

НАУЧНЫЙ ОТЧЕТ

О визите проф. Андрея Щедрова (Andre Scedrov) на математический факультет Национального исследовательского университета "Высшая школа экономики" (НИУ ВШЭ) и в Отдел математической логики Математического института им. В.А. Стеклова (МИАН) в рамках проекта фонда «Династия» «Краткосрочные визиты иностранных ученых в российские научные центры» 31.05-10.06 и 21.06-23.06 2013 года

Я посетил 31.05-10.06 и 21.06-23.06 2013 г. математический факультет НИУ ВШЭ и Отдел математической логики МИАН.

Во время визита мною был прочитан мини-курс «Analysis of Security Protocols» на факультете математики НИУ ВШЭ. Три 90-минутные лекции состоялись 3, 4 и 6 июня 2013 года, количество слушателей – около 15 человек. Среди слушателей были студенты и сотрудники факультета математики НИУ ВШЭ и сотрудники механико-математического факультета МГУ имени М.В. Ломоносова. В результате этих трех лекций было дано введение в область анализа и верификации протоколов защиты информации, а также представлены примеры успешного применения данных методов к анализу реальных промышленных протоколов.

Мною также были прочитаны две лекции «A Rewriting Framework for Activities Subject to Regulations» и «When Not All Bits Are Equal: Incorporating 'Worth' Into Information-Flow Measures» 5 июня 2013 года в Институте проблем передачи информации им. А.А. Харкевича (ИППИ РАН). На этих лекциях присутствовало 4 человека.

Я также участвовал в симпозиуме по математической логике и вычислимости «Logic and Computation Day» (МИАН, 7.06.2013) и сделал часовой доклад на тему «Bounded Memory Protocols and the Unbounded Adversary». Доклад был посвящен теоретическим результатам в области анализа протоколов в рамках модели Долева-Яо с ограничениями на количество доступной памяти.

Во время моего визита в Санкт-Петербург 14 июня 2013 года была прочитана лекция «Progressing Collaborative Systems, Bounded Protocols, and Unbounded Adversaries» в Лаборатории проблем компьютерной безопасности СПИИРАН. На лекции присутствовало около 15 человек.

В конце своего визита 22 июня 2013 года я также участвовал в конференции «Franco-Russian Workshop on Algorithms, Complexity and Applications 2013» (организаторы: Лаборатория Понселе и Независимый московский университет, 21-23.06.2013) и сделал доклад на тему «Collaborative Systems».

Кроме того, в течение визита состоялось много полезных обсуждений с коллегами из МГУ, ВШЭ, МИАН и ИППИ РАН и СПИИРАН, в частности с Л.Д. Беклемишевым, Д.С. Шамкановым, В.Б. Шехтманом, И.Б. Шапировским, А. Кудиновым, А. Мироновым, В.Н. Крупским, Р.М. Юсуповым, И.В. Котенко.

3 июля 2013 г.

А. Щедров (A. Scedrov)

