

Министерство образования XXX
Государственное бюджетное профессиональное образовательное учреждение
XXX «Колледж «XXX»

09.02.07

ОТЧЕТ

По лабораторным работам
МДК 04.02 Обеспечение качества функционирования компьютерных систем
ККОО.ПМ.XXX.000

Студент	XXX
Преподаватель	XXX
Дата защиты _____	Оценка _____

2022

Лабораторная работа № 6

Работа с программой «Просмотр событий»

Цель: научиться работать с журналами событий ОС Windows

Краткие теоретические сведения

В Microsoft Windows событие – это любое происшествие в операционной системе, которое записывается в журнал или требует уведомления пользователей или администраторов.

События регистрируются и сохраняются в журналах событий Windows и предоставляют важные хронологические сведения, помогающие вести мониторинг системы, поддерживать ее безопасность, устранять ошибки и выполнять диагностику.

Программа «Просмотр событий» - оснастка консоли управления Microsoft (MMC), которая предназначена для просмотра и управления журналами событий.

Программа «Просмотр событий» позволяет:

- просматривать события определенных журналов;
- применять фильтры событий и сохранять их для последующего использования в виде настраиваемых представлений;
- создавать подписки на события и управлять ими;
- назначать выполнение конкретных действий на возникновение определенного события.

Запуск приложения «Просмотр событий»

Приложение «Просмотр событий» можно открыть следующими способами:

1. 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».

2. Воспользоваться комбинацией клавиш Win + R для открытия диалога «Выполнить». В диалоговом окне «Выполнить», в поле «Открыть» введите eventvwr.msc и нажмите на кнопку «ОК».

Журналы событий в Windows 7

В операционной системе Windows 7 существуют две категории журналов событий:

- журналы Windows – используются операционной системой для регистрации общесистемных событий, связанных с работой приложений, системных компонентов, безопасностью и запуском;
- журналы приложений и служб – используются приложениями и службами для регистрации событий, связанных с их работой.

Типы журналов:

Приложение – хранит важные события, связанные с конкретным приложением.

Безопасность – хранит события, связанные с безопасностью, такие как вход/выход из системы, использование привилегий и обращение к ресурсам.

Установка – в этот журнал записываются события, возникающие при установке и настройке операционной системы и ее компонентов.

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.

Пересылаемые события – если настроена пересылка событий, в этот журнал попадают события, пересылаемые с других серверов.

Windows PowerShell – в этом журнале регистрируются события, связанные с использованием оболочки PowerShell.

События оборудования – если настроена регистрация событий оборудования, в этот журнал записываются события, генерируемые устройствами.

Свойства событий

					ККОО.ПМ.XXX.000	Лист
						3
Изм.	Лист	№ докум.	Подпись	Дата		

Источник – это программа, зарегистрировавшая событие в журнале.

Код события – это число, определяющее конкретный тип события.

Уровень – это уровень важности события.

В журналах системы и приложений события могут иметь следующие уровни важности:

- Уведомление - обозначает изменение в приложении или компоненте, такое как возникновение информационного события, связанного с успешным действием, создание ресурса или запуск службы.

- Предупреждение - обозначает предупреждение общего характера на неполадку, способную повлиять на службу или привести к более серьезной проблеме, если оставить ее без внимания;

- Ошибка - обозначает, что возникла проблема, которая может повлиять на функции, внешние по отношению к приложению или компоненту, вызвавшим событие;

- Критическая ошибка - обозначает, что произошел сбой, после которого приложение или компонент, инициировавшие событие, не могут восстановиться автоматически;

- Аудит успехов – успешное выполнение действий, которые вы отслеживаете через аудит, например использование какой-либо привилегии;

- Аудит отказов – неудачное выполнение действий, которые вы отслеживаете через аудит, например ошибка при входе в систему.

Пользователь – определяет учетную запись пользователя, от имени которого возникло данное событие. В этом поле может стоять N/A (Н/Д), если в данной ситуации учетная запись неприменима.

Рабочий код - содержит числовое значение, которое определяет операцию либо точку в пределах операции, при выполнении которой возникло данное событие

Журнал - имя журнала, в который было записано данное событие.

Категория и задачи – определяет категорию события, иногда используемую для последующего описания допустимого действия. У

					ККОО.ПМ.XXX.000	Лист
						4
Изм.	Лист	№ докум.	Подпись	Дата		

каждого источника событий свои категории. Например, следующие категории: вход/выход, использование привилегий, изменение политики и управление учетной записью.

Ключевые слова – это набор категорий или меток, которые могут использоваться для фильтрации или поиска событий.

Компьютер – идентифицирует имя компьютера, на котором произошло событие. Обычно это имя локального компьютера, но также может быть имя компьютера, переславшего событие, или имя локального компьютера до того, как оно было изменено.

Дата и время – определяет дату и время возникновения данного события в журнале.

ИД процесса – представляет идентификационный номер процесса, создавшего данное событие.

ИД потока – представляет идентификационный номер потока, создавшего данное событие. Процесс, порождённый в операционной системе, может состоять из нескольких потоков, выполняющихся «параллельно», то есть без предписанного порядка во времени.

ИД процессора – представляет идентификационный номер процессора, обработавшего событие.

Код сеанса – это идентификационный номер сеанса на сервере терминалов, в котором произошло событие.

Время работы в режиме ядра – определяет время, потраченное на выполнение инструкций режима ядра, в единицах времени ЦП.

Время работы в пользовательском режиме – определяет время, потраченное на выполнение инструкций пользовательского режима, в единицах времени ЦП.

Загруженность процессора – это время, потраченное на выполнение инструкций пользовательского режима, в тиках ЦП.

Задания для выполнения:

При выполнении лабораторной работы требуется оформление отчета.

					ККОО.ПМ.XXX.000	Лист
						5
Изм.	Лист	№ докум.	Подпись	Дата		

1. Запустите программу Просмотр событий.

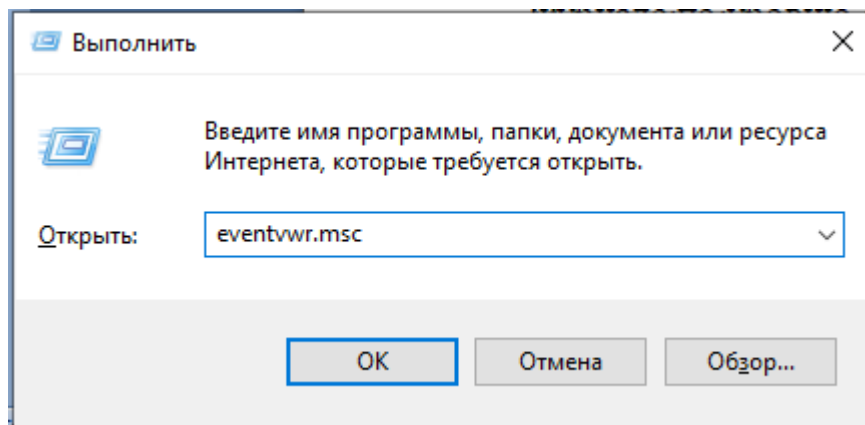


Рисунок 1 Запуск программы

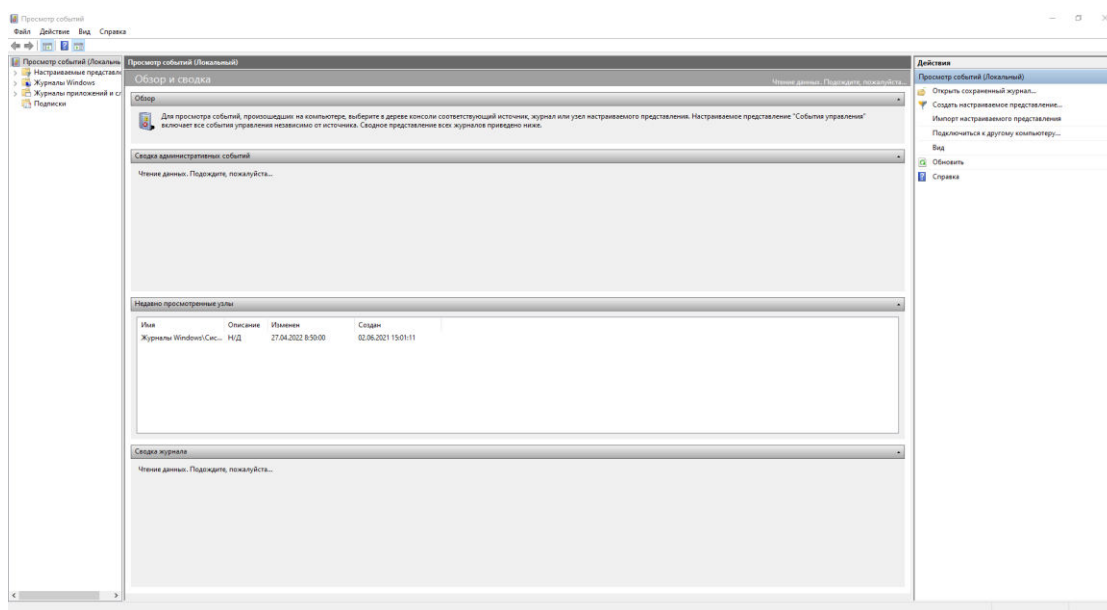


Рисунок 2 Запущенная программа

2. В дереве консоли выберите Журналы Windows.

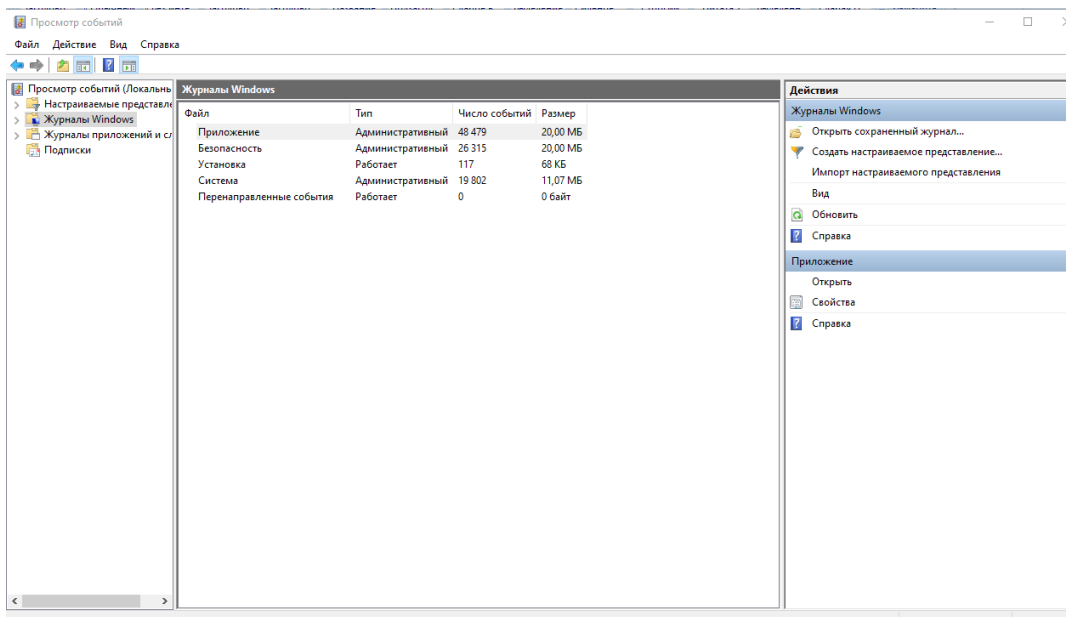


Рисунок 3 Журналы Windows

3. Выберите и просмотрите журнал Система.

