Windows_logs:
- инструкция для открытия журнала событий Windows;
- журналы: Система, Приложение, Безопасность.

В ОС линейки Windows производится регистрация всех основных событий, которые происходят в системе с последующей их записью в журнале. Записываются ошибки, предупреждения и просто различные уведомления. На основе этих записей опытный пользователь может подкорректировать работу системы и устранить ошибки.

Как открыть журнал событий в Windows 7? Журнал событий хранится в системном инструменте, который имеет название **«Просмотр событий»**.

Рассмотрим несколько способов перехода в него.

Способ 1: «Панель управления»

Один из самых распространенных способов запуска описываемого в данной статье инструмента, хотя далеко не самый легкий и удобный, осуществляется с помощью **«Панели управления»**.

1. Щелкните **«Пуск»** и перейдите по надписи **«Панель управления»**.
2. Затем зайдите в раздел **«Система и безопасность»**.
3. Далее щелкайте по наименованию раздела **«Администрирование»**.
4. Попав в указанный раздел в перечне системных утилит ищите наименование **«Просмотр событий»**. Кликните по нему.
5. Целевой инструмент активирован. Чтобы конкретно попасть в журнал системы, кликните по пункту **«Журналы Windows»** в левой области интерфейса окошка.
6. В открывшемся списке выбирайте один из пяти интересующих вас подразделов:
   - Приложение;
   - Безопасность;
   - Установка;
   - Система;
   - Перенаправление события.

   В центральной части окна отобразится журнал событий, соответствующий выбранному подразделу.
7. Аналогичным образом можно раскрыть раздел **«Журналы приложений и служб»**, но там будет больший перечень подразделов. Выбор конкретного из них приведет к отображению в центре окна списка соответствующих событий.

Способ 2: Средство «Выполнить»

Намного проще инициировать активацию описываемого инструмента при помощи средства **«Выполнить»**.

1. Задействуйте комбинацию клавиш **Win+R**. В поле запустившегося средства вбейте:
   eventvwr
   Кликните **«OK»**.

2. Нужное окно будет открыто. Все дальнейшие действия по просмотру журнала можно производить по тому же алгоритму, который был описан в первом способе.

Базовый недостаток этого быстрого и удобного способа заключается в необходимости удержать в уме команду вызова окна.

Способ 3: Поле поиска меню «Пуск»

Очень похожий метод вызова изучаемого нами инструмента осуществляется с задействованием поля поиска меню **«Пуск»**.

1. Щелкните **«Пуск»**. Внизу открывшегося меню расположено поле. Введите туда выражение:
   eventvwr

   Или просто напишите:

   Просмотр событий
   В списке выдачи в блоке **«Программы»** появится наименование **«eventvwr.exe»** или **«Просмотр событий»** в зависимости от введенного выражения. В первом случае, скорее всего, результат выдачи будет единственным, а во втором их будет несколько. Кликните по одному из указанных выше названий.

2. Журнал будет запущен.

Способ 4: «Командная строка»

Вызов инструмента через **«Командную строку»** довольно неудобен, но и такой способ существует, а поэтому он тоже стоит отдельного упоминания. Сначала нам потребуется вызвать окно **«Командной строки»**.

1. Щелкайте **«Пуск»**. Далее выбирайте **«Все программы»**.
2. Переходите в папку **«Стандартные»**.
3. В перечне открывшихся утилит щелкайте по **«Командная строка»**. Активацию с административными полномочиями производить не обязательно.
   Можете выполнить запуск и быстрее, но для этого нужно помнить команду активации **«Командной строки»**. Наберите **Win+R**, инициировав тем самым запуск инструмента **«Выполнить»**. Введите:
   cmd
   Щелкайте **«OK»**.
4. При любом из двух вышеуказанных действий будет запущено окно **«Командной строки»**. Введите знакомую команду:
   eventvwr
   Жмите **Enter**.

5. Окно журнала будет активировано.

