XXXI Неделя науки СПбГПУ. Материалы межвузовской научной конференции. Ч. VI: С.106-107, 2003.

УДК 004.7

Д.Ю. Руденко (6 курс, каф. АиВТ), Л.К. Птицына, д.т.н., проф.

ОПРЕДЕЛЕНИЕ ХАРАКТЕРИСТИК ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КЛАСТЕРНЫХ СИСТЕМ

В последнее время наблюдается устойчивый рост потребности в высокомощных вычислениях, что влечет за собой непрерывное развитие высокопроизводительных вычислительных систем. Кластерные системы являются представительной группой параллельных вычислительных систем, обладающих высокой производительностью и отказоустойчивостью, хорошей масштабируемостью и доступностью.

Хотя требования к информационной безопасности подобных систем сегодня крайне высоки, при их разработке задачи обеспечения информационной безопасности не ставились совсем или им уделялось недостаточное внимание. В результате существующие системы безопасности кластерных систем примитивны и не удовлетворяют сегодняшним стандартам безопасности. Следует отметить, что обеспечение безопасности уже существующей системы в любом случае значительно менее эффективно, чем анализ и обеспечение безопасности системы еще на этапе ее синтеза. Поэтому высокой актуальностью в данный момент обладают такие задачи: разработка методов построения защищенных кластерных систем, анализ защищенности кластерных систем, то есть получение их характеристик безопасности, оценка эффективности систем информационной безопасности, создание моделей функционирования систем безопасности.

Существующие работы по разработке систем информационной безопасности в большинстве своем рассматривают не конкретные системы (например, кластерные), а автоматизированные системы или вычислительные системы/сети в целом. При этом все они обладают рядом серьезных недостатков: рассматривается общая структура системы безопасности, но не учитываются такие моменты, как взаимодействие ее компонентов между собой с учетом временных характеристик такого взаимодействия, взаимодействие системы безопасности с вычислительной системой на уровне ресурсов, влияние на производительность. Рассматриваются понятия поля угроз, объектов системы и механизмов безопасности, но не исследуется поведение системы в динамике с учетом многократного появления угроз, сбоев и восстановлений системы безопасности. Кроме того, разработанные модели часто никак не связаны с реальными параметрами и свойствами вычислительной системы и они не позволяют получить характеристики информационной безопасности вычислительных систем. Многие работы не ставят вопрос соответствия разработанных систем безопасности существующим стандартам безопасности.

В уже существующих моделях при обеспечении информационной безопасности выделяются базовые сервисы и специальные механизмы. В результате анализа архитектуры кластерных систем и сопоставления возможностей известных механизмов обеспечения информационной безопасности формируются модели функционирования системы информационной безопасности в кластерах. Модели включают различные услуги безопасности: аутентификация и идентификация, контроль доступа, обеспечение целостности и др.

Предлагается расширить класс подобных моделей для кластерных систем, прежде всего за счет учета следующих аспектов: размерность и топология кластера, телекоммуникационные технологии, технологии программирования, различные способы распределения задач обеспечения безопасности и обмена информацией внутри кластера. Ключевой особенностью является учет асинхронизма процессов реализации различных услуг безопасности, то есть будут учитываться как временные характеристики самих процессов, так и временные характеристики взаимодействия между ними по сети. Также предполагается учесть влияние работы системы безопасности на производительность кластера.

Построенные модели позволят получить динамические характеристики функционирования системы безопасности. На основе анализа полученных характеристик и самих моделей можно будет выделить наиболее эффективные структуры систем безопасности для кластеров. Разработчику и владельцу кластера будет предоставлен математический аппарат и конкретное программное обеспечение для анализа характеристик функционирования систем безопасности, которые позволят выбрать наилучшую структуру системы безопасности, оптимальную, с точки зрения безопасности, топологию, технологию и другие аспекты построения кластеров. Важно то, что данный математический аппарат можно будет применить на любом этапе существования кластерной системы для получения характеристик ее информационной безопасности и улучшения этих характеристик.

Кроме того, результаты решения указанных выше задач можно в той или иной мере перенести на высокопроизводительные системы вообще, на сети компьютеров.