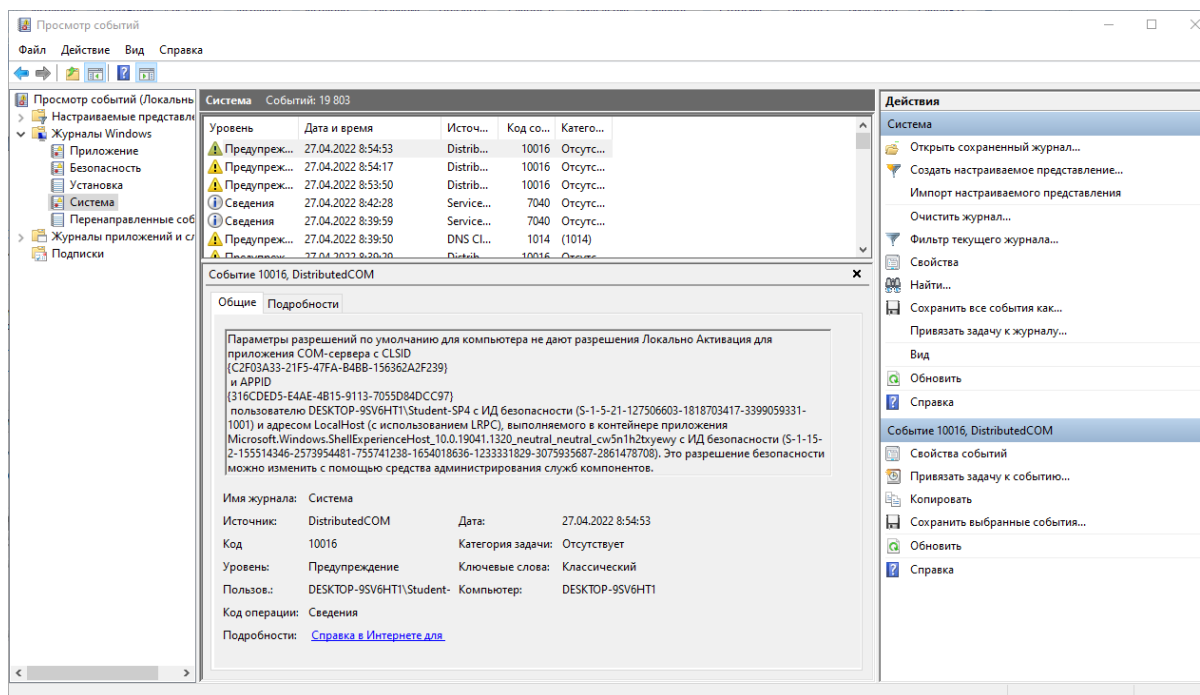


Рисунок 4 Журнал «Система»

4. Выберите и просмотрите журнал Приложения.

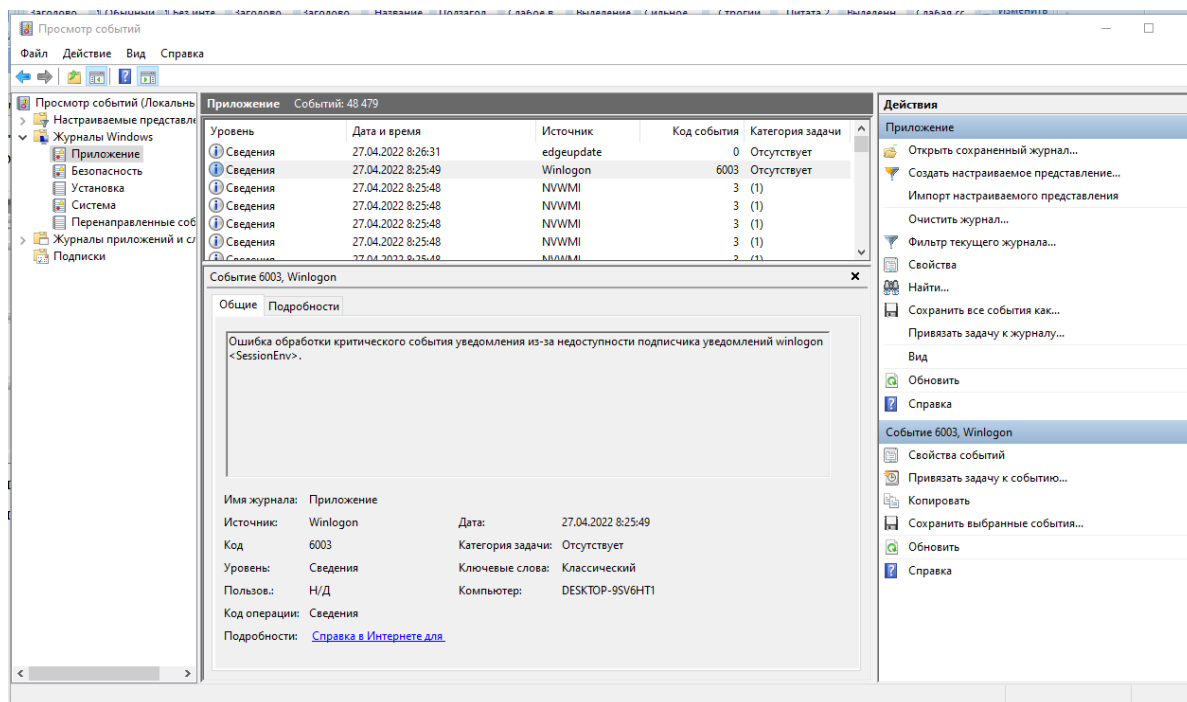


Рисунок 5 Журнал «Приложения»

5. Определите количество записанных событий в журнале Приложения.

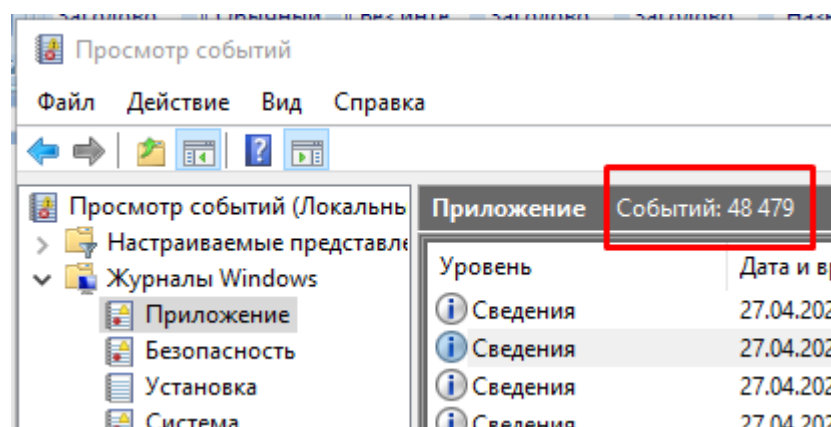


Рисунок 6 Количество записанных событий

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

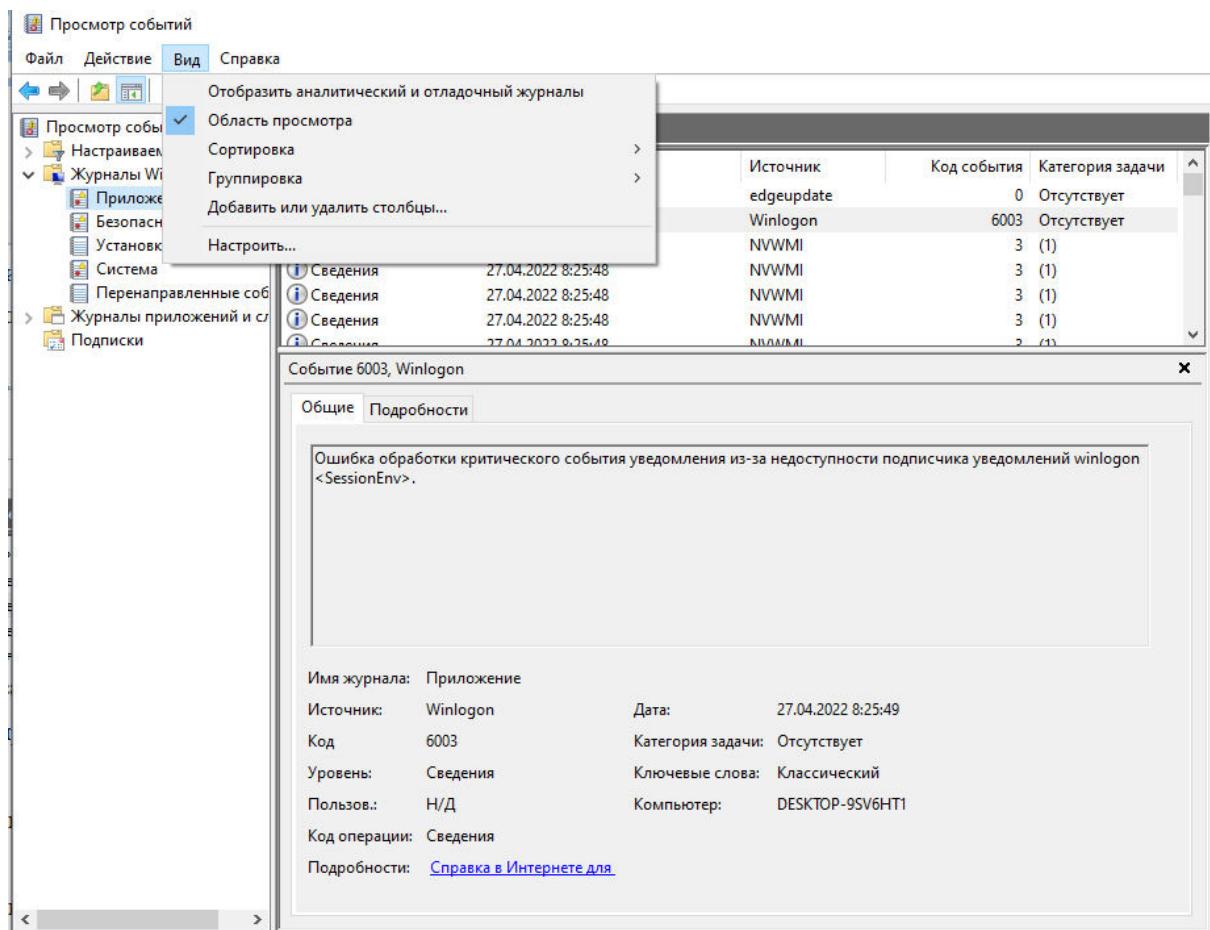


Рисунок 7 Область просмотра и подробные сведения

7. Используя меню Вид \Rightarrow Сортировка, отсортируйте события в журнале по уровню, затем по дате и времени.

