BC/NW 2012; №1 (20): 9.2

**МОДЕЛЬ БЕЗОПАСНОСТИ
ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ**

О.А. Куликова, Е.А. Панкратова

Филиал Национального Исследовательского Университета МЭИ в г. Смоленске

Жизнь современного общества уже невозможно представить без сети Internet. Несмотря на все преимущества, которые дает использование глобальной сети, имеют место и негативные последствия, связанные с низким уровнем защищенности практически всех ее служб.

Компьютерные сети относятся к распределенным вычислительным системам (РВС), основными характеристиками которых являются: наличие нескольких центров обработки данных, отсутствие ограниченного периметра сети, а также изменяемое количество и состав объектов РВС.

Проведенный анализ существующих моделей РВС [1, 2] показал, что хотя данные модели точно отражает специфику процессов, происходящих в РВС, они имеет ряд недостатков:

1. Фактическое отсутствие универсальной модели РВС, обеспечивающей комплексную защиту от различных видов атак.
2. Ограниченный список сетевых операций, выполнение которых влечет за собой те или иные угрозы безопасности, целостности и работоспособности РВС.
3. Ряд моделей РВС основывается на предположении, что распределенная вычислительная система абсолютно безопасна, другие же модели включают множество заранее предопределенных угроз и множество барьеров, препятствующих успешной реализации конкретных угроз.

Таким образом, все существующие модели РВС являются статичными, учитывают только те угрозы, которые известны на момент создания РВС.

Для того чтобы учесть данные недостатки, предлагается модель РВС, включающая 3 концепции безопасности: конфиденциальность, целостность и защиту от атак «Отказ в обслуживании».

Модель основывается на следующих положениях:

1. В основе лежит модель безопасности сети, предложенная Varadharajan [3]. Но в этой модели не рассматриваются такие операции, как выполнение, создание и удаление сетевых объектов и не учитывается необходимость закрытия соединения после окончания сеанса обмена.
2. При описании операций манипуляции информацией (чтение, запись, удаление и т.д.) используются правила моделей Белла-Лападула и Биба. Но в разрабатываемой модели РВС решается проблема объединения правил данных моделей для обеспечения и безопасности, и целостности системы.
3. Для оценки времени перехода из одного состояния в другое использована модель распределенных ресурсов Миллена. Но в разрабатываемой модели РВС к правилам модели Миллена добавлены правила предоставления ресурсов с учетом приоритета и сформулированы условия защиты от угроз отказа в обслуживании.
4. Разработанная модель РВС описывает методы защиты от атак, относящихся к разным группам по цели воздействия.

Модель РВС MODEL представляет собой набор:



где *S* – множество состояний объектов и субъектов, составляющих модель РВС; *s*0∈*S* – начальное состояние системы. Предполагается, что начальное состояние системы *s*0 является безопасным. *O* – множество операций системы, в результате выполнения операции осуществляется переход из одного состояния в другое [*si*→*sj*, *i*=0..*N*, *j*=0..*N*].

В первом приближении данная модель может быть представлена в виде растущего автомата Мура, где *S* определяет состояние автомата, множество операций *O* – входной алфавит автомата, а функция переходов автомата определяется свойствами модели, набором состояний и составом операций. Результат работы модели полностью определяется ее состояниями.

РВС может находиться в трех состояниях: в безопасном состоянии, под воздействием атаки, в неисправном состоянии. Описание каждого состояния включает в себя множества субъектов, объектов, связи между ними, степени их доверия и целостности, список доступа, а также роли пользователя.

Все операции в зависимости от выполняемых функций разбиты на следующие группы: операция связи; операция получения доступа; операция освобождения; операция манипуляции информацией; операции, модифицирующие атрибуты безопасности объектов и субъектов. При разработке модели РВС особое внимание было уделено таким операциям, как создание новых объектов, удаление объектов, выполнение операций на удаленном объекте.

**Литература**

1. **Девянин П.Н.** Модели безопасности компьютерных систем. М.: Академия, 2005.

2. **Зегжда Д.П., Ивашко А.М.** Основы безопасности информационных систем. – М.: Горячая линия-Телеком, 2000.

3. **Vijay Varadharajan.** A multilevel security policy for networks, 1990.