Министерство образования Новосибирской области

ГБПОУ НСО «Новосибирский авиационный технический колледж имени Б.С.Галущака»

Лабораторная работа 8

Работа с программой «Просмотр событий»

Учебная дисциплина: Операционные системы и среды

Выполнил: студент группы ПР-20.101

Савриков И.В

Проверил: Холин А.А.

2022

1 Цель

1.1 Научиться работать с журналами событий ОС Windows

1. Ход работы

2.1 Запустите программу Просмотр событий.

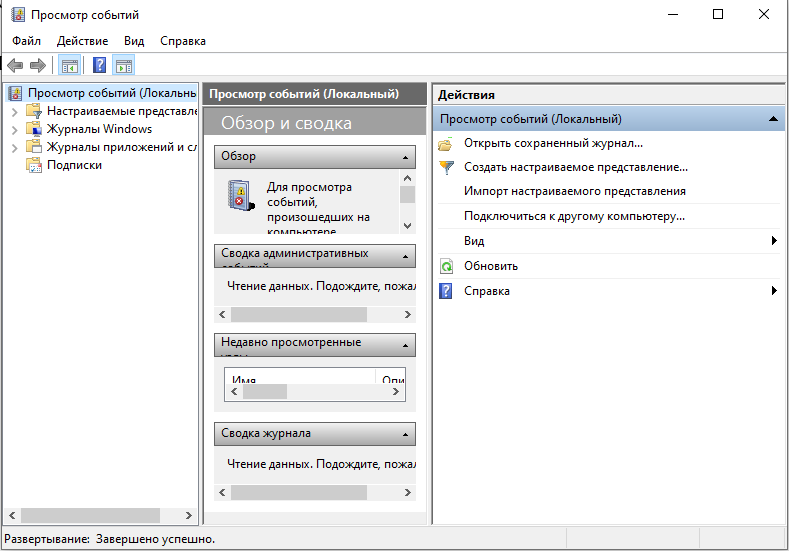


Рисунок 1 – Просмотр событий

* 1. В дереве консоли выберите Журналы Windows.

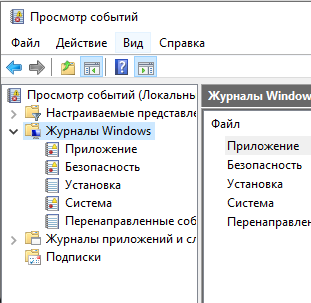


Рисунок 2 – Журналы Windows

* 1. Выберите и просмотрите журнал Система.

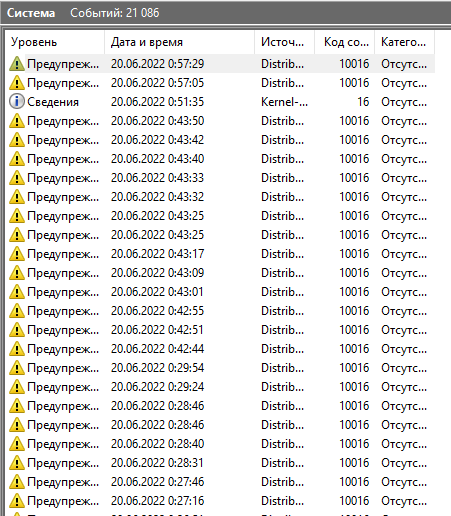


Рисунок 3 – Журналы Система

* 1. Выберите и просмотрите журнал Приложения.

