Национальный исследовательский университет –

«Высшая школа экономики»

Аспирантская школа по компьютерным наукам

Рецензия на доклад Ефремова Дениса, аспиранта первого года

на тему: «Формальная верификация модуля безопасности ядра Linux»

Доклад был посвящен проблеме формальной верификации модуля безопасности ядра Linux. В ходе доклада автор рассказал о требованиях к безопасности ядра, методах проверки этих требований, подробно останавливаясь на реализации подобных проверок для ОС AstraLinux.

В первой части было рассказано, что такое модель требований к безопасности ядра, и что она включает, также были даны определения уровням применения формальных методов.

Затем докладчик представил постановку своей задачи. В данной задаче, используя математическую модель Девянина П.Н., необходимо приблизить существующий нулевой уровень формализации к первому уровню для кода ядра ОС специального назначения AstraLinux. Также необходимо показать соответствие или несоответствие реализации её модели при помощи формальных методов. После этого была дана краткая историческая справка, посвященная истории дедуктивной верификации программ, и были обозначены основные ограничения этого метода.

Затем автором был представлен пример верификации кода функции на языке С. В ходе разбора этого примера были продемонстрированы основные программные средства, используемые автором в его работе.

В завершающей части докладчик перешел от рассказа о дедуктивной верификации к описанию динамической верификации и обозначил план своей дальнейшей работы.

В ходе ответов на вопросы автор показал хорошее знание темы своей работы. В следующем докладе хотелось бы услышать о каких-либо уже реализованных проектах по верификации программ и их результатах. В качестве пожелания можно посоветовать автору подробнее описывать и чаще использовать при рассказе схемы и диаграммы, представленные на слайдах.

Геннадий Федин

20.06.2016