Способ 5: Прямой старт файла eventvwr.exe

Можно воспользоваться таким «экзотическим» вариантом решения поставленной задачи, как прямой старт файла из **«Проводника»**. Тем не менее, и данный способ может пригодиться на практике, например, если сбои достигли такого масштаба, что другие варианты запустить инструмент просто недоступны. Такое бывает крайне редко, но вполне возможно.

Прежде всего, необходимо перейти в место нахождения файла eventvwr.exe. Он расположен в системном каталоге по такому пути:

C:\Windows\System32

1. Запустите **«Проводник Windows»**.
2. Вбейте в адресное поле тот адрес, который был представлен ранее, и кликните **Enter** или нажмите по значку справа.
3. Выполняется перемещение в каталог **«System32»**. Именно тут хранится целевой файл **«eventvwr.exe»**. Если у вас не включен в системе показ расширений, то объект будет называться **«eventvwr»**. Найдите и произведите по нему двойной клик левой кнопкой мышки (**ЛКМ**). Чтобы легче осуществлять поиск, так как элементов довольно много, можете отсортировать объекты по алфавиту, кликнув по параметру **«Имя»** вверху списка.

4. Произойдет активация окна журнала.

Способ 6: Введение пути к файлу в адресной строке

При помощи **«Проводника»** можно запустить интересующее нас окно и быстрее. При этом даже не придется искать eventvwr.exe в каталоге **«System32»**. Для этого в адресном поле **«Проводника»** просто нужно будет указать путь к данному файлу.

1. Запустите **«Проводник»** и введите в адресное поле такой адрес:
   C:\Windows\System32\eventvwr.exe
   Кликните **Enter** или нажмите по эмблеме стрелки.

2. Окно журнала тут же активируется.

Способ 7: Создание ярлыка

Если вы не хотите запоминать различные команды или переходы по разделам **«Панели управления»** считаете слишком неудобными, но при этом часто пользуетесь журналом, то в таком случае можете сформировать иконку на **«Рабочем столе»** или в другом удобном для вас месте. После этого запуск инструмента **«Просмотр событий»** будет осуществляться максимально просто и без необходимости что-то запоминать.

1. Перейдите на **«Рабочий стол»** или запустите **«Проводник»** в том месте файловой системы, где собираетесь создать иконку доступа. Кликните правой кнопкой мышки по пустой области. В меню переместитесь по **«Создать»** и далее щелкайте **«Ярлык»**.

2. Активируется инструмент формирования ярлыка. В открывшееся окошко внесите тот адрес, о котором уже шла речь:

   C:\Windows\System32\eventvwr.exe
   Кликните **«Далее»**.

3. Запускается окошко, где нужно указать наименование иконки, по которому юзер будет определять активируемый инструмент. По умолчанию в качестве названия используется имя исполняемого файла, то есть, в нашем случае **«eventvwr.exe»**. Но, конечно, это название мало что может сказать непосвященному пользователю. Поэтому лучше в поле ввести такое выражение:
   Журнал событий

   Или такое:

   Просмотр событий
   В общем, введите любое название, по которому вы будете ориентироваться, какой инструмент данная иконка запускает. После ввода жмите **«Готово»**.

4. Иконка запуска появится на **«Рабочем столе»** или в другом месте, где вы её создали. Для активации инструмента **«Просмотр событий»** достаточно кликнуть по ней дважды **ЛКМ**.

5. Необходимое системное приложение будет запущено.

Проблемы с открытием журнала

Бывают такие случаи, когда возникают проблемы с открытием журнала вышеописанными способами. Чаще всего это происходит из-за того, что отвечающая за работу данного инструмента служба деактивирована. При попытке запуска инструмента **«Просмотр событий»** отобразится сообщение, где говорится о том, что служба журнала событий недоступна. Тогда необходимо произвести её активацию.