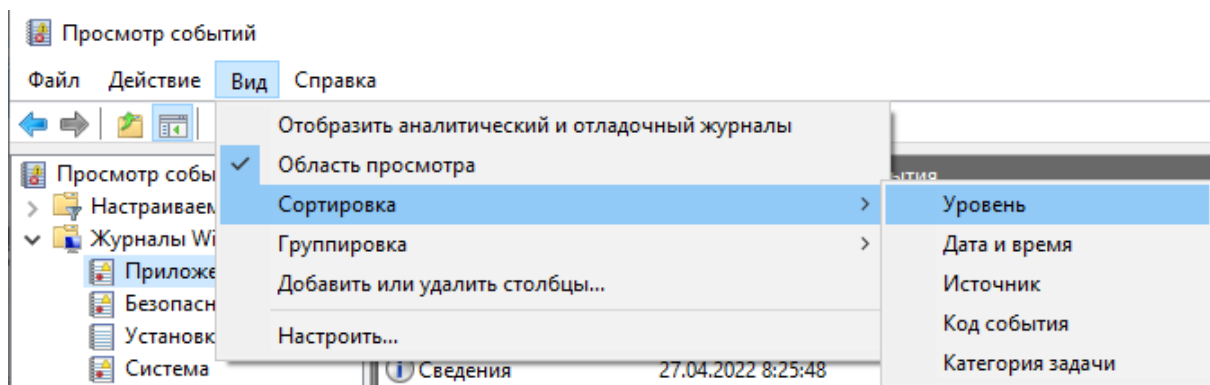


Рисунок 8 Сортировка по уровню

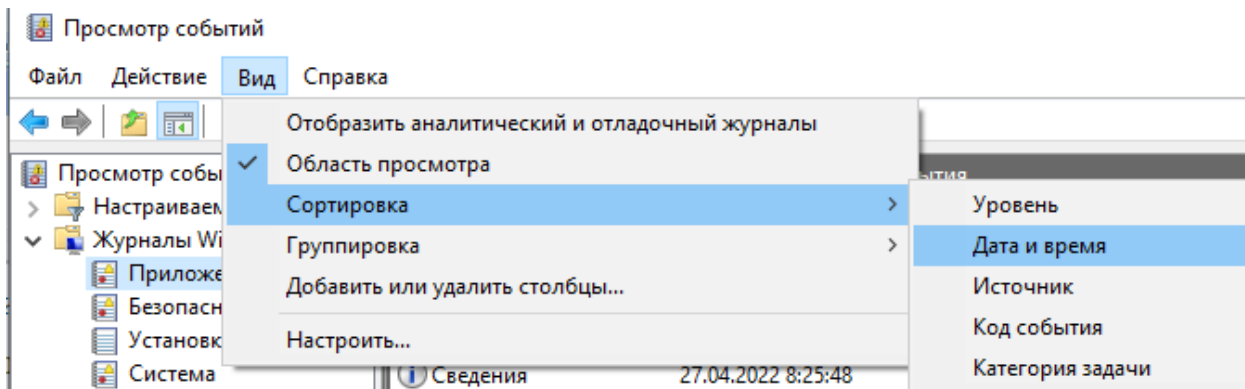


Рисунок 9 Сортировка по дате и времени

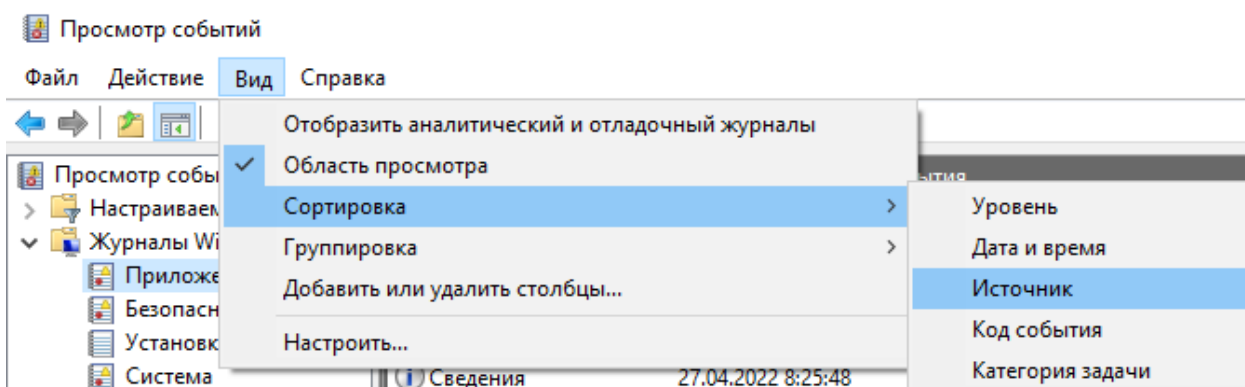


Рисунок 10 Сортировка по источнику

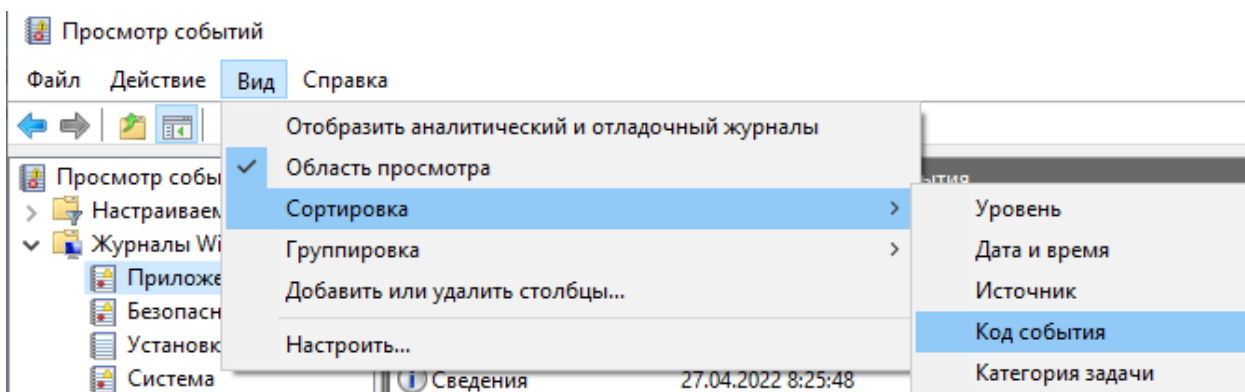


Рисунок 11 Сортировка по коду события

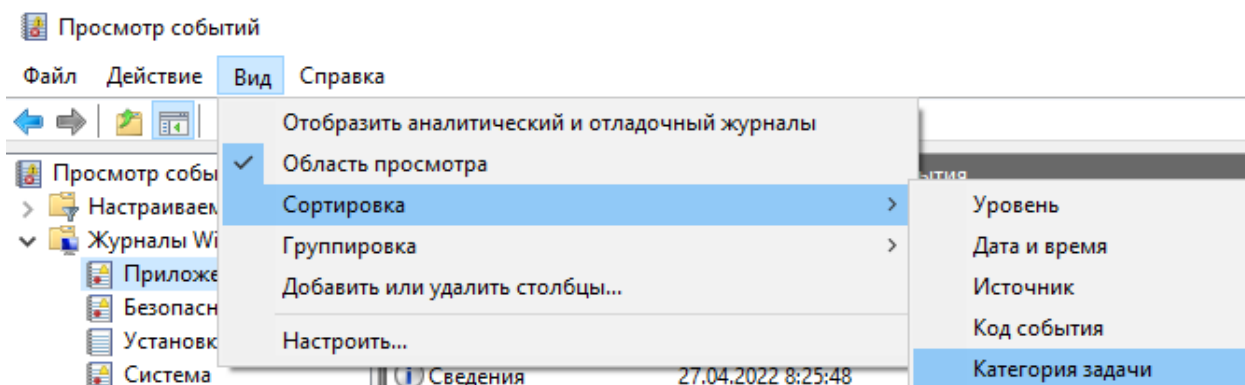


Рисунок 12 Сортировка по категории задачи

Приложение Событий: 48 485 (!) Есть новые события				
Уровень	Дата и время	Источник	Код события	Категория задачи
Сведения	27.04.2022 8:30:05	NVWMI	3 (1)	
Сведения	27.04.2022 8:30:05	NVWMI	3 (1)	
Сведения	27.04.2022 8:30:05	NVWMI	3 (1)	
Сведения	27.04.2022 8:30:05	NVWMI	3 (1)	
Сведения	27.04.2022 8:30:05	NVWMI	3 (1)	
Сведения	27.04.2022 8:30:05	NVWMI	3 (1)	
Сведения	27.04.2022 8:30:05	NVWMI	3 (1)	
Сведения	27.04.2022 8:30:14	Security-SPP	16394	Отсутствует
Сведения	27.04.2022 8:30:54	NVWMI	3 (1)	
Сведения	27.04.2022 8:30:54	NVWMI	3 (1)	
Сведения	27.04.2022 8:30:54	NVWMI	3 (1)	
Сведения	27.04.2022 8:30:54	NVWMI	3 (1)	
Сведения	27.04.2022 8:30:54	NVWMI	3 (1)	
Сведения	27.04.2022 8:30:54	NVWMI	3 (1)	
Сведения	27.04.2022 8:30:54	NVWMI	3 (1)	
Сведения	27.04.2022 8:30:54	NVWMI	3 (1)	
Сведения	27.04.2022 8:30:57	Security-SPP	16384	Отсутствует
Сведения	27.04.2022 8:31:58	Security-SPP	16394	Отсутствует
Сведения	27.04.2022 8:32:29	Security-SPP	16384	Отсутствует
Сведения	27.04.2022 8:32:57	RestartManager	10000	Отсутствует
Сведения	27.04.2022 8:32:57	RestartManager	10001	Отсутствует
Сведения	27.04.2022 8:32:58	RestartManager	10000	Отсутствует
Сведения	27.04.2022 8:32:58	RestartManager	10001	Отсутствует
Сведения	27.04.2022 8:57:23	ESENT	102	Общие
Сведения	27.04.2022 8:57:23	ESENT	300	Ведение журнал...
Сведения	27.04.2022 8:57:23	ESENT	301	Ведение журнал...
Сведения	27.04.2022 8:57:23	ESENT	302	Ведение журнал...
Сведения	27.04.2022 8:57:23	ESENT	105	Общие
Сведения	27.04.2022 8:57:23	ESENT	326	Общие

Рисунок 13 Сортировка списка событий

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

Добавление и удаление столбцов

Доступные столбцы:

Ключевые слова
Рабочий код
Журнал
ИД процесса
ИД потока
ИД процессора
Код сеанса
Время работы в режиме ядра
Время работы в пользовательском режиме
Загруженность процессора
Идентификатор корреляции
Идентификатор относительной корреляции
Имя источника события

Добавить ->
< Удалить
По умолчанию

Отображаемые столбцы:

Дата и время
Источник
Код события
Категория задачи
Пользователь
Компьютер

Вверх
Вниз

OK
Отмена

Рисунок 14 Добавление столбцов

9. Откройте программу Excel.

