А. А. Шагун, А. В. Баранов

(ГрГУ им. Я. Купалы, Гродно)

УТИЛИТА АНАЛИЗА СИСТЕМНЫХ

ПРОЦЕССОВ, СЛУЖБ И ЛОГИРОВАНИЯ

ОПЕРАЦИОННОЙ СИСТЕМЫ WINDOWS

На компьютере с установленной ОС Windows запись событий ведется в трех журналах: журнале приложений, журнале безопасности и журнале системы. В журнале приложений содержатся информация о событиях, связанных с работой программ. Например, программа работы с базами данных может записать в журнал приложений ошибку доступа к файлу. В журнал безопасности записываются такие события, как удачные и неудачные попытки входа в систему, а также события, связанные с использованием ресурсов (такие как создание, открытие или удаление файлов). В журнале системы содержатся события, записанные системными компонентами Windows. Например, если происходит сбой загрузки драйвера при запуске системы, соответствующее информация о нем записывается в журнал системы.

К сожалению, в журналах Windows информация хранится в неудобном для пользователей виде. Поэтому актуальна разработка приложения, которое устранило бы эту проблему: предоставляло бы пользователю подробную информацию об ошибке и сохраняло её в базу данных, которая могла бы использоваться другими программами. Также приложение должно помогать оперативно следить за запущенными процессами и сервисами, потеря работоспособности которых очень нежелательна для функционирования системы.

Нами разрабатывается учебная утилита, которая позволяет решать проблему получения и анализа данных лог-файлов, а также контроля за запущенными процессами и сервисами операционной системы Windows. Используя ее возможности можно оперативно получать информацию о состоянии системы разными способами: через web-интерфейс, интерфейс самого приложения, а также посредством отправки сообщений на e-mail или некоторую систему мгновенных сообщений. Не смотря на то, что существует ряд программ, которые используются для решения подобных задач, данная утилита актуальна и представляет как теоретический интерес, так и способствует получению глубоких практических навыков.

Утилита в первую очередь рассчитана на применение системными администраторами, но может быть использована обычными пользователям. Она может настраиваться на разные уровни уведомления пользователей о нарушении безопасности или же каких-либо системных ошибках. В случае возникновения ошибки или нарушения пользователь мгновенно информируется о данном событии. В уведомлении будет указываться характер события, уровень ошибки, наименование процесса или сервиса, с которым связана данная ошибка.