1. Прежде всего, нужно перейти в **«Диспетчер служб»**. Это можно сделать из раздела **«Панели управления»**, который называется **«Администрирование»**. Как в него перейти, подробно описывалось при рассмотрении **Способа 1**. Попав в данный раздел, ищите пункт **«Службы»**. Кликните по нему.
   В **«Диспетчер служб»** можете перейти с помощью средства **«Выполнить»**. Вызовите его, набрав **Win+R**. В область для ввода вбейте:
   services.msc

Жмите **«OK»**.

2. Независимо от того, совершили вы переход через **«Панель управления»** или использовали ввод команды в поле инструмента **«Выполнить»**, запускается **«Диспетчер служб»**. В списке ищите элемент **«Журнал событий Windows»**. Чтобы облегчить поиск, можете выстроить все объекты перечня в алфавитном прядке, кликнув по названию поля **«Имя»**. После того, как нужная строка найдена, взгляните на соответствующее ей значение в колонке **«Состояние»**. Если служба включена, то там должна находиться надпись **«Работает»**. Если же там пусто, то это означает, что служба деактивирована. Также посмотрите на значение в колонке **«Тип запуска»**. В нормальном состоянии там должна находиться надпись **«Автоматически»**. Если там стоит значение **«Отключена»**, то это означает, что служба не активируется при запуске системы.
3. Чтобы это исправить, перейдите в свойства службы, кликнув по наименованию дважды **ЛКМ**.
4. Открывается окно. Кликните по области **«Тип запуска»**.
5. Из раскрывшегося списка выбирайте **«Автоматически»**.
6. Жмите по надписям **«Применить»** и **«OK»**.
7. Возвратившись в **«Диспетчер служб»**, отметьте **«Журнал событий Windows»**. В левой области оболочки кликните по надписи **«Запустить»**.
8. Запуск службы произведен. Теперь в соответствующем ей поле колонки **«Состояние»** отобразится значение **«Работает»**, а в поле колонки **«Тип запуска»** появится надпись **«Автоматически»**. Теперь журнал можно открыть любым из тех способов, которые мы описывали выше.

Существует довольно много вариантов активировать журнал событий в Виндовс 7. Конечно, самые удобные и популярные способы – это переход через **«Панель инструментов»**, активация при помощи средства **«Выполнить»** или поля поиска меню **«Пуск»**. Для удобного доступа к описываемой функции можете создать иконку на **«Рабочем столе»**. Иногда возникают проблемы с запуском окна **«Просмотр событий»**. Тогда нужно проверить, активирована ли соответствующая служба.

Журналы: Система, Приложение, Безопасность

В операционной системе Windows 7, так же как и в Windosw Vista, существуют две категории журналов событий: **журналы Windows** и **журналы приложений и служб**. **Журналы Windows** – используются операционной системой для регистрации общесистемных событий, связанных с работой приложений, системных компонентов, безопасностью и запуском. А **журналы приложений и служб** – используются приложениями и службами для регистрации событий, связанных с их работой. Для управления журналами событий можно использовать оснастку **«Просмотр событий»** или программу командной строки *wevtutil*, о которой будет рассказано во второй части статьи. Все типы журналов описаны ниже:

Система – хранит события операционной системы или ее компонентов, например неудачи при запусках служб или инициализации драйверов, общесистемные сообщения и прочие сообщения, относящиеся к системе в целом. По умолчанию помещается в %SystemRoot%\System32\Winevt\Logs\System.Evtx

Приложение – хранит важные события, связанные с конкретным приложением. Например, Exchange Server сохраняет события, относящиеся к пересылке почты, в том числе события информационного хранилища, почтовых ящиков и запущенных служб. По умолчанию помещается в %SystemRoot%\System32\Winevt\Logs\Application.Evtx.

Безопасность – хранит события, связанные с безопасностью, такие как вход/выход из системы, использование привилегий и обращение к ресурсам. По умолчанию помещается в %SystemRoot%\System32\Winevt\Logs\Security.Evtx