**EVENT LOG** – журнал событий windows, это средство, позволяющее программам и самой системе Windows регистрировать и хранить уведомления в одном месте. В журнале регистрируются все ошибки, информационные сообщения и предупреждения программ.

Команда для открытия **EVENTVWR**

Логи можно экспортить. Выбираем лог > **save selected logs**

Логи можно копировать. Нажимаем 2 раза на лог > нажимаем **copy** в открывшемся окне

Логи можно очищать – **clear log…**

**Application** – логи приложения

**Security** – вход в систему/выход из системы, вход в домен/выход из домена, любое событие безопасности, …

**Setup** – логи установки

**System** – системные логи

**Forwarded** **Event** – те события которые пришли с другого сервера

Виды событий

| **Тип** | **Описание** |
| --- | --- |
| Информация | События указывают редкие и важные успешные операции. |
| Предупреждение | События указывают проблемы, которые не требуют немедленного вмешательства, но могут привести к ошибкам в будущем. Примером такого рода событий может служить исчерпание ресурсов. |
| Ошибка | События указывают существенные проблемы, обычно приводящие к потере функциональности или данных. Примером может служить невозможность запуска службы при загрузке. |
| **Security** Успешный аудит | События безопасности, которые происходят при успешном обращении к аудируемым ресурсам. Примером может служить успешный вход в систему. |
| **Security** Не успешный аудит | События безопасности, которые происходят при неуспешном обращении к аудируемым ресурсам. Примером может служить попытка открыть файл, не имея соответствующих прав доступа. |