

Windows_logs

Запустить утилиту “Журнал событий Windows” можно из классической Панели управления, перейдя по цепочке *Администрирование – Просмотр событий* или выполнив в окошке Run (Win+R) команду **eventvwr.msc**

Наибольший интерес представляет раздел «Журналы Windows», именно с ним чаще всего приходится работать, выясняя причины неполадок в работе системы и программ. Журнал системных событий включает три основных и две дополнительных категории. Основные это «Система», «Приложения» и «Безопасность», дополнительные – «Установка» и «Перенаправленные события».

Категория «Система» содержит события, сгенерированные системными компонентами – драйверами и модулями Windows. Это наиболее важный журнал. С его помощью можно определить большинство ошибок ОС.

Категория «Приложения» включает записи, созданные различными программами. Эти данные могут пригодиться как системным администраторам и разработчикам программного обеспечения, так и обычным пользователям, желающим установить причину отказа той или иной программы.

Категория «Безопасность» содержит сведения, связанные с безопасностью системы. К ним относятся входы пользователей в аккаунты, управление учётными записями, изменение разрешений и прав доступа к файлам и папкам, запуск и остановка процессов и так далее.