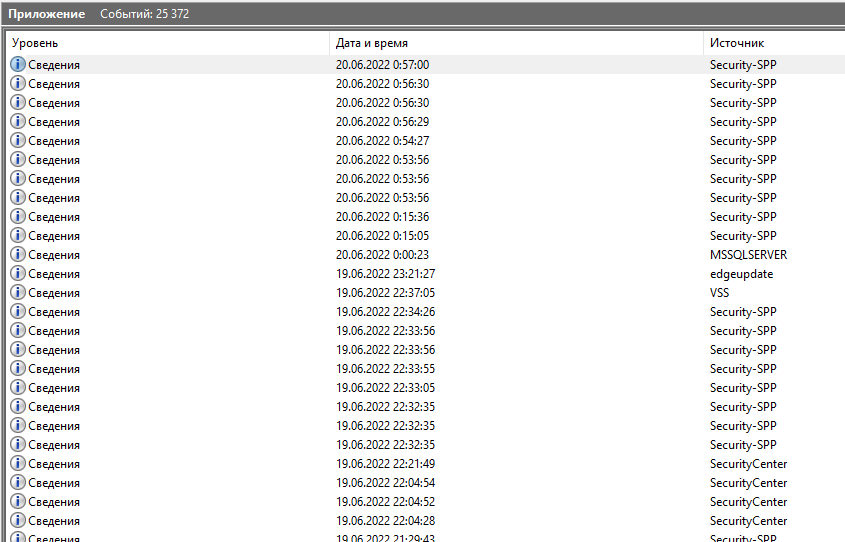


Рисунок 4 – Журналы Приложения

* 1. Определите количество записанных событий в журнале Приложения.

Событий: 25372

* 1. Используя меню Вид ⇒ Область просмотра, отобразите более подробные сведения.

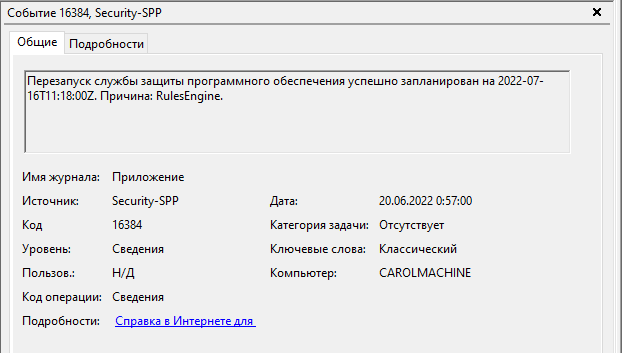


Рисунок 5 – Подробные сведения

* 1. Используя меню Вид ⇒ Сортировка, отсортируйте события в журнале по уровню, затем по дате и времени.

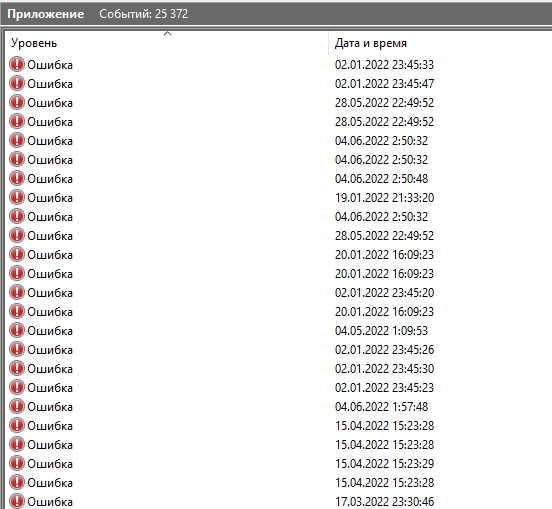


Рисунок 6 – Сортировка по уровню

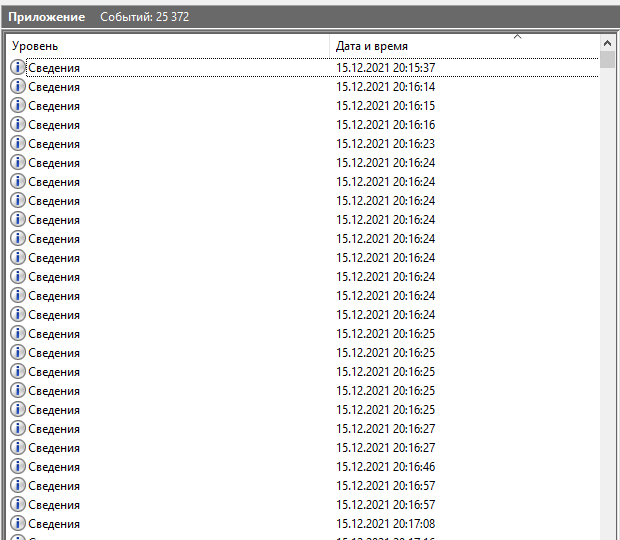


Рисунок 7 – Сортировка по дате и времени

* 1. Используя меню Вид ⇒ Добавить или удалить столбцы, добавьте столбцы Пользователь и Компьютер.

