А. С. Михайлов, С. С. Селезнёв

Итерационный процесс разработки протоколов информационного обмена[1]

В современных условиях всесторонней информатизации общества и стремительного развития распределенных информационных систем, систем электронного документооборота, электронного бизнеса особую актуальность имеет задача разработки надежных и безопасных протоколов информационного обмена.

В самом общем случае протокол информационного обмена представляет собой последовательность передачи сообщений с применением вычислительных, в том числе криптографических, алгоритмов в процессе обработки данных. Спецификой протоколов является наличие в них возможных *несостоятельностей* — ситуаций, когда злоумышленник может причинить ущерб участникам протокола или когда цели протокола не достигаются [12, 14]. Наличие несостоятельностей в протоколах в некоторой степени схоже с наличием ошибок в программном обеспечении. Тестирование и верификация программного обеспечения являются общепризнанными необходимыми этапами процесса разработки программных продуктов. Подобным образом ставится вопрос об анализе моделей протоколов с целью выявления возможных несостоятельностей с последующим внесением исправлений.

На кафедре «Кибернетика» Национального исследовательского ядерного университета «МИФИ»[2] был предложен и исследован итерационный процесс для разработки протоколов, состоящий из трех основных этапов: визуальное моделирование протокола, анализ формальной математической модели протокола и практический анализ протокола в исследовательской среде информационного обмена (рис. 1).

Визуальные модели способствуют целостному восприятию моделируемых протоколов, используются для обмена знаниями между разработчиками. Визуальное моделирование позволяет представить протокол в форме диаграмм, показывающих участников протокола и их возможности (статическое представление), а также процессы взаимодействия между участниками (динамическое представление). На основе визуальных моделей возможна генерация формализованных моделей протоколов, например с использованием языка XML, что позволяет автоматически экспортировать модели между различными инструментальными средствами моделирования и анализа.

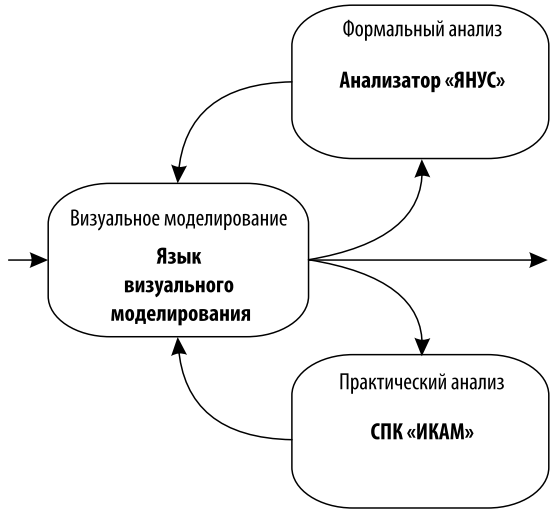

Рис. 1. Итерационный процесс разработки протоколов

[1] Статья подготовлена по результатам Всероссийской научно-практической конференции Московской финансово-промышленной академии «Развитие конкуренции на рынке информационных технологий» (25–26 марта 2009 г.). — *Прим. ред.*

[2] http://cyber.mephi.ru.