

УДК 004.7

Д.Ю.Руденко (магистр, каф. АиВТ), Л.К.Птицына, д.т.н., проф.

МОДЕЛИ, МЕТОДЫ И СРЕДСТВА ОПРЕДЕЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КЛАСТЕРНЫХ СИСТЕМ

Одно из направлений развития безопасных информационных технологий связано с обеспечением защиты информации кластерных систем. Многообразие сочетания новых технологий, применяемых при построении кластерных систем, предопределяет нестандартность решений при организации защиты информации. Известные теоретические исследования по организации защиты информации не принимают во внимание дуальные особенности кластерных систем, которые позволяют описывать кластеры, с одной стороны, как высокопроизводительные вычислительные системы, а, с другой стороны, как сети компьютеров. Созданные средства защиты информации кластерных систем не отвечают требованиям, которые предъявляются к сетям компьютеров. Более того, реализованная в них защита информации по типу вычислительных систем не предусматривает анализ достижимости целей и сопутствующих характеристик функционирования. Подобные обстоятельства предопределяют объективную необходимость развития методологий проектирования систем защиты информации в кластерах.

Формированию цели и задач исследований предшествовал анализ основных тенденций в развитии архитектуры кластерных систем, особенностей внедряемых коммуникационных технологий кластеров, их топологий, предъявляемых требований к информационной безопасности кластеров, угроз безопасности, необходимости сочетания различных механизмов безопасности кластерных структур.

Задачи исследований ориентированы на развитие известных подходов к интеграции отдельных механизмов защиты информации, расширение теоретических элементов по определению характеристик функционирования систем защиты информации кластеров и разработку программных средств для исследования влияния параметров, отражающих специфику архитектурных решений на поведение характеристик.

Характер поставленных задач отражает их научно-техническую направленность.

При построении моделей функционирования систем информационной безопасности кластеров обоснован выбор адекватного класса моделей, принципов декомпозиции моделей, базовых приемов построения моделей. Разработанные модели предусматривают различение трех видов ситуаций:

- обнаружение угроз при доступе к кластерной системе;
- обнаружение угроз при доступе к ресурсам кластерной системы;
- обнаружение угроз целостности информации.

Для каждой ситуации предложена серия моделей, вариации в которой отражают различные приемы интеграции механизмов защиты в условиях последовательной и последовательно-параллельной обработки информации.

В отличие от известных моделей расширено поле ситуаций и вариаций, что в большей степени соответствует архитектурным особенностям кластерных систем.

Посредством преобразования построенных моделей выведены новые аналитические соотношения для динамических характеристик систем информационной безопасности кластеров. Вывод выполнен на основе модифицированного метода свертки. При этом осуществлено развитие метода на обобщенный случай комплексирования последовательных

процессов согласно логической функции «ИЛИ». При выводе охвачен полный спектр построенных моделей.

Для нахождения количественных оценок динамических характеристик разработаны программные средства. Спланированный и реализованный эксперимент подтвердил корректность выполненной разработки.