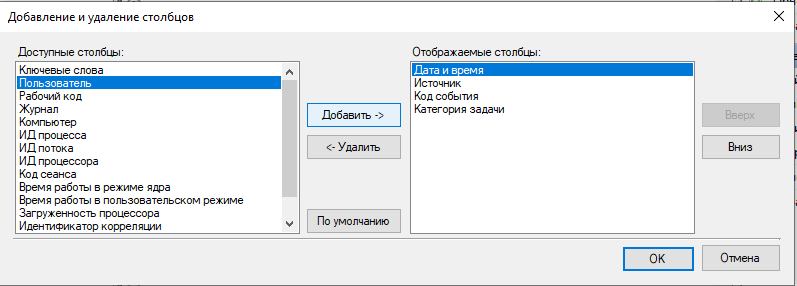


Рисунок 8 – Добавление и удаление столбцов

* 1. Откройте программу Excel.

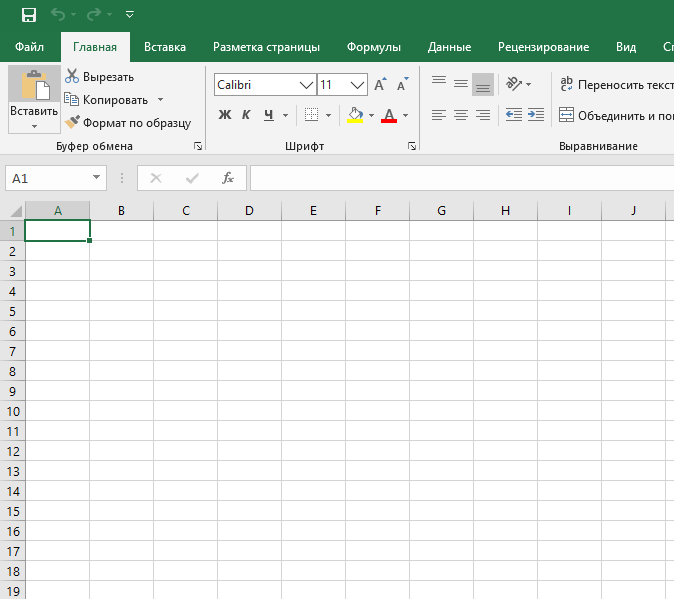


Рисунок 9 – Программа Excel

* 1. Обновите события в журнале Приложения. Для этого вызовите контекстное меню и выберите пункт Обновить.

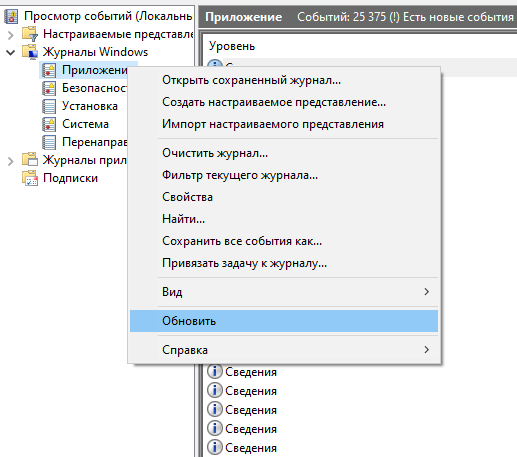


Рисунок 10 – Обновление события в журнале Приложения

* 1. Просмотрите новое событие в журнале, которое появилось после запуска программы Excel.