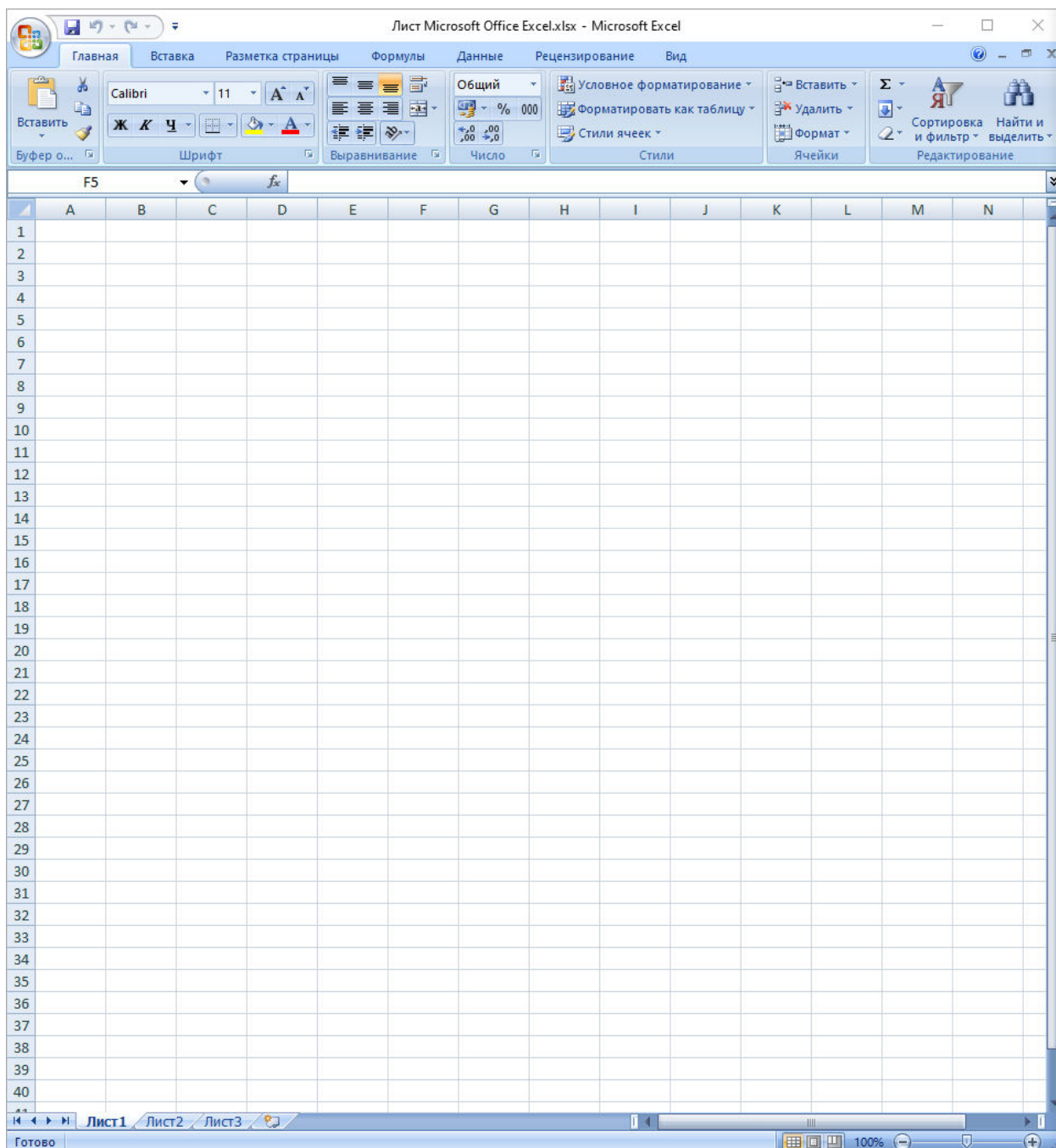


Рисунок 15 Открытая программа Excel

10. Обновите события в журнале Приложения. Для этого вызовите контекстное меню и выберите пункт «Обновить».

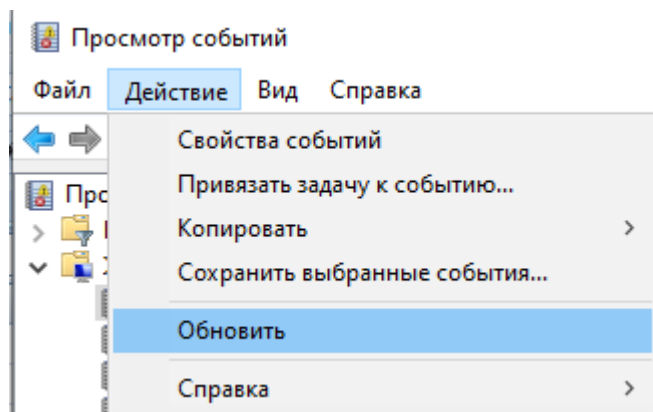


Рисунок 16 Пункт «Обновить»

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

Событие не появилось. Вместо Excel я взял приложение антивируса Касперского.

12. Привяжите новое событие к задаче. Для этого:

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

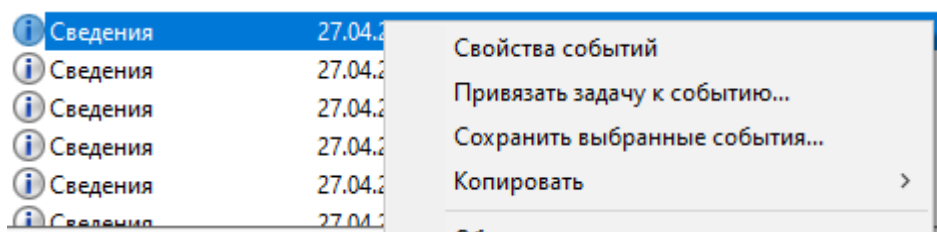



Рисунок 17 Привязка задачи к событию

– введите имя – ваша фамилия, нажмите кнопку Далее;

Мастер создания простой задачи

 Создать простую задачу

Создание простой задачи

При записи в журнал

Действие

Завершение

Этот мастер используется для быстрого планирования обычных задач. Для выбора дополнительных возможностей, таких как многозадачные действия или триггеры, используйте команду "Создать задачу" в области "Действия".

Имя:


Описание:

< Назад **Далее >** Отмена

Рисунок 18 Создание простой задачи

- в следующем окне нажмите кнопку Далее;

Мастер создания простой задачи

 При записи определенного события в журнал

Создание простой задачи

При записи в журнал

Действие

Завершение

Журнал:

Источник:


Код события:

< Назад **Далее >** Отмена

Рисунок 19 Создание простой задачи

- выберите действие для задачи – Отобразить сообщение, нажмите кнопку Далее;

Мастер создания простой задачи

 Действие

Создание простой задачи

При записи в журнал

Действие

Вывести сообщение (не рекомендуется)

Завершение

Выберите действие для задачи

☐ Запустить программу

☐ Отправить сообщение электронной почты (не рекомендуется)


☒ Вывести сообщение (не рекомендуется)

< Назад Далее > Отмена

Рисунок 20 Создание простой задачи

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

Мастер создания простой задачи

 Вывести сообщение (не рекомендуется)

Создание простой задачи

При записи в журнал

Действие

Вывести сообщение (не рекомендуется)

Завершение

Выведение окна сообщения на рабочем столе.

Заголовок:

Сообщение:

< Назад Далее > Отмена

Рисунок 21 Создание простой задачи

- в следующем окне нажмите кнопку Готово.

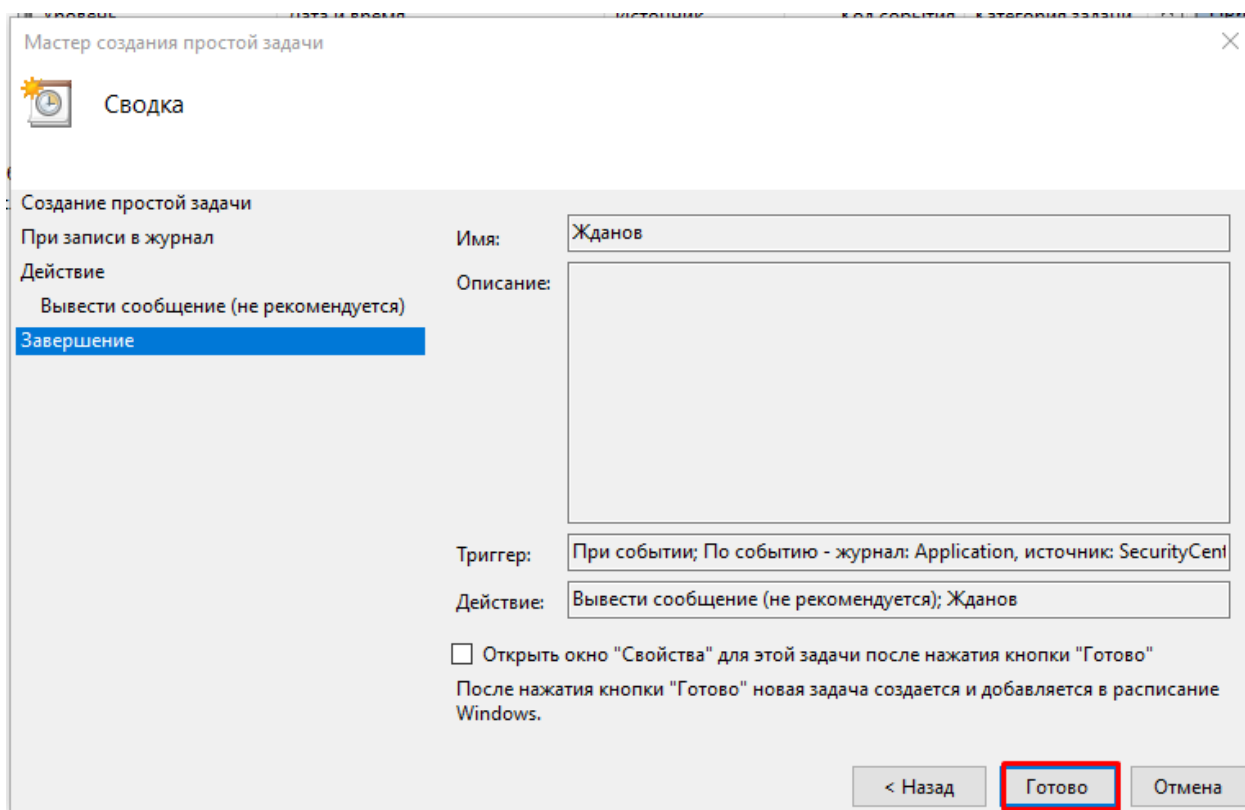


Рисунок 22 Кнопка «Готово»

13. Закройте и снова откройте программу Excel. Убедитесь в появлении окна с сообщением.

После нажатия кнопки «Готово», нам пишут об ошибке использования не рекомендуемого компонента.

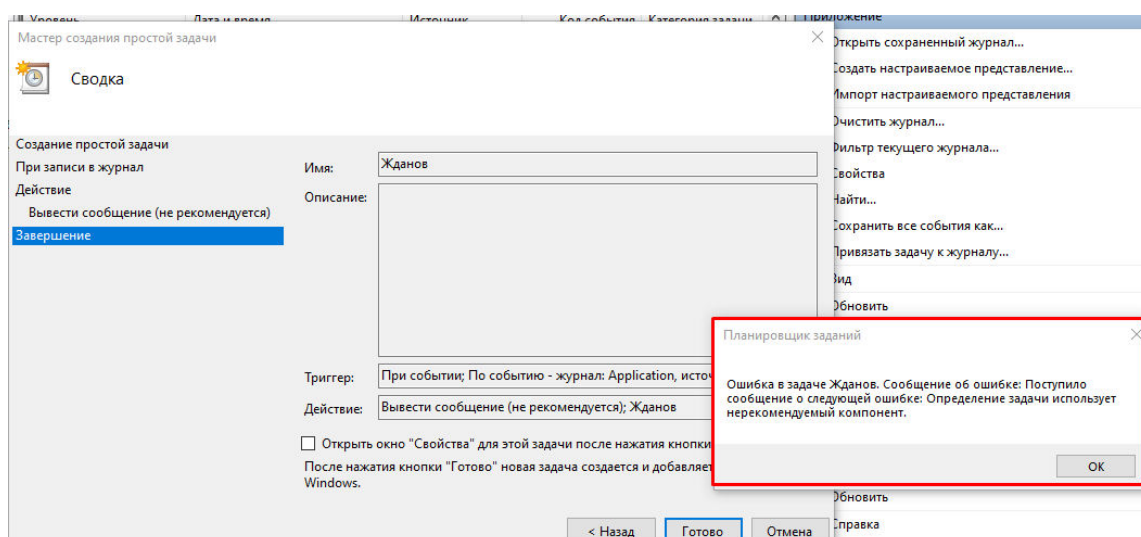


Рисунок 23 Ошибка об использовании не рекомендуемого компонента

14. Используя Фильтр, отобразите события за последние 24 часа.

