УДК 519.63

Об аналитической модели повышения надёжности управления информационной безопасностью

Кочуров В.А., Харма Укба
Белорусский национальный технический университет

Защита информации в корпоративной информационной системе является весьма сложной подсистемой, поскольку уязвимыми являются буквально все основные структурно-функциональные элементы КС: рабочие станции, серверы (Host-машины), межсетевые мосты (шлюзы, центры коммутации), каналы связи и т.д. При этом применяются различные методы и средства защиты информации в сетях:

- физическая защита информации;
- аппаратные средства защиты информации;
- программные средства защиты информации;
- обеспечение безопасности на уровне операционной системы и т.п.

Современное требование постоянного повышения надёжности управления информационной безопасностью и необходимость анализа с целью совершенствования функционирования и повышения эффективности обусловливают необходимость применения специальных средств описания и анализа таких систем.

Применяемая для таких целей методологии IDEF0, являющаяся графическим языком, ориентирована только на ***визуальное восприятие специалистами***. Однако представление сложной системы посредствам большого числа IDEF0-диаграмм встречается с другим барьером сложности – необходимостью зрительного анализа большого количества графического материала. Кроме того система управления информационной безопасностью требует принятия оперативных решений и, следовательно, нуждается в соответствующей Системе Поддержки Принятия Решений (СППР).

Разработанная на кафедре САПР БНТУ методика и модель представления сложных объектов обеспечивают возможность занесения комплекта IDEF0-диаграмм, описывающих сложную систему, в базу данных и проведения соответствующего OLAP-анализа. На основе результатов OLAP-анализа требуется принятие соответствующих решений, для чего служит в качестве ядра СППР управления информационной безопасностью корпоративной информационной системы, созданный на основе упомянутой методики прототип программного продукта - Сервер информационно-логических таблиц (СИЛТ). СИЛТ позволяет создать базу правил в формате «Если..То» над базой данных комплекта IDEF0-диаграмм.