Рисунок 11 – Просмотр нового события

2.12 Привяжите новое событие к задаче. Для этого:

* выделите событие и вызовите контекстное меню, выберите пункт Привязать задачу к событию;

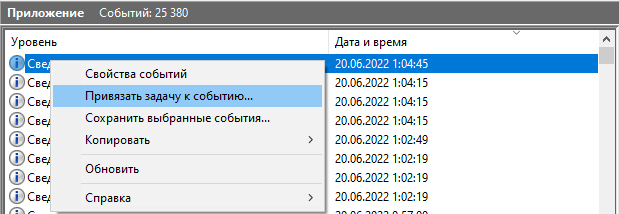


Рисунок 12 –Пункт Привязать задачу к событию

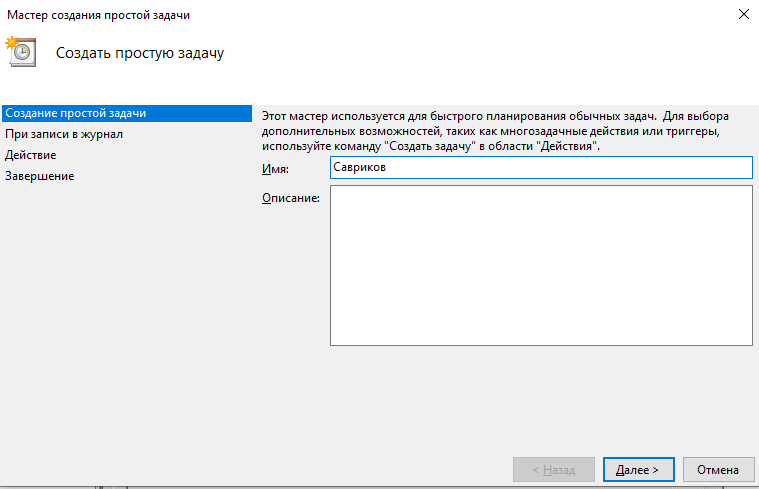
* введите имя – ваша фамилия, нажмите кнопку Далее;
* 

Рисунок 13 – Ввод имени

* в следующем окне нажмите кнопку Далее;
* выберите действие для задачи – Отобразить сообщение, нажмите кнопку Далее;

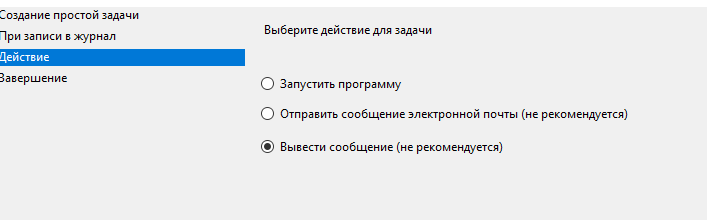


Рисунок 13 – Действие для задачи

* в следующем окне введите заголовок – ваша фамилия, сообщение – Вы запустили программу Excel, нажмите кнопку Далее;

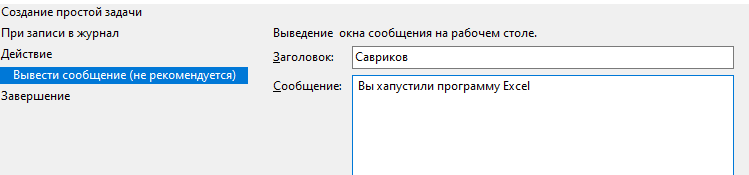
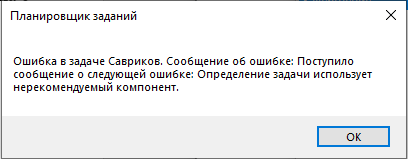


Рисунок 14 – Заголовок и сообщение

* в следующем окне нажмите кнопку Готово.
  1. Закройте и снова откройте программу Excel. Убедитесь в появлении окна с сообщением.



* 1. Используя Фильтр, отобразите события за последние 24 часа.

