

ISSN 1818-1015

Министерство образования и науки Российской Федерации  
Ярославский государственный университет им. П.Г. Демидова

МОДЕЛИРОВАНИЕ И АНАЛИЗ  
ИНФОРМАЦИОННЫХ СИСТЕМ

Том 17 № 4 2010

Основан в 1999 г.

Выходит 4 раза в год

*Свидетельство о регистрации №019209 от 16.08.99*

*Государственного Комитета Российской Федерации по печати*

*Главный редактор*

**В.А. Соколов**

*Редакционная коллегия*

С.М. Абрамов, О.Л. Бандман, В.А. Бондаренко, И.Б. Вирбицкайте,  
С.Д. Глызин (зам. гл. ред.), М.Г. Дмитриев, В.Л. Дольников, В.Г. Дурнев,  
А.В. Зафиевский, Л.С. Казарин, Ю.Г. Карпов, С.А. Кащенко, А.Ю. Колесов,  
И.А. Ломазова, В.Э. Малышкин, В.А. Непомнящий,  
П.Г. Парфенов, Р.Л. Смелянский

*Ответственный секретарь* Е.А. Тимофеев

**Адрес редакции:** 150000, Ярославль, ул. Советская, 14

**E-mail:** mais@uniyar.ac.ru

**Website:** mais.uniyar.ac.ru

Научные статьи в журнал принимаются по электронной почте и на кафедре теоретической информатики Ярославского государственного университета. Статьи должны содержать УДК, аннотации на русском и английском языках и сопровождаться набором текста в редакторе LaTeX. Плата с аспирантов за публикацию рукописей не взимается.

©Ярославский государственный  
университет им. П.Г. Демидова, 2010

## СОДЕРЖАНИЕ

---

*Моделирование и анализ информационных систем. Т. 17, №4. 2010*

---

От редакторов специального выпуска <i>Непомнящий В.А., Соколов В.А.</i>	5
Automated Correctness Proof of Algorithm Variants in Elliptic Curve Cryptography <i>Anikeev M., Madlener F., Schlosser A., Huss S. A., Walther C.</i>	7
Генерация тестовых данных на основе формального анализа данных конфигурации проекта <i>Батаев А. В., Давыдов А. А., Налютин Н. Ю., Смицын С. В.</i>	17
Безопасное тестирование симуляции систем с отказами и разрушением <i>Бурдонов И.Б., Косачев А.С.</i>	27
О сложности верификации недетерминированных вероятностных мультиагентных систем <i>Валиев М.К., Дехтярь М.И.</i>	41
Проверка моделей распределенных систем с помощью аффинного представления данных <i>Гаранина Н.О.</i>	52
Об исчислении позитивно-образованных формул для автоматического доказательства теорем <i>Давыдов А.В., Ларионов А.А., Черкашин Е.А.</i>	60
Интеграция семантических верификаторов в компиляторы языка Java <i>Клепинин А. В., Мелентьев А. А.</i>	70
Адаптивная редукция симметричных моделей в задаче верификации моделей программ для логики линейного времени <i>Коннов И.В., Захаров В.А.</i>	78
Верификация С-программ в мультиязыковой системе СПЕКТР <i>Непомнящий В.А., Ануреев И.С., Атучин М.М., Марьясов И.В., Петров А.А., Промский А.В.</i>	88
Верификация и синтез программ сложения на базе правил корректности операторов <i>Шелехов В.И.</i>	101
Пример верификации в проекте F@BOOL@, основанном на булевских решателях <i>Шилов Н.В.</i>	111
Проектирование программных бортовых систем управления с поддержкой верификации <i>Шошмина И.В.</i>	125

---

Редактор, корректор А.А. Аладьева. Редактор перевода Э.И. Соколова.

Подписано в печать 15.12. 2010. Формат 60x84<sup>1</sup>/<sub>8</sub>. Усл. печ. л. 15,75. Уч.-изд. л. 12,5.

Т. 500 экз. Заказ 06/011. Отпечатано на ризографе. Ярославский государственный университет им. П. Г. Демидова, 150 000, Ярославль, ул. Советская, 14. Телефон редакции (4852) 79-77-51.