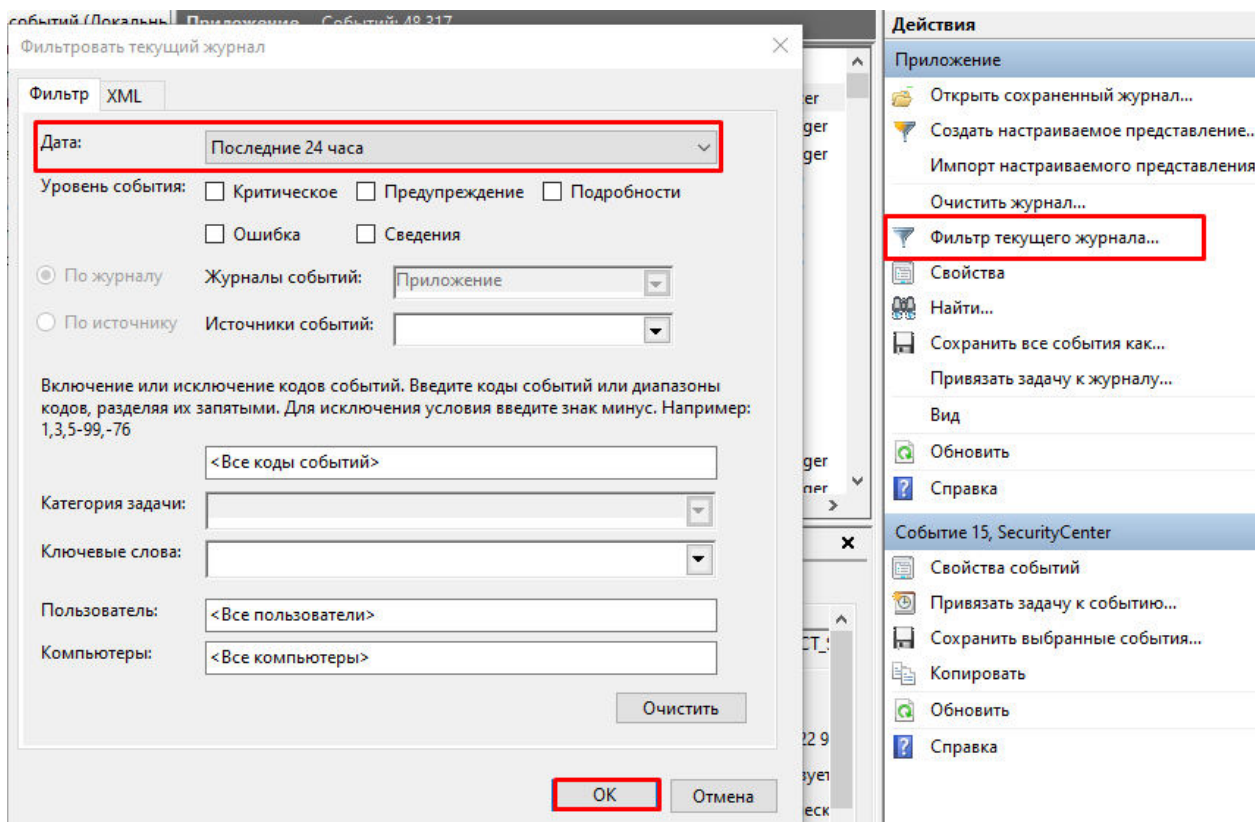


Рисунок 24 Фильтр за последние 24 часа

Приложение Событий: 48 317

Отфильтровано: Журнал: Application; Источник: Диапазон дат: Последние 24

Уровень	Дата и время	Источник
Сведения	27.04.2022 9:28:15	SecurityCenter
Сведения	27.04.2022 9:18:20	RestartManager
Сведения	27.04.2022 9:18:09	RestartManager
Сведения	27.04.2022 9:13:36	Security-SPP
Сведения	27.04.2022 9:12:59	Security-SPP
Сведения	27.04.2022 9:12:31	Security-SPP
Сведения	27.04.2022 9:11:52	Security-SPP
Сведения	27.04.2022 8:57:23	ESENT
Сведения	27.04.2022 8:57:23	ESENT
Сведения	27.04.2022 8:57:23	ESENT
Сведения	27.04.2022 8:57:23	ESENT
Сведения	27.04.2022 8:57:23	ESENT
Сведения	27.04.2022 8:57:23	ESENT

Рисунок 25 Отфильтрованные события

15. Очистите фильтр.

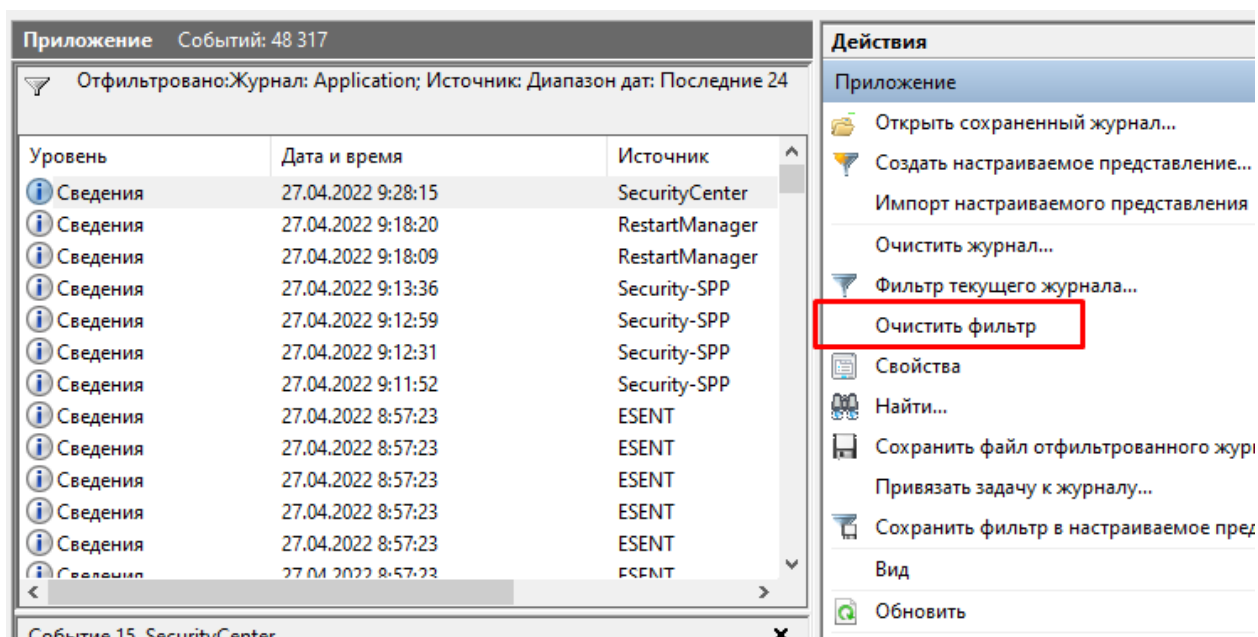


Рисунок 26 Кнопка «Очистить фильтр»

16. Используя Фильтр, отобразите события за последние 10 дней.

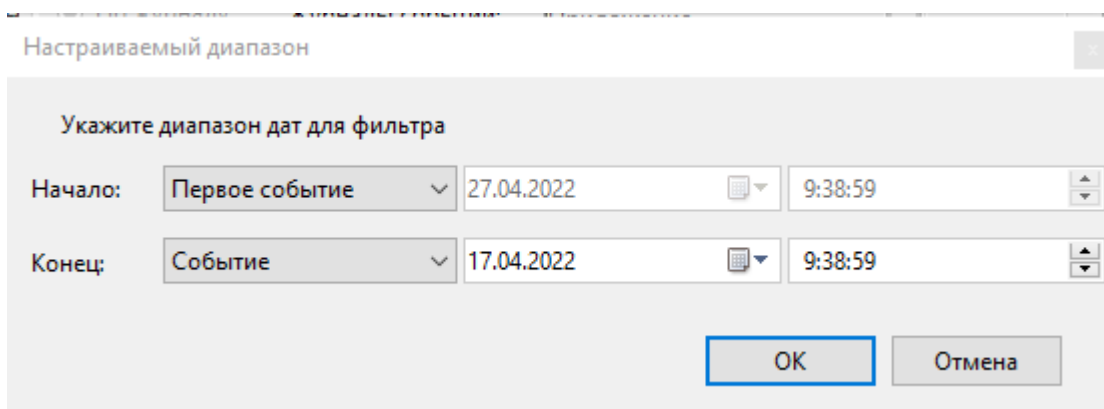


Рисунок 27 Настройка диапазона за последние 10 дней

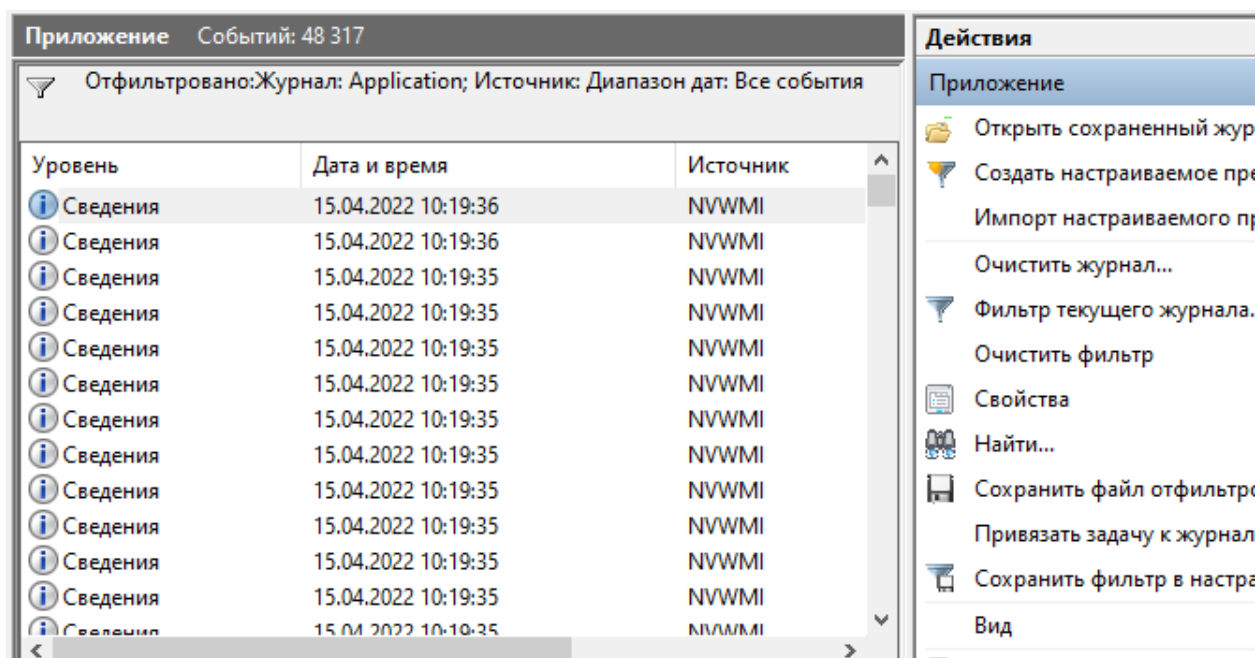


Рисунок 28 Отфильтрованные события

17. Очистите фильтр.

