УДК 004.056

**ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ РАСПРЕДЕЛЕННЫХ СВЯЗЕЙ**

П.С. Романов

*Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технологический университет»*

*119454, Москва, Россия*

В сегодняшнем мире сетей компьютеры редко работают в изоляции. Они сотрудничают друг с другом в целях обеспечения связи, распределения процессов обработки, передачи, хранения данных и т.д. Системы, которые используют такой коллаборативный подход в работе, и которые географически разбросаны на большой площади широко известны как распределенные системы.

Объединяя определения Таненбаума [1] и Кулуриса [2], можно сказать, что распределенная система — это приложение, которое взаимодействует с множеством рассредоточенных аппаратных средств и программным обеспечением для координирования действий нескольких процессов, выполняющихся на различных автономных компьютерах посредством связи через сеть, так что все компоненты аппаратного и программного обеспечения сотрудничают друг с другом для выполнения ряда задач, нацеленных на достижение общей цели.

Самыми популярными и широко используемыми видами распределенных систем в наше время являются:

* кластерные вычисления
* грид-вычисления
* распределенные системы хранения данных
* распределенные базы данных

Безопасность является одним из наиболее важных вопросов в распределенных системах. Когда данные распределяются по нескольким сетям или информация передается через общедоступные сети, она становится уязвимой для атак со стороны злоумышленников. Также, другие вычислительные ресурсы, такие как процессоры, устройства хранения данных, сети и т.д., также могут быть подвержены атакам.

В распределенных компьютерных системах угрозы информационной безопасности делятся на пассивные и активные [3]. Пассивные угрозы – это угрозы, целью которых является получение информации о системе во время прослушивания каналов передачи информации. Активные угрозы предусматривают воздействие на передаваемые сообщения и несанкционированную передачу информации по сети.

Обеспечение безопасности в кластерах несколько проще по сравнению с грид-сетями из-за однородности кластеров. Одна из основных атак, которым подвержены кластеры – атака «Отказа в обслуживании» (*DoS*). Для снижения урона от *DoS*-атак были предложены различные методы на основе цепей Маркова.

В грид-вычислениях уровень промежуточного программного обеспечения обеспечивает платформу для обеспечения безопасности на всей сети. Грид-системы используют сильную защиту на основе сертификатов *PKI* и *X.509*. Модуль аутентификации пользователей в сети обеспечивает защиту от угроз со стороны внешних источников и нелегальных действий со стороны внутренних пользователей.

Безопасность распределенных систем хранения данных в основном сосредоточена на обеспечении безопасности данных. Основные задачи, которые должна решать система безопасности распределенных хранилищ – защита от повреждения данных и защита данных в ситуациях сбоев узлов. В данной сфере были предложены различные модели и схемы для защиты системы хранения от атак и сбоев узлов.

В распределенной системе баз данных обеспечение безопасности усложняется из-за наличия различных моделей баз данных. Одним из самых часто применяемых решений вопроса обеспечения безопасности данных является организация многоуровневой системы безопасности, которая присваивает уровень безопасности каждой транзакции и всем данным и ограничивает операции, проводимые над базами данных на основе уровней безопасности [4].

Ни одна компьютерная система защиты информации не является абсолютно безопасной. Однако адекватные меры защиты значительно затрудняют доступ к системе и снижают эффективность усилий злоумышленников. Учитывая то, что распределенные системы все чаще и чаще используются крупными корпорациями и государственными службами, решение вопроса обеспечения безопасности таких систем является критически важным и требует внимания исследователей и разработчиков.

Список использованных источников

1. George Coulouris, Jean Dollimore, and Tim Kindberg, Distributed Systems - Concepts and Design, 4th ed. London, England: Addison - Wesley, 2005.

2. Andrew S Tanenbaum and Maarten van Steen, Distributed Systems: Principles and Paradigms, 2nd ed. Upper Saddle River, NJ, USA: Pearson Higher Education, 2007.

3. Артюхов Ю. В. Некоторые аспекты информационной безопасности в распределенной компьютерной системе // Молодой ученый. — 2011. — №2. Т.1. — С. 60-62.

4. Navdeep Kaur, Rajwinder Singh, A K Sarje, and Manoj Misra, "Performance evaluation of secure concurrency control algorithm for multilevel secure distributed database system," in International Conference on Information Technology: Coding and Computing (ITCC 2005), Las Vegas, NV, USA