ISSN 1818-1015

Ministry of Education and Science of the Russian Federation  
Yaroslavl Demidov State University

MODELING AND ANALYSIS  
OF INFORMATION SYSTEMS

Volume 17    No 4    2010

Founded in 1999  
4 issues per year

*State Registration License No 019209 of 16.08.1999*

*Editor-in-Chief*

**V. A. Sokolov**

*Editorial Board*

S.M. Abramov, O.L. Bandman, V.A. Bondarenko, I.B. Virbitskayte,  
S.D. Glyzin (*Deputy Editor-in-Chief*), M.G. Dmitriev, V.L. Dol'nikov,  
V.G. Durnev, A.V. Zafievsky, L.S. Kazarin, Yu.G. Karpov,  
S.A. Kashchenko, A.Yu. Kolesov, I.A. Lomazova,  
V.E. Malyshkin, V.A. Nepomniaschy, P.G. Parfionov, R.L. Smeliansky

*Responsible Secretary* E. A. Timofeev

**Editorial Office Address:** Sovetskaya str., 14, Yaroslavl, 150000, Russia

**E-mail:** mais@uniyar.ac.ru

**Website:** mais.uniyar.ac.ru

©Yaroslavl Demidov State University, 2010

## Contents

---

*Modeling and Analysis of Information Systems. Vol. 17, No 4. 2010*

---

Automated Correctness Proof of Algorithm Variants in Elliptic Curve Cryptography <i>Anikeev M., Madlener F., Schlosser A., Huss S. A., Walther C.</i>	7
Test data generation based on a formal analysis of the project configuration <i>Bataev A.V., Davydov A.A., Nalutin N.Y., Sinitsyn S.V.</i>	17
Safe simulation testing of systems with refusals and destructions <i>Burdonov I.B., Kosachev A.S.</i>	27
On complexity of verification of nondeterministic probabilistic multiagent systems <i>Valiev M.K., Dekhtyar M.I</i>	41
Model Checking of Distributed Systems with Affine Data Structures <i>Garanina N.O.</i>	52
On the calculus of positively constructed formulas for authomated theorem proving <i>Davydov A.V., Larionov A.A., Cherkashin E.A.</i>	60
Integration of semantic verification into Java compilers <i>Klepinin A. V. , Melentyev A. A.</i>	70
The application of adaptive symmetry reduction for LTL model checking <i>Konnov I.V., Zakharov V.A.</i>	78
C Program Verification in the Multilanguage System Spectrum <i>Nepomniashy V.A., Anureev I.S., Atuchin M.M., Maryasov I.V., Petrov A.A., Promsky A.V.</i>	88
Verification and synthesis of addition programs under the rules of statement correctness <i>Shelekhov V.I.</i>	101
F@BOOL@: experiment with a simple verifying compiler based on SAT-solvers <i>Shilov N.V.</i>	111
Distributed embedded control systems design with verification support <i>Shoshmina I.V.</i>	125

## От редакторов специального выпуска

В.А. Непомнящий, В.А. Соколов

Данный выпуск представляет статьи, подготовленные на основе избранных докладов международного семинара «Семантика, спецификация и верификация программ: теория и приложения» (Workshop on Program Semantics, Specification and Verification: Theory and Applications, PSSV 2010). Этот семинар был проведен 14 – 15 июня 2010 года в городе Казань в рамках 5-го Международного симпозиума по компьютерным наукам в России (5th International Computer Science Symposium in Russia, CSR 2010). Его труды, содержащие краткое изложение 24 докладов, опубликованы в сборнике издательства «Отечество», г. Казань. Тематика семинара включала направления исследований, относящиеся к методам дедуктивной верификации программ, методу проверки моделей (model checking method), формальным подходам к тестированию и валидации программ, а также к разработке и применению систем тестирования и верификации.

Настоящий выпуск включает 12 статей. Теоретическим проблемам посвящены 4 статьи.

В статье М.К. Валиева и М.И. Дехтяря «О сложности верификации недетерминированных вероятностных мультиагентных систем» рассматриваются вероятностные системы взаимодействующих недетерминированных интеллектуальных агентов. Описан и обоснован полиномиальный алгоритм, который моделирует эти системы конечными Марковскими процессами принятия решений.

В статье Н.О. Гараниной «Проверка моделей распределенных систем с помощью аффинного представления данных» предложено символьное представление моделей распределенных систем, определяемых линейными функциями над целочисленными переменными.

В статье А.В. Давыдова, А.А. Ларионова и Е.А. Черкашина «Об исчислении позитивно-образованных формул для автоматического доказательства теорем» предложены новый вариант логического языка и основанное на нем исчисление. Рассмотрены вопросы об эффективной реализации этого исчисления в виде программной системы для автоматического доказательства теорем.

В статье И.В. Коннова, В.А. Захарова «Адаптивная редукция симметричных моделей в задаче верификации моделей программ для логики линейного времени» предложен новый теоретико-автоматный метод верификации моделей программ, который использует метод адаптивной редукции симметричных моделей с целью сокращения пространства поиска при верификации методом проверки моделей.

6 статей посвящено разработке теоретических методов и экспериментальных подходов, ориентированных на практические применения.

В статье M. Anikeev, F. Madlener, A. Schlosser, S. A. Huss, C. Walther «Automated Correctness Proof of Algorithm Variants in Elliptic Curve Cryptography» предлагается новый подход к формальному доказательству корректности алгоритмов из области эллиптической криптографии. Для формального доказательства использовалась система VeriFun.