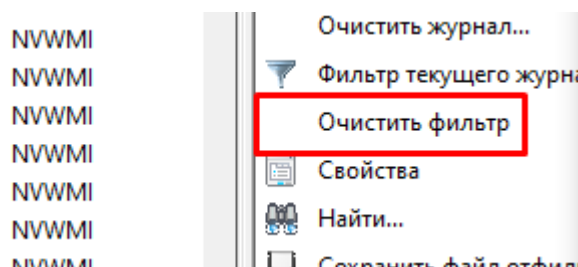


Рисунок 29 Кнопка «Очистить фильтр»

18. Используя Фильтр, отобразите события Ошибка.

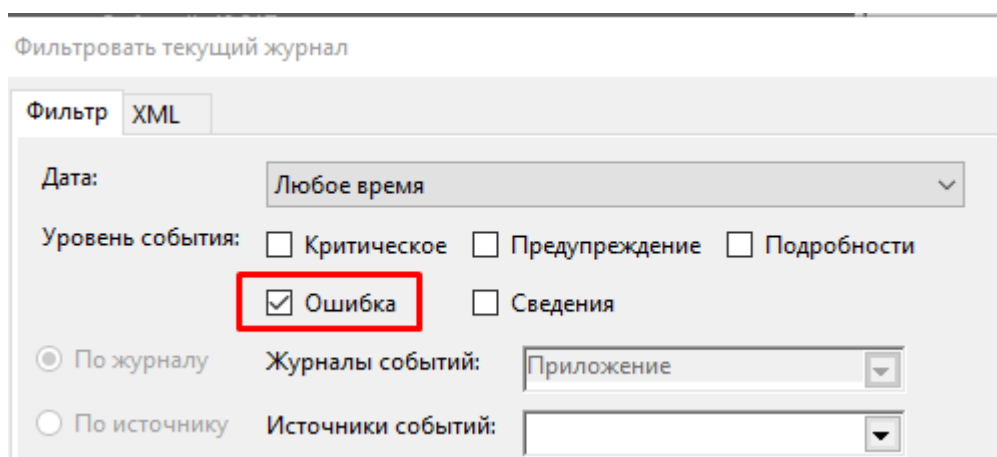


Рисунок 30 Фильтр по событиям «Ошибка»

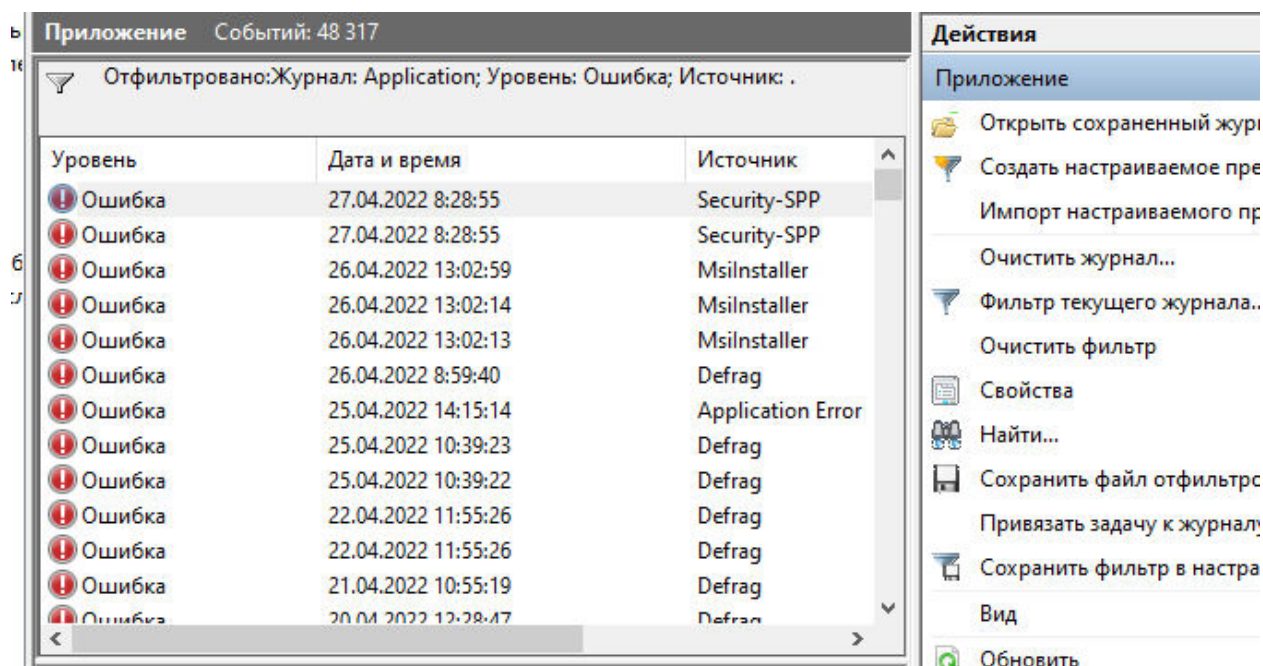


Рисунок 31 Отфильтрованные события

19. Очистите фильтр.

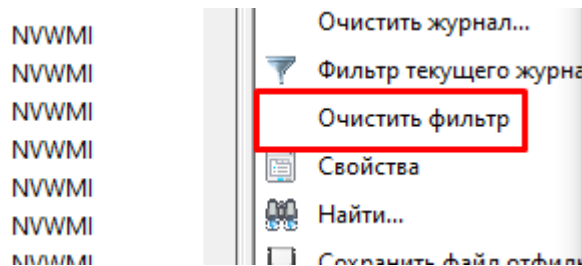


Рисунок 32 Кнопка «Очистить фильтр»

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

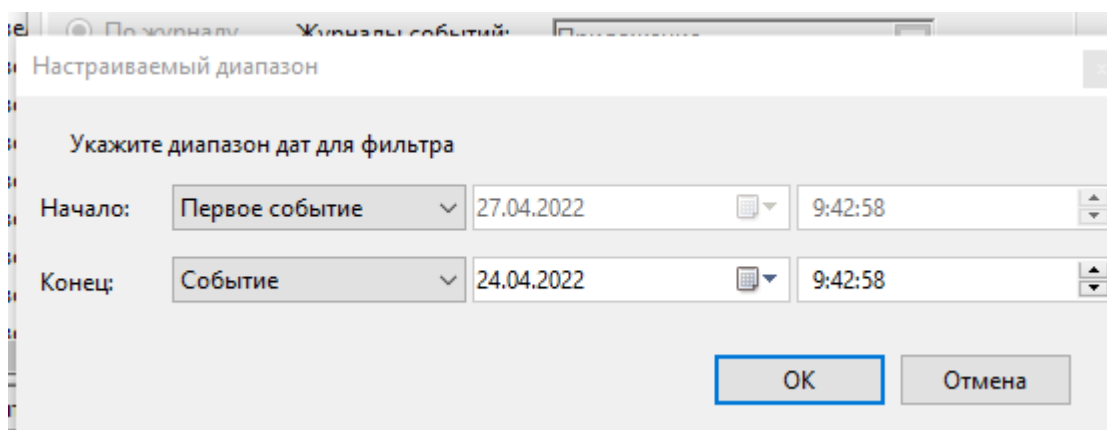


Рисунок 33 Диапазон 3 дня

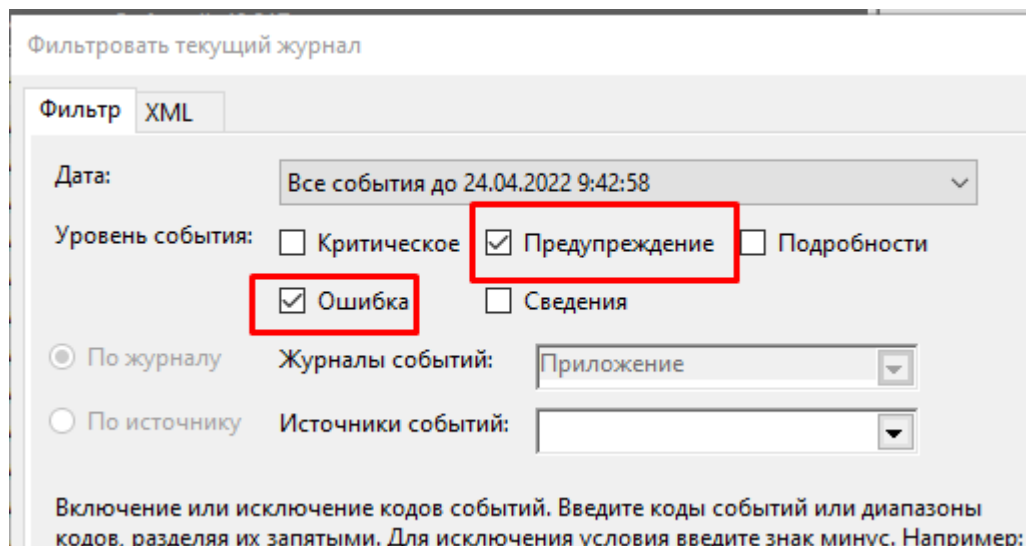


Рисунок 34 Отображение ошибок и предупреждений

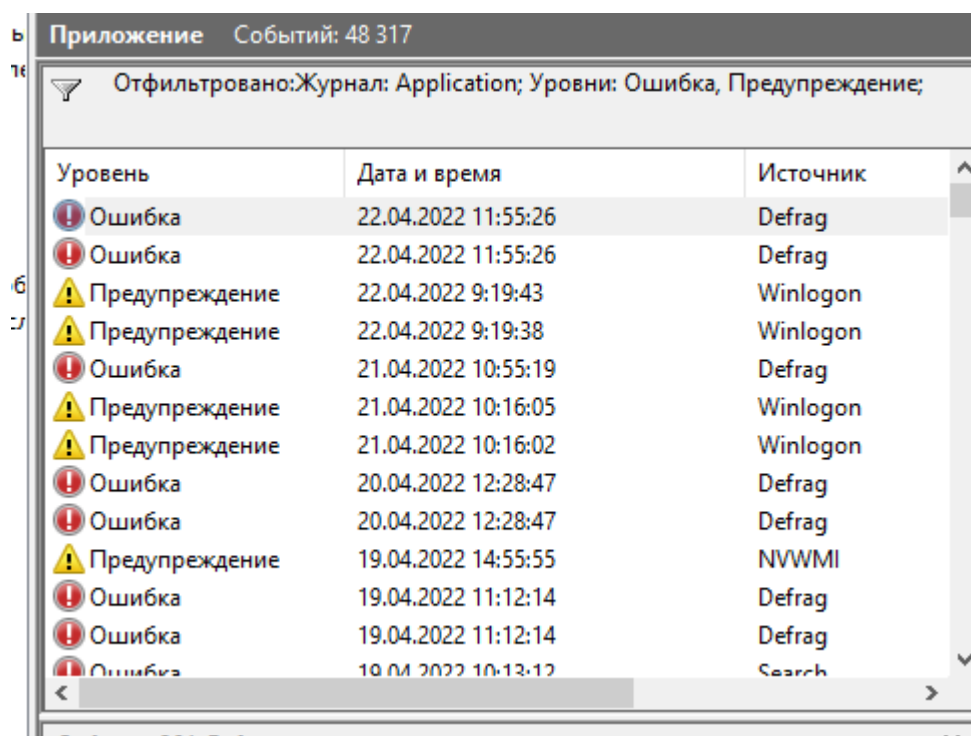


Рисунок 35 Отфильтрованные события

21. Используя элемент окна Действия, сохраните выбранные события в файл, именем которого является ваша фамилия в формате .evtx.

