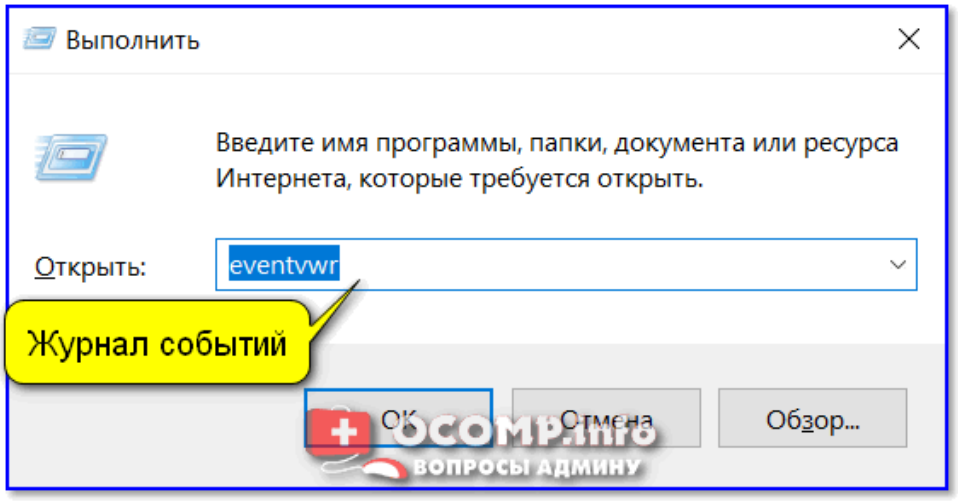
Инструкция для открытия журнала событий Windows

Вариант 1

Этот вариант универсальный и работает во всех современных версиях ОС Windows.

1. Нажать сочетание кнопок ***Win+R*** — должно появиться окно "Выполнить".
2. Ввести команду ***eventvwr*** и нажать ОК (примечание: также можно воспользоваться диспетчером задач (Ctrl+Shift+Esc) — нажать по меню *"Файл/новая задача"* и ввести ту же команду *eventvwr*).



eventvwr — команда для вызова журнала событий

3. По умолчанию, *Просмотр событий* откроет вкладки, в том числе со сводкой административных событий, где перечислена информация по важности для администратора.

Вариант 2

1. Сначала необходимо открыть *Панель управления* и перейти в раздел *"Система и безопасность"*.
2. Далее необходимо перейти в раздел *"Администрирование"*.
3. После кликнуть мышкой по ярлыку *"Просмотр событий"*.

Вариант 3

Актуально для пользователей Windows 10/11.

1. Нажать по значку с "лупой" на панели задач, в поисковую строку написать "событий" и в результатах поиска ОС Windows предоставит вам ссылку на журнал (см. скрин ниже).

2. Еще один способ: нажать сочетание **Win+X** — появится меню со ссылками на основные инструменты, среди которых будет и журнал событий.

Журналы Windows

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».

Журнал событий Приложение

Журнал событий **Приложение** содержит события, сгенерированные приложениями, а не системой. Например, сервер базы данных может записывать ошибки, возникающие при его работе в журнал приложений. Разработчики программ сами решают какие события имеет смысл протоколировать в журнале событий Приложение, а какие – в журнале приложений и служб. Например, Microsoft SQL Server протоколирует подробную информацию о важных аварийных ситуациях, возникающих при работе SQL-сервера, таких как "недостаточно памяти", "сбой при резервном копировании базы данных" и т.д. При этом события, сгенерированные разными приложениями, попадают в единый журнал приложений. Приложения идентифицируются как разные "источники" в базовом свойстве событий. Поэтому несложно выделить события конкретного приложения. Также стоит учитывать, что ID события (код события) тоже определяется приложением, сгенерировавшим событие, коды могут дублироваться для разных источников. Таким образом события определенного типа идентифицируются и источником, и кодом, а не только кодом, как для других журналов, например, для журнала Безопасность.

Журнал событий Система

Журнал событий Система содержит события, сгенерированные системными компонентами. Например, отказы драйверов или других системных компонентов при запуске системы записываются в системный журнал событий. Типы и коды событий системных компонентов предопределены разработчиками операционной системы Windows. Аналогично журналу приложений, системный журнал содержит события из разных источников (системных компонентов) и следует учитывать, что конкретные события идентифицируются не только кодом, но источником. Журнал событий Система - важный источник информации при поиске причин отказов и проблем системными администраторами и техническими специалистами.

Журнал событий Безопасность

Журнал событий Безопасность содержит события, влияющие на безопасность системы. Это попытки (удачные и неудачные) входа в аккаунты системы, использование ресурсов (файлов, реестра, устройств), управление учетными записями, изменения прав и привилегий аккаунтов, запуск и остановка процессов

(программ) и т.д. Администратор может сконфигурировать какие категории событий необходимо регистрировать. Например, по умолчанию система сконфигурирована регистрировать события управления учетными записями, события входа в систему, а аудит доступа к объектам не включен. Стоит быть осторожным при настройке аудита доступа к файлам, так как это может привести к появлению большого количества событий, что в свою очередь может негативно отразиться на общей производительности системы и быстрому переполнению журнала безопасности.

Запись в журнал безопасности производится только системными компонентам, коды событий однозначно идентифицируют события. Журнал событий Безопасность является важным источником информации при расследовании инцидентов нарушения безопасности и его анализ актуален для администраторов безопасности, специалистов по информационной безопасности и специалистов по цифровой криминалистической экспертизе.

Сами события также разделяются на типы:

- **Сведения (Information)** — информируют о штатной работе приложений.
- **Предупреждение (Warning)** — событие, свидетельствующее о возможных проблемах в будущем (например, заканчивается свободное место на диске – приложения могут продолжать работу в штатном режиме, но, когда место закончится совсем, работа будет невозможна).
- **Ошибка (Error)** — проблема, ведущая к деградации приложения или службы, потерям данных.
- **Критическое (Critical)** — значительная проблема, ведущая к неработоспособности приложения или службы.
- **Аудит успеха (Success audit)** — событие журнала **Безопасность (Security)**, обозначающее успешно осуществленное действие, для которого включено отслеживание (например, успешный вход в систему).
- **Аудит отказа (Failure audit)** — событие журнала **Безопасность (Security)** обозначающее безуспешную попытку осуществить действие, для которого включено отслеживание (например, ошибка входа в систему).