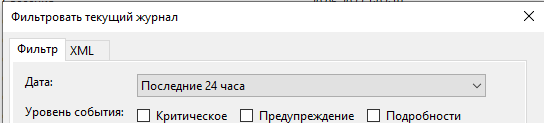


Рисунок 16 – Фильтр за последние 24 часа

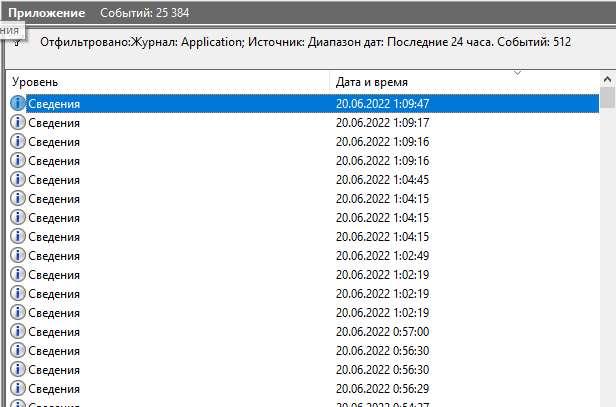


Рисунок 17 – Фильтр за последние 24 часа

* 1. Очистите фильтр.

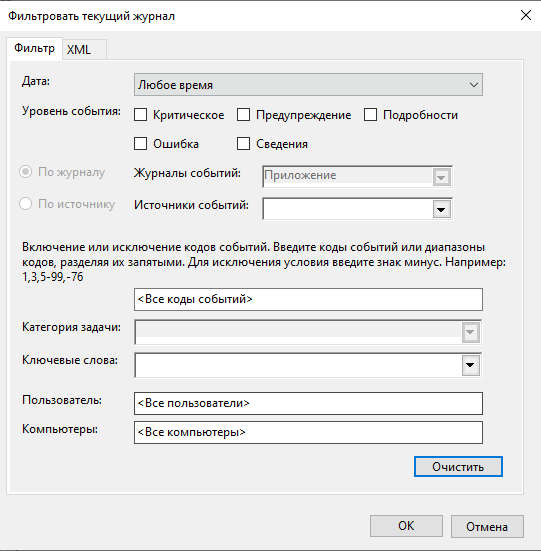


Рисунок 18 – Очистка фильтра

* 1. Используя Фильтр, отобразите события за последние 10 дней.

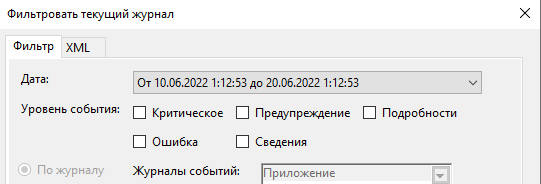


Рисунок 19 – Фильтр ха последние 10 дней

* 1. Очистите фильтр.

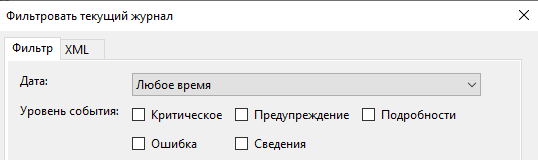


Рисунок 20 – Очистка фильтра

* 1. Используя Фильтр, отобразите события Ошибка.



Рисунок 21 – Фильтр Ошибка

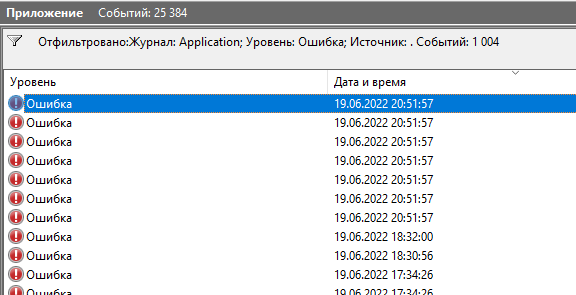


Рисунок 22 – Фильтр Ошибка

* 1. Очистите фильтр.

Рисунок 23 – Очистка фильтра

* 1. Используя Фильтр, отобразите события Ошибка и Предупреждения за последние 3 дня.