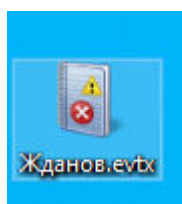


Рисунок 36 Сохраненный файл с событиями

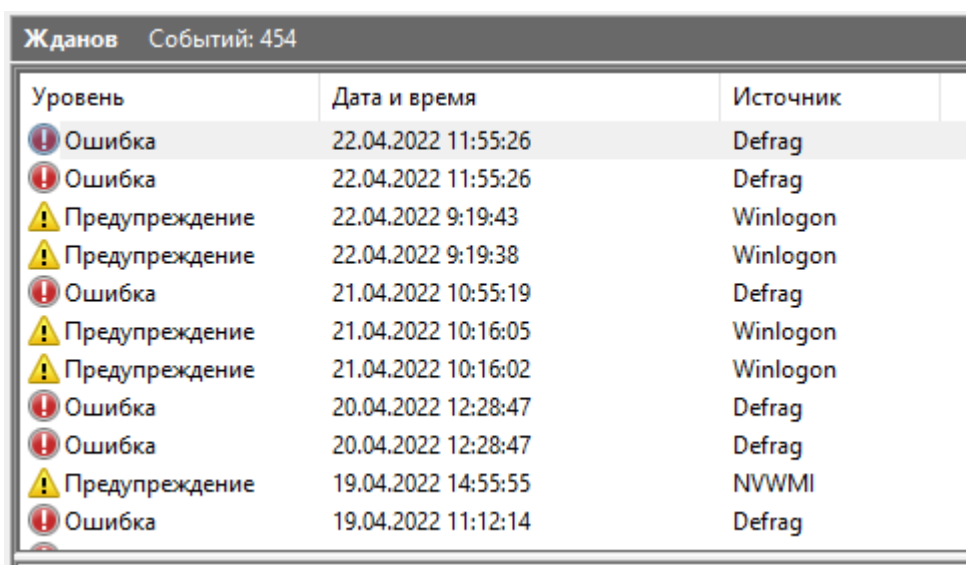


Рисунок 37 Сохраненный файл с событиями

22. Очистите фильтр.

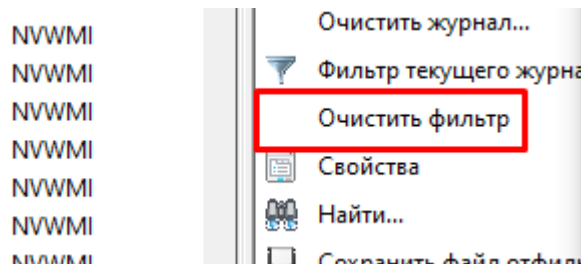


Рисунок 38 Кнопка «Очистить фильтр»

23. Откройте сохраненный файл.

Жданов Событий: 454		
Уровень	Дата и время	Источник
❗ Ошибка	22.04.2022 11:55:26	Defrag
❗ Ошибка	22.04.2022 11:55:26	Defrag
⚠ Предупреждение	22.04.2022 9:19:43	Winlogon
⚠ Предупреждение	22.04.2022 9:19:38	Winlogon
❗ Ошибка	21.04.2022 10:55:19	Defrag
⚠ Предупреждение	21.04.2022 10:16:05	Winlogon
⚠ Предупреждение	21.04.2022 10:16:02	Winlogon
❗ Ошибка	20.04.2022 12:28:47	Defrag
❗ Ошибка	20.04.2022 12:28:47	Defrag
⚠ Предупреждение	19.04.2022 14:55:55	NVWMI
❗ Ошибка	19.04.2022 11:12:14	Defrag

Рисунок 39 Сохраненный файл с событиями

24. Используя Фильтр, отобразите события Сведения за последние 12 часов.

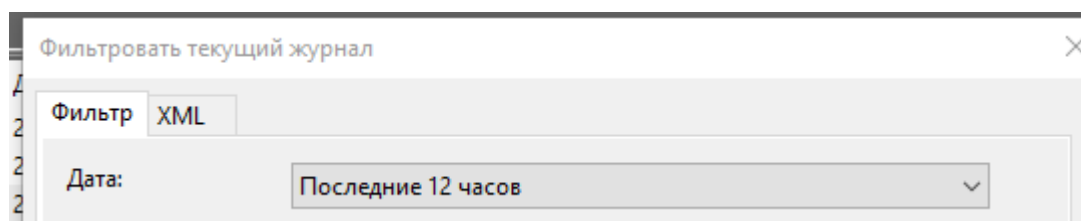


Рисунок 40 Фильтр за последние 12 часов

Жданов Событий: 454				
Отфильтровано: Журнал: file://C:\Users\Student-SP4\Desktop\Жданов.evtx; Источник: Диапазон дат: Последние 12				
Уровень	Дата и время	Источник	Код события	Категория задачи

Рисунок 41 Отфильтрованные события

25. Используя элемент окна Действия, сохраните файл отфильтрованного журнала, именем которого является ваша фамилия в формате .txt.

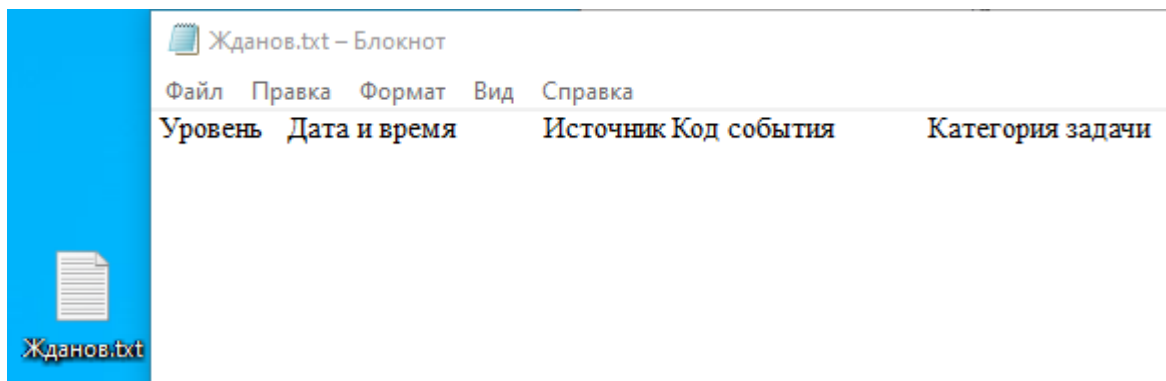


Рисунок 42 Сохраненный файл

26. Откройте сохраненный файл.

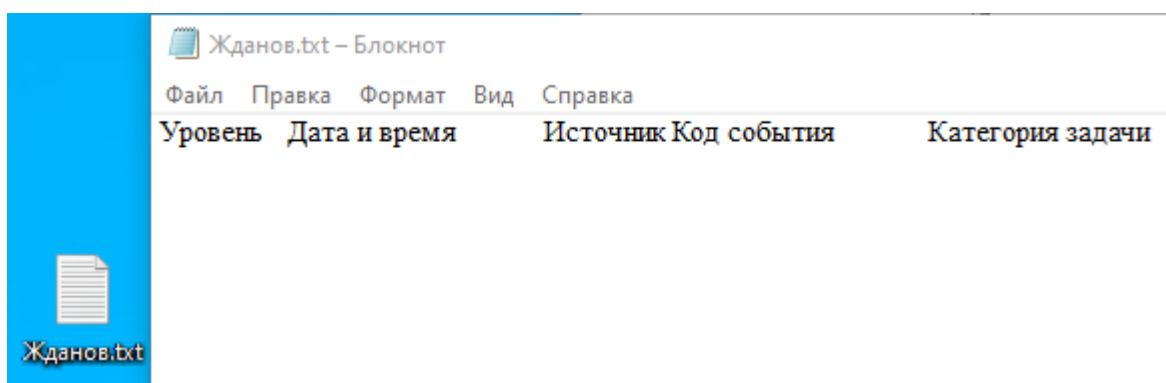


Рисунок 42 Сохраненный файл

27. Сохраните выбранные события в настраиваемом представлении.
Для этого:

- в окне Действия нажмите «Сохранить фильтр» в настраиваемое представление;

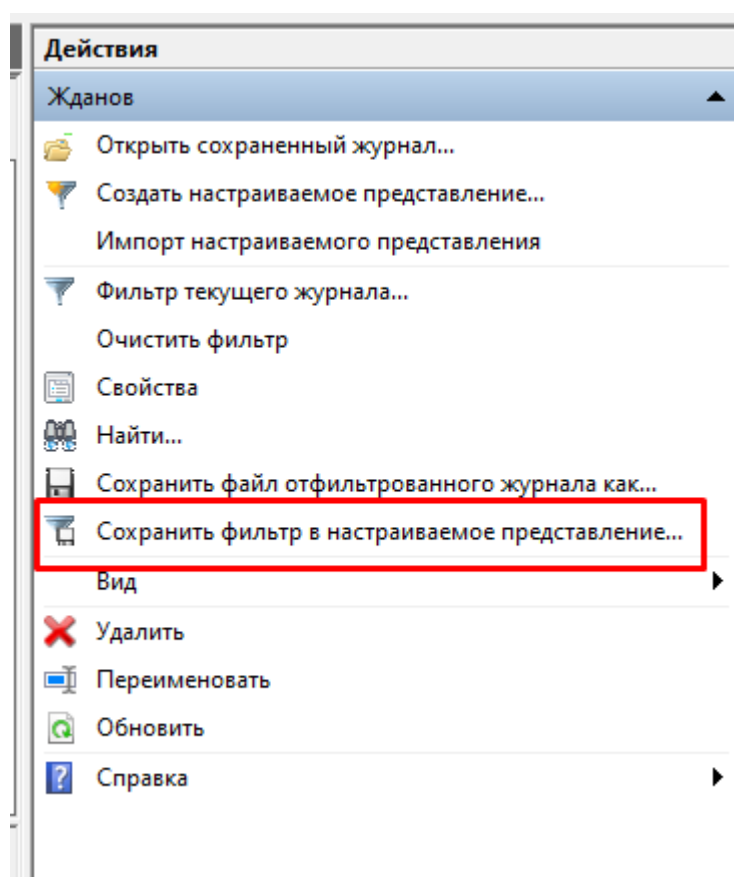


Рисунок 43 Кнопка «Сохранить фильтр в настраиваемое представление»

– нажмите кнопку «Создать папку», введите имя папки – ваша фамилия;

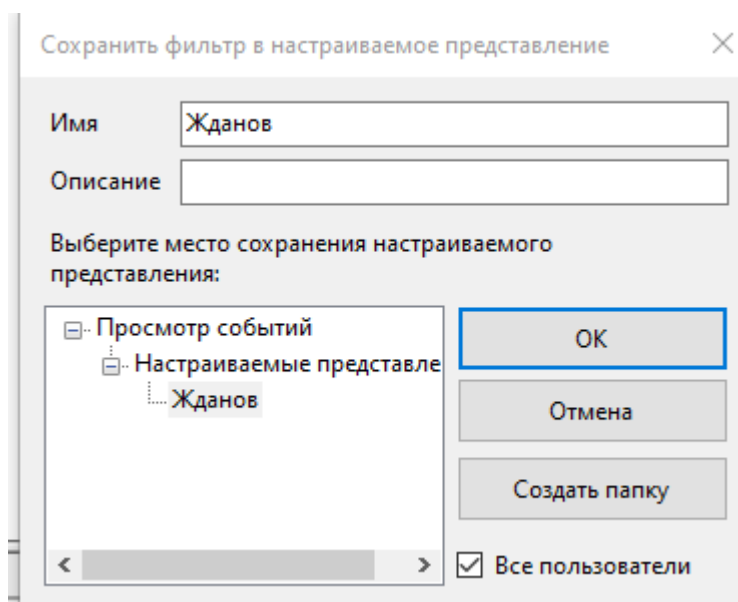


Рисунок 44 Создание папки

– введите имя настраиваемого представления – ваша фамилия;

