссертации отсутствуют достоверные сведения об опубликованных соискателем ученой степени работах, в которых изложены основные научные результаты диссертации.

Наиболее значительные научные работы по теме диссертации, опубликованные в журналах, включенных в Перечень рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук:

1. **Ермаков А. Д.** Тестирование безопасности программного обеспечения с использованием верификаторов / А. Д. Ермаков // Известия высших учебных заведений. Физика. – 2013. – Т. 56, № 9/2. – С. 181–183. – 0,21 п.л.

2. **Ермаков А. Д.** Синтез проверяющих последовательностей для недетерминированных автоматов относительно редукции / А. Д. Ермаков // Труды Института системного программирования РАН. – 2014. – Т. 26, вып. 6. – С. 111–124. – DOI: 10.15514/ISPRAS-2014-26(6)-10. – 0,62 п.л.

3. **Ермаков А. Д.** К синтезу адаптивных проверяющих последовательностей для недетерминированных автоматов / А. Д. Ермаков, Н. В. Евтушенко // Труды Института системного программирования РАН. – 2016. – Т. 28, вып. 3. – С. 123–144. – DOI: 10.15514/ISPRAS-2016-28(3)-8. – 1,24 / 0,62 п.л.

4. **Ермаков А. Д.** Метод синтеза тестов с гарантированной полнотой по модели расширенного автомата / А. Д. Ермаков, Н. В. Евтушенко // Моделирование и анализ информационных систем. – 2016. – Т. 23, № 6. – С. 729–740. – DOI: 10.18255/1818-1015-2016-6-729-740. – 1,4 / 0,7 п.л.

На автореферат поступили 6 положительных отзывов. Отзывы представили:

1. **Л. Д. Черемисинова**, д-р техн. наук, проф., главный научный сотрудник лаборатории логического проектирования Объединенного института проблем информатики НАН Беларуси, г. Минск, *с замечаниями*: отсутствует методика выбора мутантов, генерируемых программным инструментом *μJava* и обеспечивающих полноту искомой проверяющей последовательности; не приведены сравнительные оценки сложности разработанных и известных алгоритмов построения тестов для программного обеспечения; не ясна размерность практических задач, которые могут быть решены в рамках предложенных подходов. 2. **Л. С. Ломакина**, д-р техн. наук, проф., профессор кафедры «Вычислительные системы и технологии» Нижегородского государственного технического университета им. Р. Е. Алексеева и **Д. В. Жевневчук**, канд. техн. наук, доц., доцент кафедры «Вычислительные системы и технологии» Нижегородского государственного технического университета им. Р. Е. Алексеева, *с вопросом*: насколько ограничения Java Path Finder, накладываемые на диапазон используемых библиотек и размер тестируемой программы сужают возможность применения полученных результатов в промышленных программных разработках, на основе комплекса языковых средств, подключаемых модулей, web-сервисов и др.? *и замечанием*: пункт 4 научной новизны, в котором заявлен обзор известных статических методов и разработка учебного программного комплекса, целесообразно было бы отнести к задачам диссертации. 3. **Г. Б. Захарова**, канд. техн. наук, доц., заведующий кафедрой прикладной информатики Уральского государственного архитектурно-художественного университета, г. Екатеринбург, *с замечанием*: автореферат содержит опечатки и ошибки пунктуации; в автореферате не хватает хотя бы небольшого примера тестирования или верификации на базе предложенных алгоритмов. 4. **А. Д. Хомоненко**, д-р техн. наук, проф., заведующий кафедрой

«Информационные и вычислительные системы» Петербургского государственного университета путей сообщения Императора Александра I, *с замечаниями*: не представлено обоснование выбора типа мутаций, указанных при генерации в *μJava*; отсутствует оценка того, как может повлиять трансляция кода на результат поиска уязвимостей. 5. **Н. Г. Кудрявцев**, канд. техн. наук, старший научный сотрудник, доцент кафедры физики и информатики Горно-Алтайского государственного университета, *с замечанием*: в автореферате отсутствует пример программной реализации, в котором алгоритмы автора смогли обнаружить ошибки, не обнаруженные тестами, построенными другими методами. 6. **С. Л. Собко**, канд. техн. наук, начальник управления перспективных методик разработки программного обеспечения Исследовательского Центра Самсунг Электроникс, г. Москва, *с замечаниями*: не совсем понятно, каким образом проводился поиск уязвимостей в программном обеспечении на языке C на основе верификатора *Java Path Finder*, который требовал множественного выполнения программы на виртуальной Java-машине; отсутствует сравнение результатов разработанного программного комплекса с результатами существующих инструментов; в автореферате отсутствуют примеры тестирования или верификации программной реализации.