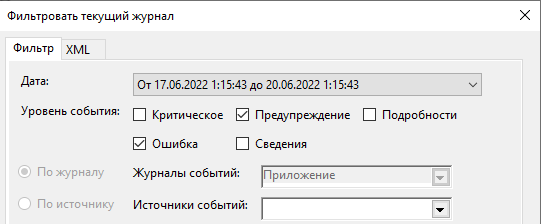


Рисунок 24 – Фильтр Ошибка и Предупреждения за последние 3 дня

* 1. Используя элемент окна Действия, сохраните выбранные события в файл, именем которого является ваше фамилия в формате .evtx.

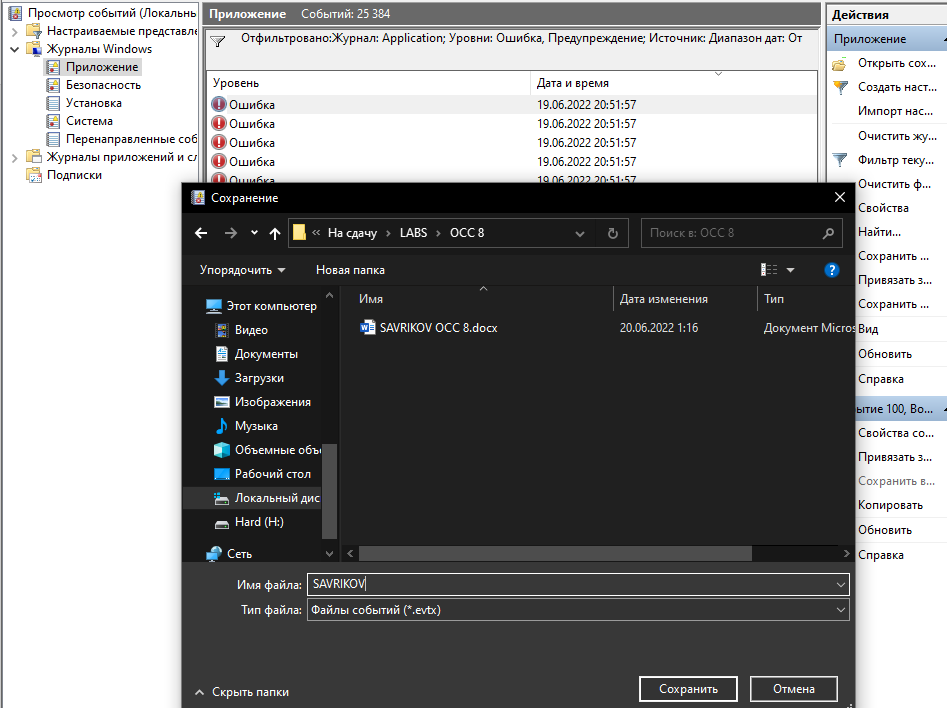


Рисунок 25 – Сохранение событий в файл

* 1. Очистите фильтр.

Рисунок 26 – Очистка фильтра

* 1. Откройте сохраненный файл.
  2. Используя Фильтр, отобразите события Сведения за последние 12 часов.

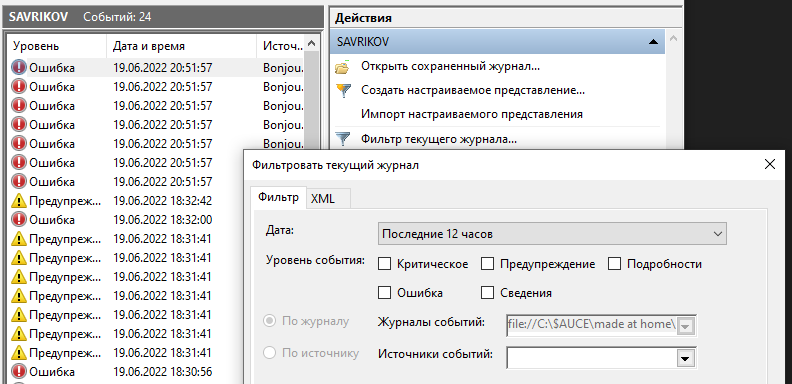


Рисунок 25 – Фильтр сведений за последние 12 часов

* 1. Используя элемент окна Действия, сохраните файл отфильтрованного журнала, именем которого является ваше фамилия в формате . txt.



