Аннотация проекта (ПНИЭР), выполняемого в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014 – 2020 годы»

Номер Соглашения о предоставлении субсидии/государственного контракта: 14.604.21.0051
Название проекта*:* Разработка методов и инструментов для дедуктивной верификации модулей ядра операционной системы Linux.
Основное приоритетное направление: Информационно-телекоммуникационные системы
Исполнитель: Федеральное государственное бюджетное учреждение науки Институт системного программирования Российской академии наук
Руководитель проекта: Хорошилов Алексей Владимирович
Должность: в.н.с.
E-mail: khoroshilov@ispras.ru

Ключевые слова: *верификация, дедуктивная верификация, доказательство правильности, доказательство корректности, инструменты верификации, информационная безопасность, надежность, операционная система, сертификация, формальные методы, ядро операционной системы*

Цель проекта

Целью проекта является разработка методов и инструментов дедуктивной верификации компонентов операционных систем.

Основные планируемые результаты проекта
Основными теоретическими результатами являются:
- разработка метода генерации модели памяти компонентов операционных систем с возможностью интерпретации участков памяти как объектов разных типов;
- разработка метода генерации моделей памяти разделяемой между несколькими потоками управления;
- разработка метода генерации условий верификации для программ, работающих с разделяемыми данными.

Основным практическим результатом является разработка экспериментального образца, реализующего предложенные методы дедуктивной верификации программ системного уровня на языке Си.

Краткая характеристика создаваемой/созданной научной (научно-технической, инновационной) продукции
Ключевыми характеристиками разрабатываемых методов и инструментов дедуктивной верификации является применимость к коду ядра ОС Linux и способность доказывать его корректность с учетом его многопоточности и использования в нем разнообразных механизмов синхронизации.
Основными особенностями кода модулей ядра операционной системы, которые полноценно не поддерживаются современными методами и инструментами дедуктивной верификации, являются:
- наличие работы с разделяемыми данными, т. е. с данными, которые могут

быть изменены параллельно выполняющимися функциями;
- наличие работы с состоянием потока управления, в котором выполняется функция;
- использование указателей на внутренние поля структур и адресная арифметика с такими указателями;
- наличие неявных преобразований типов посредством обращения к содержимому одной области памяти как к объектам разных типов;
- использование функциональных указателей.

Назначение и область применения, эффекты от внедрения результатов проекта

Разработанные методы дедуктивной верификации будут востребованы при разработке компонентов операционных систем, а также компонентов других уровней стека, применяемых в составе ответственных систем, то есть систем к которым предъявляются повышенные требования к надежности. Примерами таких систем являются системы управления на транспорте, в медицине, на энергетических и промышленных объектах, от корректности поведения которых зависят жизни людей, а также информационные системы от защищенности которых зависит сохранность персональных, коммерческих и государственных данных.

При появлении эффективных методов дедуктивной верификации компании, взявшие их на вооружения, получат дополнительные конкурентные преимущества на рынке разработки ответственных систем, поскольку у них появится возможность поставлять продукт с ранее недостижимым уровнем надежности. соответствующим максимальным уровням оценки надежности EAL6 и EAL7, определенным в международном стандарте по компьютерной безопасности ISO/IEC 15408, а также аналогам постепенно появляющимся в других отраслевых стандартах.

Потребителей предлагаемых методов и инструментов верификации можно разбить на три группы:
- Разработчики и поставщики программно-аппаратных решений для ответственного применения преимущественно в областях, где существуют регламенты по сертификации программных систем на соответствие требованиям надежности и безопасности.
- Разработчики и поставщики операционных систем, которые поставляют операционные системы, в частности, Linux для ответственных применений и нуждающихся в доказательной верификации и сертификации.
- Компании, специализирующиеся в верификации и сертификации программных систем.

Текущие результаты проекта

Разработаны следующие методы:
- метод генерации модели памяти компонентов операционных систем с

возможностью интерпретации участков памяти как объектов разных типов;
- метод генерации моделей памяти разделяемой между несколькими потоками управления;
- метод генерации условий верификации для программ, работающих с разделяемыми данными.