# От редакторов выпуска

*В. А. Захаров*[1,2], *Н. В. Шилов*[3]

1 ВШЭ
2 ИСП РАН
3 Университет Иннополис

# From the Editors of the Issue

*V. A. Zakharov*[1,2], *N. V. Shilov*[3]

1 HSE
2 ISP RAS
3 Innopolis University

04–05 ноября 2021 г. в Иннополисе прошел двенадцатый международный научно–исследовательский семинар **«Семантика, спецификация и верификация программ: теория и приложения»** (12-th Workshop on Program Semantics, Specification and Verification: Theory and Applications, PSSV 2021). Ввиду непростой эпидемической обстановки в стране заседания семинара проводились в формате видеоконференции. Организатором семинара выступила лаборатория программной инженерии университета Иннополис (рук. лаборатории Н. В. Шилов).

Первая сессия семинара была посвящена юбилею выдающегося ученого, специалиста в области информационных технологий и программирования, заведующего отделом технологии программирования Института системного программирования им. В. П. Иванникова, профессора Московского государственного университета им. М. В. Ломоносова и Высшей Школы Экономики Александра Константиновича Петренко. В своем докладе, озаглавленном «The position of formal methods in nowadays software industrial development», А. К. Петренко проанализировал тенденции развития и практического применения формальных методов в разработке промышленного программного обеспечения, рассказал о своем опыте использования этих методов в решении разнообразных задач системного программирования, начиная от работ по созданию программного обеспечения для советской космической программы «Буран» до недавних прикладных исследований по проектированию и верификации критических по безопасности и надежности программных систем.

Редколлегия журнала присоединяется к теплым пожеланиям, высказанным участниками семинара PSSV 2021 в адрес Александра Константиновича Петренко.

На юбилейной сессии семинара также прозвучали доклады ближайших коллег

А. С. Камкин: *High-Level Synthesis of Computing Systems: Motivation, Challenges, and Existing Solutions*,
В. В. Кулямин: *Formal Security Models*,
А. В. Хорошилов: *Verification of operating systems*.

Программа семинара PSSV 2021 включала

- 5 регулярных докладов

  Anton Gnatenko, Vladimir Zakharov: *Satisfiability and model checking for one extension of Linear Time Temporal Logic*,
  Alexander Bolotov, Alex Abuin Yepes, Paqui Lucio and Montserrat Hermo: *Certifying Proofs and Models for CTL Satisfiability and Model Checking*,
  Hans de Nivelle: *A Recursive Inclusion Checker for Recursively Defined Subtypes*,
  Thomas Baar, Horst Schulte: *On the Need to Support Vectors and Matrixes in KeYmaera*,
  Dmitry Kondratyev: *Towards automatic deductive verification of C programs with Sisal loops using C-lightVer system*,
- 7 кратких сообщений

  Thanh-Hai Tran, Igor Konnov and Josef Widder: *EDTL4CSRS: Event-Driven Temporal Logic for Control Software Requirements Specification*,
  Julio Cesar Carrasquel: *Validating Real Behavior of Agents in Trading Systems using Nested Petri Nets*,

Anton Zavyalov, Sergey Staroletov: *Flovver: A Graphical Functional Language with a Compiler Focused on Recursion Optimization*,
Mohammadsadegh Mohagheghi, Khayyam Salehi: *Statistical Verification of Qualitative Reachability Properties for Markov Decision Processes*,
Andrei Klimov: *On Recent Achievements in Theory of Names to be Used in Semantics of Object-Oriented Languages*,
Andrew Mironov: *Mathematical model and method for verifying parallel programs*,
Nikolay Shilov, Dmitry Kondratyev, Boris Faifel: *Platform-independent model of fix-point arithmetic for verification of the standard mathematical functions*,

- 4 лекции приглашенных докладчиков
  Nataliya O. Garanina (Laboratory of Theoretical Programming of A.P. Ershov Institute of Informatics Systems, Novosibirsk, Russia): *The Optimization Problem with Model Checking*,
  Dmitry A. Kondratyev (Laboratory of Theoretical Programming of A.P. Ershov Institute of Informatics Systems, Novosibirsk, Russia): *Automatic deductive verification of C programs using the C-lightVer system*,
  Alexandr V. Naumchev (Innopolis University, Russia): *Security audit of code using contracts and program proving*,
  Nikolai D. Kudasov (Innopolis University, Russia): *Nameless and scope-safe: de Bruijn notation as a nested datatype*.