Рисунок 29 – Сохранение отфильтрованного журнала

* 1. Откройте сохраненный файл.

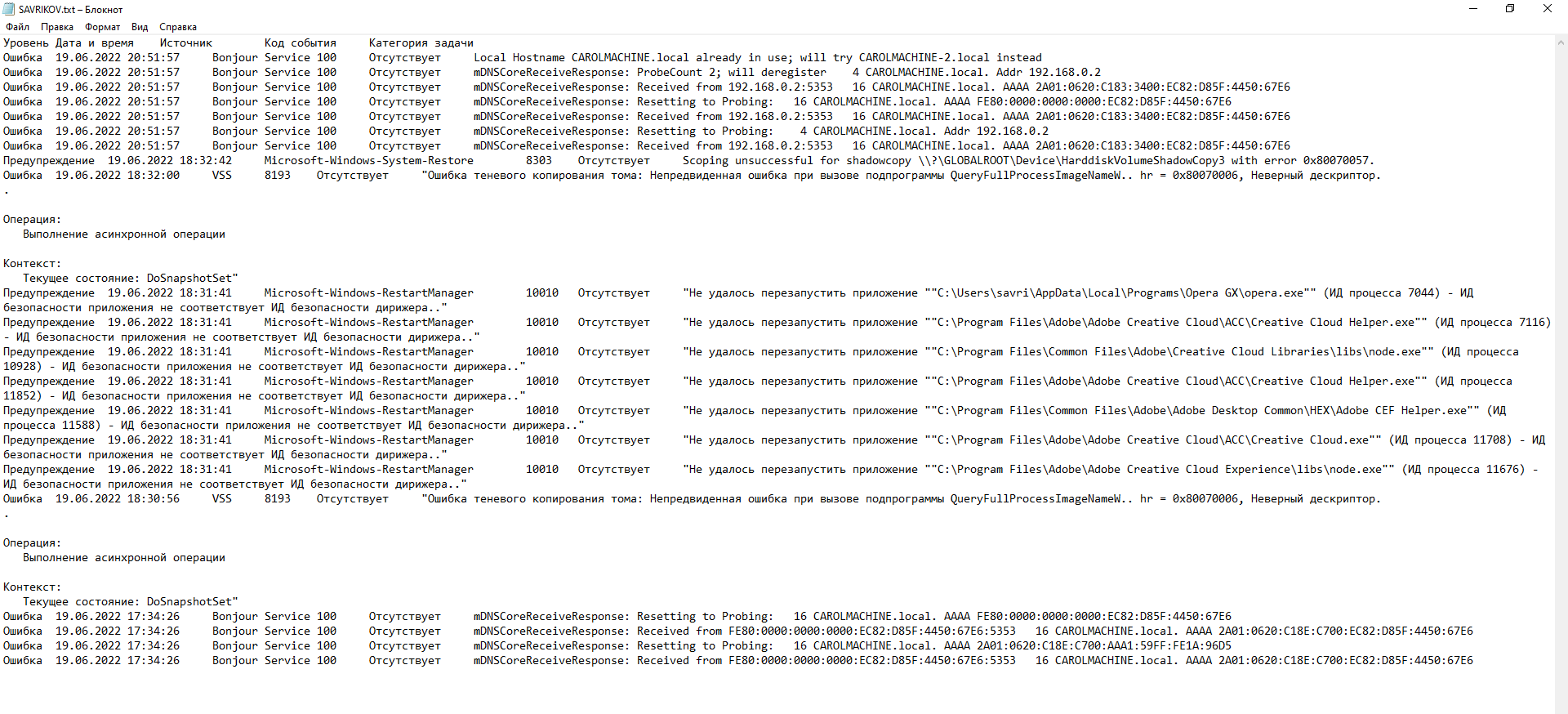


Рисунок 26 – Открытие сохраненного файла

* 1. Сохраните выбранные события в настраиваемом представлении. Для этого:
* в окне Действия нажмите Сохранить фильтр в настраиваемое представление;
* нажмите кнопку Создать папку, введите имя папки – ваша фамилия;
* введите имя настраиваемого представления – ваша фамилия;
* в левой части окна консоли должно появиться созданное представление.

