XXXII Неделя науки СПбГПУ. Материалы межвузовской научно-технической конференции. Ч.V : С.169-170

УДК 50.41.00

А.Г.Лысенко (5 курс, каф. ИБКС), М.О.Калинин, ст. преп.

РАЗРАБОТКА АВТОМАТИЧЕСКОГО СРЕДСТВА ОЦЕНКИ ЗАЩИЩЕННОСТИ ОПЕРАЦИОННЫХ СИСТЕМ

Современные операционные системы достаточно сложны. В каждой операционной системе присутствуют множество субъектов, которые осуществляют доступ к множеству объектов. Доступ определяется атрибутами безопасности. Эти множества изменяются в процессе эксплуатации системы. Следовательно, в каждый момент времени безопасность системы характеризуется безопасностью ее состояния, т.е. множествами субъектов, объектов, их атрибутов и отношениями между ними.

Полностью проверить соответствие атрибутов безопасности операционной системы правилам политики безопасности администратором вручную затруднительно. Поэтому сегодня актуальна проблема выработки универсальных средств, осуществляющих автоматическую проверку защищенности системы, позволяющих прогнозировать поведение системы в будущем.

В СЦЗИ СПБГПУ ведется разработка автоматизированного программного комплекса оценки защищенности операционных систем. В состав комплекса входит анализатор начального состояния, правила контроля доступа и критерии безопасности (рис.1).

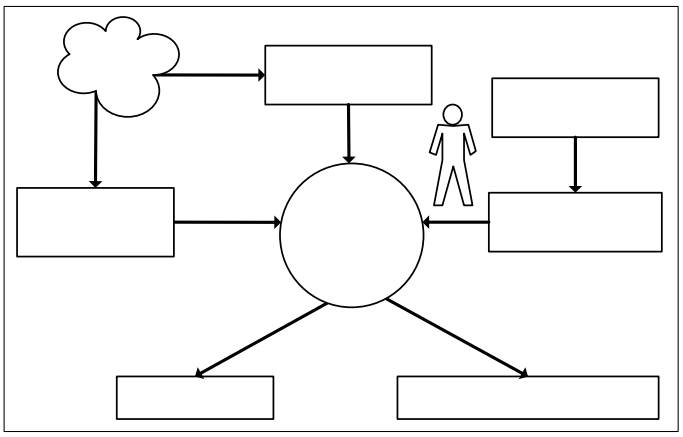

Рис. 1. Состав автоматизированного программного комплекса оценки защищенности операционных систем

Анализатор начального состояния формирует начальное состояние ОС. Эксперт задает правила контроля доступа для ОС WIN2000. На основе правил политики безопасности он формирует критерии безопасности.

Требуется средство, которое производило бы обработку логических описаний, задаваемых анализатором начального состояния и экспертом. Это и определило цель данной работы (данное средство получило название анализатор защищенности).

В качестве цели данной работы выступает разработка автоматического, независимого от оцениваемой системы программного средства оценки защищенности операционных систем.

Назначение программного комплекса на базе А3:

- оценка существующих систем на предмет соответствия текущих установок безопасности заданным правилам политики безопасности;
- оценка разрабатываемых средств защиты информации на предмет корректности архитектуры информационной системы, сформулированных правил контроля доступа, значений по умолчанию.

В процессе выполнения работы был предложен новый подход к оценке защищенности ОС, который базируется на начальном состоянии системы, генерации новых состояний и их оценке. За счет использования начального состояния обеспечивается независимость от оцениваемой операционной системы. В связи с проведением оценки на основе указанных описаний возможна оценка защищенности информационных систем, отличных от операционных систем. Данное средство послужило базой для построения автоматизированного комплекса средств оценки защищенности операционных систем.

При оценке защищенности информационных систем рекомендуется совместное использование автоматизированного комплекса оценки защищенности на базе АЗ и средств моделирования атак.

Анализатор защищенности может применяться для оценки защищенности как существующих информационных систем, так и для разрабатываемых, для которых возможно задание описания начального состояния системы, правил контроля доступа и критериев безопасности.