В своих выступлениях участники семинара рассказали о результатах недавно завершенных научных работ и о продолжающихся исследованиях, посвященных развитию и применению математических методов для разработки программного обеспечения, вычислительной и телекоммуникационной аппаратуры, созданию новых математических моделей в области информатики, развитию и внедрению перспективных средств программирования. Большое внимание было уделено методам дедуктивной проверки правильности программ, задачам верификации моделей программ, новым методам анализа типов данных, а также вопросам построения формальных моделей информационных систем. Данный выпуск журнала включает 6 статей участников семинара PSSV 2021, рекомендованных программным комитетом семинара к публикации в журнале.

T. Baar и H. Schulte исследовали вопрос о применении программно-инструментального средства верификации программ на основе логики Хоара KeYmaeraX для обоснования свойств поведения гибридных систем. Эти системы определяются совокупностью дискретных и непрерывных переменных, значения которых могут изменяться скачком или постепенно. Одной из многообещающих областей применения KeYmaeraX являются системы управления с обратной связью. На примере одной из таких управляющих систем авторы показывают, как можно получить строгое математическое доказательство асимптотической устойчивости ее поведения с использованием средства дедуктивной верификации KeYmaeraX. В статье также обсуждаются некоторые открытые вопросы, связанные с формализацией требования асимптотической устойчивости гибридных систем.

В статье Н. О. Гараниной и С. П. Горлача представлен новый подход к автоматизации поиска оптимальных параметров структуры многопроцессорных программ, предназначенных для параллельной обработки данных. Для решения этой задачи авторы предлагают применять средства верификации моделей вычислительных систем, способные формировать контрпримеры по результатам проверки требований правильного поведения программ. Описанный в статье метод поиска оптимальных параметров конструкции вычислительных систем при помощи построения контрпримеров предусматривает представление исполнения абстрактной программы на абстрактной

модели многопроцессорной системы, формулировку свойства оптимальности в виде требования безопасности вычислений полученной абстрактной модели, применение алгоритма верификации формальной модели и выбор оптимальных значений параметров настройки вычислительной системы на основании анализа контрпримеров, полученных в ходе верификации.

В статье А.Р. Гнатенко и В.А. Захарова установлены оценки вычислительной сложности задач верификации автоматных моделей последовательных реагирующих систем и проверки выполнимости формул параметризованного расширения темпоральной логики линейного времени, которое авторы описали в своих более ранних работах. При помощи теоретико-автоматного подхода удалось показать, что эффективные решения обеих рассматриваемых задач можно получить, используя лишь полиномиально ограниченный объем памяти. В свете ранее полученных результатов это означает, что обе задачи являются PSPACE-полными.

Статья Д.А. Кондратьева посвящена исследованию одной из задач, которая возникла при выполнении долгосрочного проекта, проводимого в Институте систем информатики СО РАН, по созданию программно-инструментального комплекса C-lightVer для дедуктивной верификации С-программ. Эта задача связана с попытками расширить область применения проектируемого средства дедуктивной верификации и использовать его для проверки правильности программ, выполненных в системе облачного параллельного программирования CPPS, которая также разрабатывается в ИСИ СО РАН.

В статье А.М. Миронова излагается новая математическая модель распределенных вычислительных систем, предназначенная для верификации программ, которые выполнены с использованием программного интерфейса параллельного программирования MPI. Параллельная программа моделируется системой вычислительных процессов, взаимодействующих путем асинхронной передачи и приема сообщений по каналам связи. Главным преимуществом предложенной автором модели является возможность моделирования и верификации параллельных программ с неограниченно большим числом последовательных взаимодействующих процессов. На основе предложенной модели была проведена верификация MPI программы перемножения матриц.

H. de Nivelle предложил в своей статье оригинальный логический подход к построению систем типов данных, допускающий введение зависимых и индуктивно определяемых типов. Эта работа является частью проекта по разработке нового языка программирования, подходящего для применения в области математической логики. Так как логические формулы представляют собой древовидные структуры с множеством разнотипных конструкторов, алгоритмы их обработки должны учитывать согласование типов различных узлов таких деревьев. Наиболее часто такое согласование осуществляется путем сопоставления с образцом. Автор статьи предлагает иной подход: вместо сопоставления деревьев с разными шаблонами, соответствующими определениями типов, он предлагает использовать аппарат логического (табличного) вывода, исходя из системы определений типов и подтипов.