Создайте еще одно настраиваемое представление, отфильтровав журнал Система по-своему выбору.

2.29 Используя элемент окна Действия, выведите свойства журнала Приложение. Определите размер журнала и политику сохранения журнала.

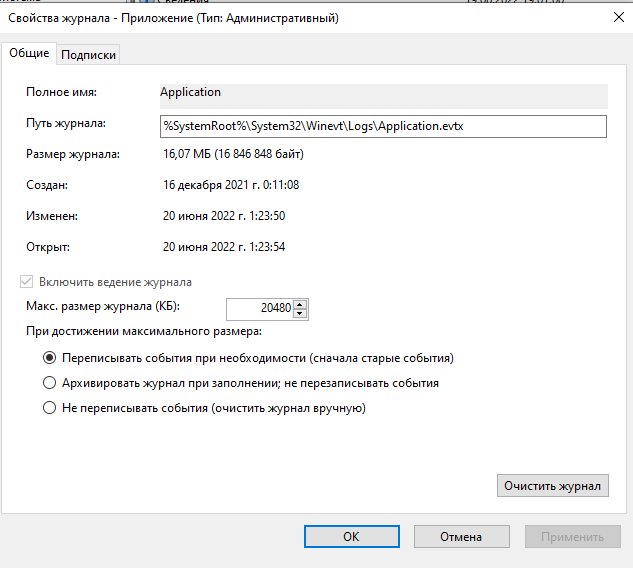


Рисунок 27 – Свойства журнала Приложение

Контрольные вопросы

1. Что такое Просмотр событий?

Это встроенное приложение Windows, или Компонент, включённый в состав операционных систем семейства Windows NT, разрабатываемых Microsoft.

1. Что позволяет программа Просмотр событий?

Позволяет проверять события, происходящие на компьютере, предоставляя доступ к журналам о программах, безопасности и системных событиях.

С помощью информации, найденной в средстве просмотра событий, можно устранить неполадки на компьютере Windows и посмотреть, есть ли какие-либо проблемы с оборудованием или программным обеспечением.

1. Как запустить приложение Просмотр событий?

* Нажмите на кнопку «Пуск» для открытия меню, откройте «Панель управления», из списка компонентов панели управления выберите «Администрирование» и из списка административных компонентов стоит выбрать «Просмотр событий»;
* Откройте «Консоль управления MMC». Для этого нажмите на кнопку «Пуск», в поле поиска введите mmc, а затем нажмите на кнопку «Enter».

1. Какие существуют категории журналов событий?

* Приложение;
* Безопасность;
* Установка;
* Система;
* Перенаправленные события.

1. Назовите типы журналов.

* Сведения;
* Предупреждение;
* Ошибка.

1. Какие существуют свойства событий (назовите несколько)?

* Источник;
* Код события;
* Уровень;
* Пользователь;
* Рабочий код;
* Журнал;
* Категория и задачи;
* Ключевые слова;
* Компьютер;
* Дата и время;
* ИД процесса;
* ИД потока;
* ИД процессора;
* Код сеанса;
* Время работы в режиме ядра;
* Время работы в пользовательском режиме;
* Загруженность процессора;
* Код корреляции;
* ИД относительной корреляции.

1. Какие уровни важности имеют события в журналах Windows?

* Сообщение.
* Предостережение.
* Ошибка.
* Опасная ошибка.
* Мониторинг успешных операций по исправлению ошибок.
* Аудит неудачных действий.