XXXI Неделя науки СПбГПУ. Материалы межвузовской научной конференции. Ч. VI: С.103-104, 2003.

УДК 004.436:004.457

А.В. Матвеев (6 курс, каф. АиВТ), В.М. Ицыксон, к.т.н., доц

УПРАВЛЯЕМЫЙ ЯЗЫКОМ АНАЛИЗАТОР ФАЙЛОВ ПРОТОКОЛОВ

В последнее время значительно возросла ценность информации. Поэтому современные информационные системы нуждаются в качественном управлении, мониторинге и обеспечении должного уровня безопасности. В частности, одним из важных этапов в решении указанных задач, является регулярный анализ файлов протоколов работы модулей и программ, входящих в состав информационной системы. Своевременное обнаружение событий, указывающих прямо или косвенно на отклонения от нормальной работы, позволяет предотвратить потерю, порчу или кражу информации и, как следствие, предотвращение значительных временных и материальных затрат на восстановление работоспособного состояния системы. Так же это позволяет определить и оптимально распределять нагрузку на отдельные составляющие и всю систему в целом.

При решении задач администрирования приходиться решать такие задачи как:

- Контроль сетевой активности;
- Процент использования файловой системы;
- Процент использования CPU;
- Активность пользователей;
- Использование сервисов;
- Учет трафика и т.д.

Существующие на сегодняшний момент средства анализа файлов отчетов, обеспечивают, в основном, лишь простой подсчет количества событий или указанных величин, характеризующих состояние информационной системы. В этих программах не уделено достаточного внимания именно анализу происходящих событий.

Предлагаемая концепция построения универсального анализатора предлагает наличие встроенных средств, позволяющих описывать форматы исходных данных (файлы протоколов), целей анализа и действий при достижении(или не достижении) этих целей. Предлагается заменить множество настроек и конфигурационных файлов – языком описаний. Такой язык будет иметь характерные черты и элементы традиционных языков программирования, таких как функция, переменная и прочие, но при этом его ориентация направлена на решение указанной задачи. Предлагается наличие небольшого числа синтаксически простых языковых конструкций, допускающих вложенность, позволяющих описывать алгоритмы анализа записей файла протокола. Так же должна присутствовать возможность описания способа представления результатов анализа.

Таким образом, для решения задач администрирования, вместо огромного количества разнородных программ, достаточно будет иметь всего лишь одна утилиту и несколько файлов с описаниями для каждой из задач. Разработка и внедрение такого универсального анализатора позволит упростить процесс администрирования информационных систем, повысить надежность и качество их работы.