Авторы отзывов на автореферат отмечают, что процесс верификации и тестирования (встроенного) при проектировании программного обеспечения, несомненно, является одной из важнейших проблем при проектировании и разработке программного обеспечения. А.Д. Ермаковым предложено улучшить качество тестов, построенных по модели расширенного автомата за счет применения инструментов мутационного тестирования к «шаблонной» программной реализации расширенного автомата-спецификации; предлагается достраивать тесты различающимися последовательностями, которые строятся не для двух программных реализаций, а для двух автоматов (автомата-спецификации и мутанта расширенного автомата), что во многих случаях может оказаться более простой задачей; предложен метод построения адаптивной проверяющей последовательности по недетерминированному автомату, при условии, что поведение проверяемой

реализации является детерминированным; расширены существующие подобные результаты для детерминированных автоматов с использованием новых понятий адаптивной различимости и достижимости; разработан пакет программ на основе верификатора *Java Path Finder* для обнаружения в программном обеспечении на языке C/C++ уязвимостей типа переполнения буфера, которые могут повлиять на конфиденциальность и целостность информации. Новизна представляемой диссертационной работы заключается в развитии формальных методов синтеза проверяющих тестов с гарантированной полнотой на основе автоматных моделей. Полученные теоретические результаты ориентированы на использование в современных программных системах диагностики и тестирования программного обеспечения, функциональные требования к которому описаны посредством расширенных автоматов. Полученные автором результаты работы представляют большой интерес для развития методов проектирования качественных программных продуктов, отвечающих всем требованиям безопасности.

Выбор официальных оппонентов и ведущей организации обоснован тем, что **А.А. Шалыто** является высококвалифицированным специалистом в области аппаратного программирования, проектирования и верификации алгоритмов логического управления на основе моделей с конечным числом состояний, а также в области теории автоматов; **Ю.Г. Медведев** – высококвалифицированный специалист в области использования автоматных моделей для моделирования и верификации различных технических систем; в **Санкт-Петербургском институте информатики и автоматизации Российской академии наук** работают высококвалифицированные специалисты в области информатики и автоматизации, в том числе в области использования формальных моделей в программной инженерии, тестировании и верификации программного обеспечения.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований получены следующие новые научные результаты:

разработан алгоритм повышения полноты тестов для программного обеспечения, построенных по модели расширенного автомата, с использованием мутантов, генерируемых программным инструментом *μJava*;

разработан алгоритм локализации неисправной компоненты в многокомпонентной автоматной композиции на основе трассировки исполнения проверяющего теста;

предложен алгоритм обнаружения уязвимостей в программном обеспечении на языках C/C++ с использованием верификатора *Java Path Finder*; алгоритм сочетает в себе элементы верификации программного обеспечения и динамический подход к тестированию безопасности и ориентирован на обнаружение следующих типов уязвимостей:

- уязвимость переполнения типа,
- уязвимость переполнения приведения типа,
- уязвимость переполнения в массивах,
- отрицательное переполнение в массивах,
- повторное освобождение памяти,
- повторное выделение памяти;

решена задача построения адаптивной проверяющей последовательности для случая, когда спецификация системы является неинициальным полностью определенным наблюдаемым конечным автоматом, а реализация – неинициальным полностью определенным детерминированным конечным автоматом, а именно: *разработан* метод построения адаптивной проверяющей последовательности для недетерминированного полностью определенного конечного автомата относительно редукции;

по результатам проведенных компьютерных экспериментов *сделан вывод* об эффективности разработанных алгоритмов.