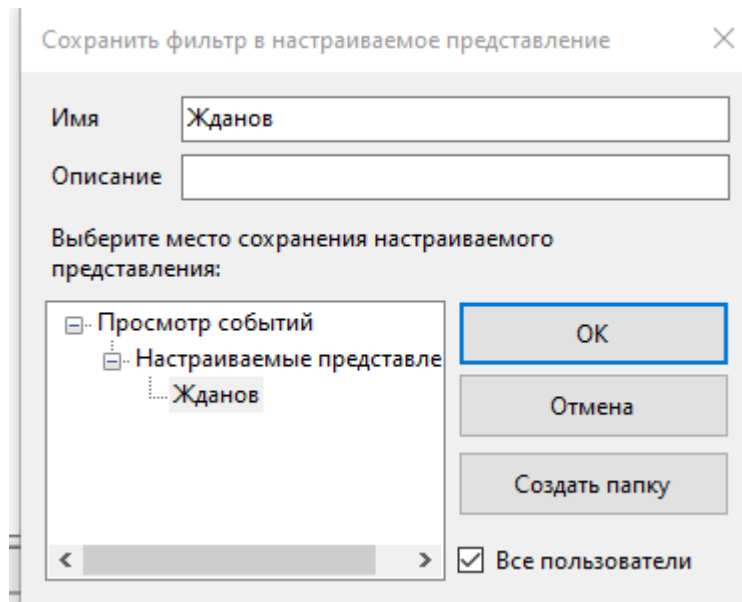


Рисунок 45 Ввод имени настраиваемого представления

— в левой части окна консоли должно появиться созданное представление.

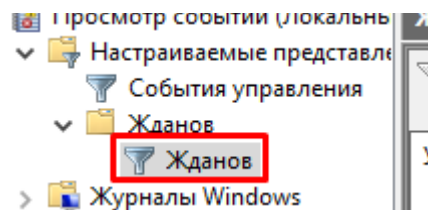


Рисунок 46 Созданное представление в левой части окна

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

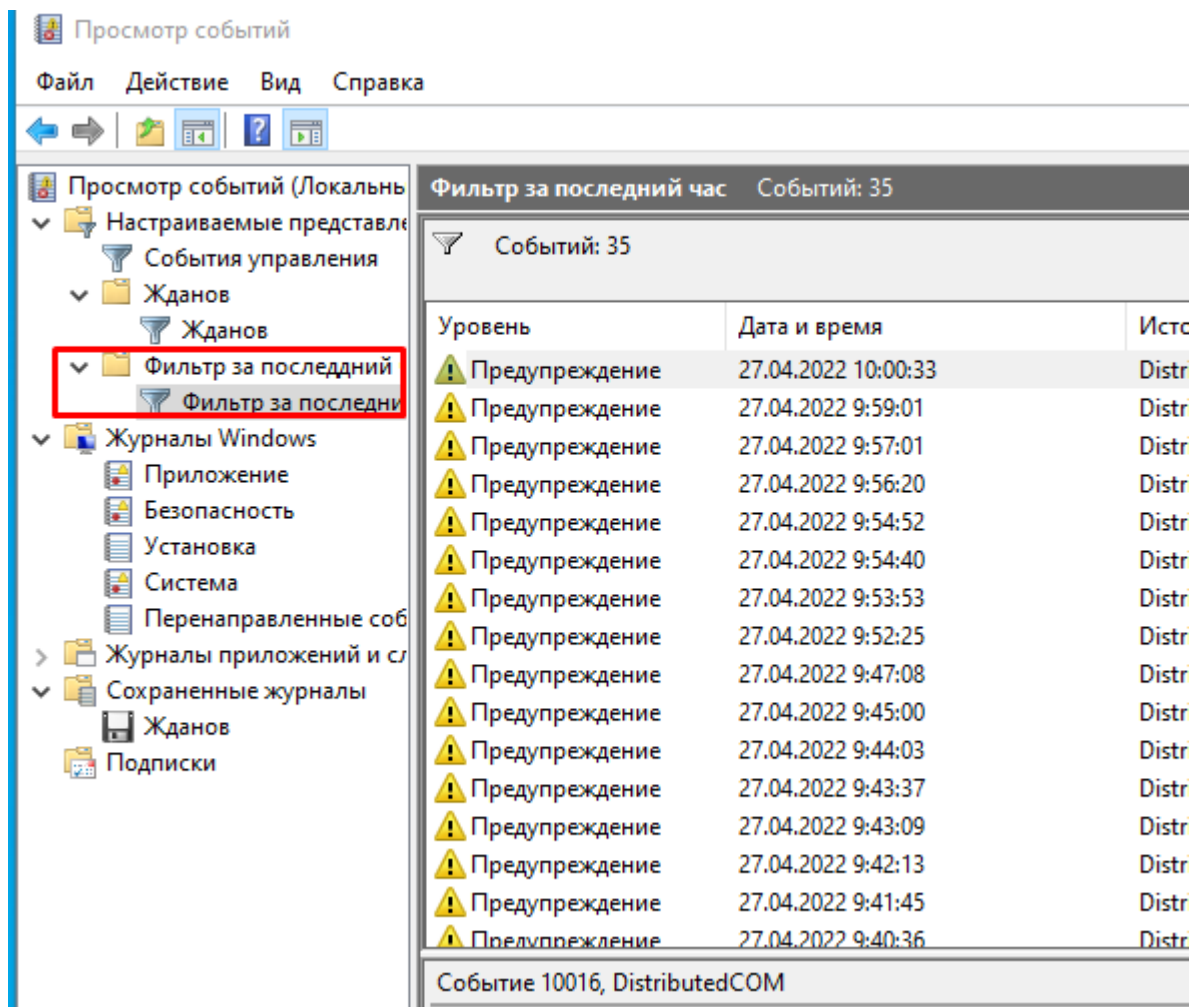


Рисунок 47 Созданное настраиваемое представление

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

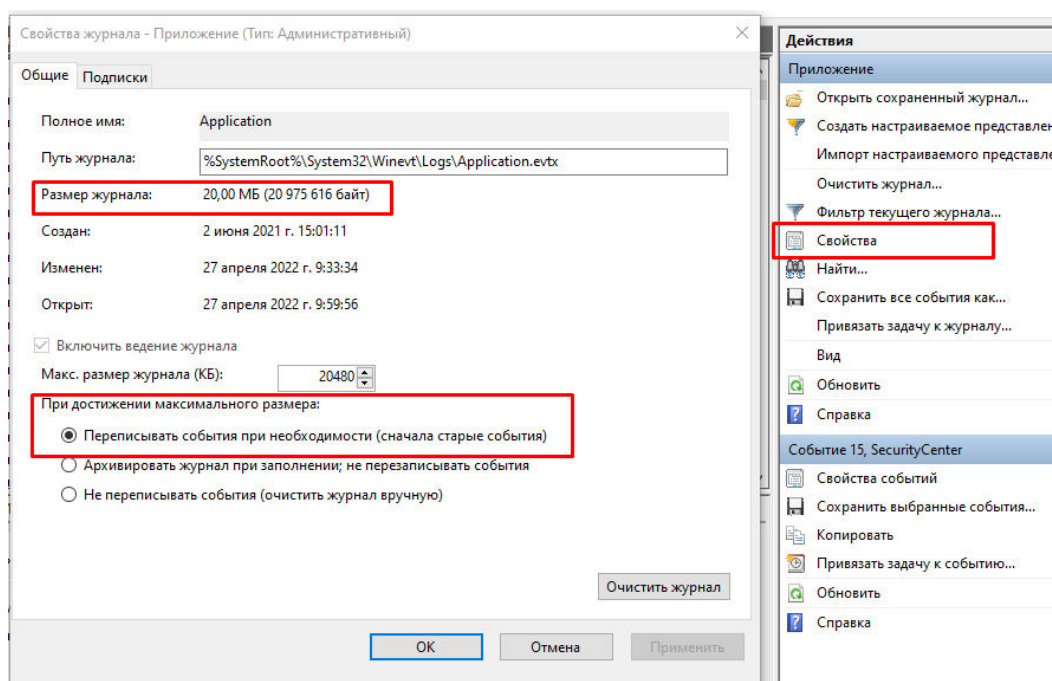


Рисунок 48 Свойства журнала «Приложение»

Контрольные вопросы

1. Что такое Просмотр событий?

Просмотр событий (англ. Event Viewer) — компонент, включённый в состав операционных систем семейства Windows NT, разрабатываемых Microsoft, который позволяет администраторам просматривать лог событий на локальном компьютере или на удалённой машине.

2. Что позволяет программа Просмотр событий?

Программа «Просмотр событий» позволяет просматривать события всех компьютеров локальной сети на любом компьютере, даже удалённом. Система может получать копии событий, зарегистрированных на различных удалённых компьютерах, и сохранять их локально.

3. Как запустить приложение Просмотр событий?

Приложение «Просмотр событий» можно открыть следующими способами:

- 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».
- Воспользоваться комбинацией клавиш Win+R для открытия диалога «Выполнить». В диалоговом окне «Выполнить», в поле «Открыть» введите eventvwr.msc и нажмите на кнопку «ОК».

4. Какие существуют категории журналов событий?

В операционной системе Windows 7 существуют две категории журналов событий:

- журналы Windows — используются операционной системой для регистрации общесистемных событий, связанных с работой приложений, системных компонентов, безопасностью и запуском;
- журналы приложений и служб — используются приложениями и службами для регистрации событий, связанных с их работой.

					ККОО.ПМ.XXX.000	Лист
						27
Изм.	Лист	№ докум.	Подпись	Дата		

5. Назовите типы журналов.

Типы журналов:

- Приложение – хранит важные события, связанные с конкретным приложением.
- Безопасность – хранит события, связанные с безопасностью, такие как вход/выход из системы, использование привилегий и обращение к ресурсам.
- Установка – в этот журнал записываются события, возникающие при установке и настройке операционной системы и ее компонентов.
- 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.
- Пересылаемые события – если настроена пересылка событий, в этот журнал попадают события, пересылаемые с других серверов.
- Windows PowerShell – в этом журнале регистрируются события, связанные с использованием оболочки PowerShell.
- События оборудования – если настроена регистрация событий оборудования, в этот журнал записываются события, генерируемые устройствами.

6. Какие существуют свойства событий (назовите несколько)?

- Источник – это программа, зарегистрировавшая событие в журнале.
- Код события – это число, определяющее конкретный тип события.
- Уровень – это уровень важности события.

7. Какие уровни важности имеют события в журналах Windows?

- Уведомление - обозначает изменение в приложении или компоненте, такое как возникновение информационного события, связанного с успешным действием, создание ресурса или запуск службы.

- Предупреждение - обозначает предупреждение общего характера на неполадку, способную повлиять на службу или привести к более серьезной проблеме, если оставить ее без внимания;
- Ошибка - обозначает, что возникла проблема, которая может повлиять на функции, внешние по отношению к приложению или компоненту, вызвавшим событие;
- Критическая ошибка - обозначает, что произошел сбой, после которого приложение или компонент, инициировавшие событие, не могут восстановиться автоматически;
- Аудит успехов – успешное выполнение действий, которые вы отслеживаете через аудит, например использование какой-либо привилегии;