# НА ПУТИ К ВЕРИФИКАЦИИ СИ-ПРОГРАММ: СТАНДАРТНАЯ БИБЛИОТЕКА

**Промский А.В.**[1]

*Институт систем информатики им. А.П. Ершова СО РАН*
*630090 Новосибирск, просп. Лаврентьева, 6*
*E-mail: promsky@iis.nsk.su*

**Аннотация**

Для решения важной задачи верификации Си-программ в лаборатории теоретического программирования ИСИ СО РАН развит двухуровневый подход. Входной язык C-light является представительным подмножеством стандарта Си. Его формальное определение задано в виде операционной семантики. Суть двухуровневого подхода в том, что в языке C-light выделено ядро — язык C-kernel, в которое транслируются исходные программы. Были разработаны правила перевода из C-light в C-kernel, а также аксиоматическая семантика языка C-kernel, используемая для верификации. Были формально доказаны корректность перевода и непротиворечивость аксиоматической семантики относительно операционной.

Успешная разработка теоретических методов позволяет перейти к решению ряда практических задач, одной из которых является разработка логических спецификаций для стандартной библиотеки языка Си. Заметим, что эта проблема практически не отражена в литературе. Причиной является как низкий уровень многих функций библиотеки, так и отсутствие (до недавнего времени) удобного языка спецификаций Си-программ.

В данной работе описан подход к специфицированию библиотеки посредством языка ACSL. Изученное подмножество, названное Lib-light, включает такие важные средства, как файловый ввод-вывод, обработка строк, работа с памятью и математические функции. Спецификации включают в себя логические определения типов (в том числе рекурсивные), используемых в этих библиотеках, пред- и постусловия для библиотечных функций, а также инварианты циклов. Достоинством языка ACSL является нотация на основе самого языка Си, поэтому спецификации будут понятны не только теоретикам, но и программистам-практикам. Ряд библиотечных функций были не просто специфицированы, но и верифицированы в рамках двухуровневого метода.

1 Работа поддержана Лаврентьевским молодежным грантом СО РАН «*Верификация программ на языке С с эффективной локализацией ошибок*» и частично поддержана грантом РФФИ № 11-01-00028-а.