Теоретическая значимость исследования обоснована тем, что:

предложен метод построения адаптивной проверяющей последовательности для недетерминированного автомата при условии, что проверяемые реализации являются детерминированными, и в реализациях отсутствует надежный сигнал сброса в начальное состояние; *доказано*, что в большинстве случаев длина такой последовательности имеет тот же порядок, что и для детерминированных автоматов;

предложен алгоритм повышения полноты тестов, построенных по модели расширенного автомата с использованием мутантов, генерируемых программным инструментом *μJava*; система мутантов соответствуют наиболее часто встречающимся ошибкам разработчиков программного обеспечения, и алгоритм гарантирует полноту построенных тестов относительно одиночных функциональных ошибок в «шаблонной» программной реализации расширенного автомата.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

Полученные в диссертационной работе результаты могут быть использованы при тестировании и верификации программных и/или аппаратных компонентов телекоммуникационных систем, при анализе безопасности компьютерных систем, при оценке качества специализированного программного обеспечения, так как проведенные компьютерные эксперименты показали, что сгенерированные тесты обнаруживают функциональные ошибки в программном обеспечении, не обнаружимые тестами, построенными другими известными способами.

Результаты диссертационной работы используются в учебном процессе на радиофизическом факультете Томского государственного университета (акт о внедрении от 08.11.2016). Предложенные алгоритмы используются при построении проверяющих тестов для программных реализаций протоколов в процессе проведения практических и лабораторных занятий. Разработанный пакет прикладных программ для поиска уязвимостей в программном обеспечении на языках C/C++ используется для анализа студенческих программных реализаций на наличие уязвимостей типа «переполнение буфера».

Результаты работы были также использованы на предприятии ОАО «ТомскНИПИнефть», а именно: разработанный пакет прикладных программ для поиска уязвимостей в программном обеспечении на основе верификатора *Java Path Finder* позволил проверить ряд производственных программ на наличие уязвимостей типа «переполнение буфера», а предложенный алгоритм построения тестов на основе расширенных автоматов с использованием мутационного тестирования позволил повысить качество функциональных тестов для штатного

программного обеспечения за счет генерации дополнительных функциональных тестов (акт внедрения от 11.11.2016).

Рекомендации об использовании результатов диссертационного исследования

Предложенные методы и алгоритмы могут быть использованы при тестировании программного обеспечения, функциональные требования к которому описаны посредством расширенного автомата, в том числе для тестирования программных реализаций телекоммуникационных протоколов, программ автоматизированного управления и т.д. Пакет программ для поиска уязвимостей в программном обеспечении на основе верификатора *Java Path Finder* может быть использован при тестировании безопасности программного обеспечения.

Результаты диссертационной работы рекомендуются для использования в учебном процессе Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики, Санкт-Петербургского института информатики и автоматизации РАН, Института вычислительной математики и математической геофизики СО РАН (г. Новосибирск), Объединенного института проблем информатики НАН Беларуси (г. Минск), Нижегородского государственного технического университета им. Р.Е. Алексева, Уральского государственного архитектурно-художественного университете, (г. Екатеринбург), Петербургского государственного университета путей сообщения Императора Александра I, а также в компании Самсунг и других организациях, занимающихся исследованием телекоммуникационных и информационно-вычислительных систем и сетей связи.

Оценка достоверности результатов исследования выявила:

Обоснованность полученных результатов обеспечена строгими математическими доказательствами с использованием аппарата дискретной математики.

Личный вклад соискателя состоит в: совместных с научным руководителем постановках задач и выборе основных направлений исследований; самостоятельном получении результатов, изложенных в исследовании

и выносимых на защиту. Математические выкладки, программная реализация разработанных в ходе исследования алгоритмов и численные расчеты выполнены лично автором.

Диссертация отвечает критериям, установленным Положением о присуждении ученых степеней для диссертаций на соискание ученой степени кандидата наук, и, в соответствии с п. 9 Положения, является научно-квалификационной работой, в которой изложены новые научно-обоснованные технические решения и разработки для тестирования программных реализаций телекоммуникационных протоколов, программ автоматизированного управления, встроенных программных продуктов, имеющие существенное значение для развития тестирования (встроенного) программного обеспечения.

На заседании 31.05.2017 диссертационный совет принял решение присудить **Ермакову А.Д.** ученую степень кандидата технических наук.

При проведении тайного голосования диссертационный совет в количестве 16 человек, из них 7 докторов наук по специальности 05.13.01 – Системный анализ, управление и обработка информации (в отраслях информатики, вычислительной техники и автоматизации), технические науки, из 21 человека, входящего в состав совета, проголосовал: за – 16, против – нет, недействительных бюллетеней – нет.

Председатель

диссертационного совета

Ученый секретарь

диссертационного совета



Горцев Александр Михайлович

Тарасенко Петр Феликсович

31.05.2017