|  |
| --- |
| **МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ** |
| **ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ** |
| **УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ** |
| **«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»** |
|  |
| Институт информационных технологий и управления в технических системах |
| (полное название института) |
|  |
| кафедра «Информационные системы» |
| (полное название кафедры) |

**ОТЧЁТ**

по лабораторной работе №8

на тему«аудит»

по дисциплине **«**Операционные системы»

Выполнил

студент ИИТУТС

группы ИС/б-18-2-о

Радыгина Екатерина

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | | | | | | | | |
|  | (должность, учёная степень преподавателя) | | | | | | | | |
|  |  | | | | | | | | |
|  | (ФИО преподавателя) | | | | | | | | |
|  | « |  | » |  |  |  | 20 | 20 | г. |
|  |  | | | | | | | | |
|  | (оценка) | | | | | | | | |
|  |  | | | | | | | | |
|  |  | | | | | | | | |

Севастополь 2020

**8.1 Цель работы**

Ознакомиться с встроенными средствами протоколирования событий ОС Windows.

**8.2 Ход работы**

8.2.1 Откроем раздел «Локальная политика безопасности». Для этого нажмём кнопку Пуск, в строке Поиск введём secpol.msc и нажмём по имени.

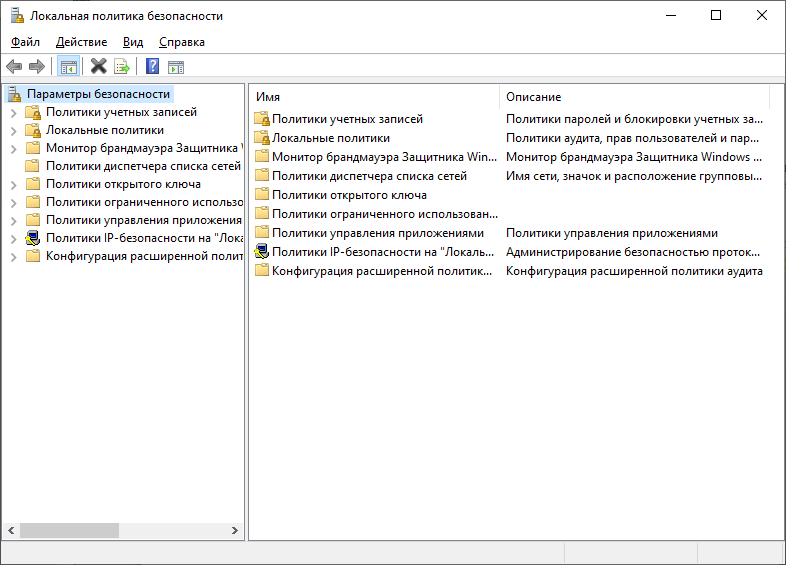


Рисунок 8.1 – Окно «Локальная политика безопасности»

В левой области дважды щелкнем строку Локальные политики и выберем пункт Политика аудита. Дважды щелкнем событие, за которым нужно наблюдать, например, Аудит входа в систему. Установить флажки Успех или Отказ (или оба одновременно), затем нажмём ОК.

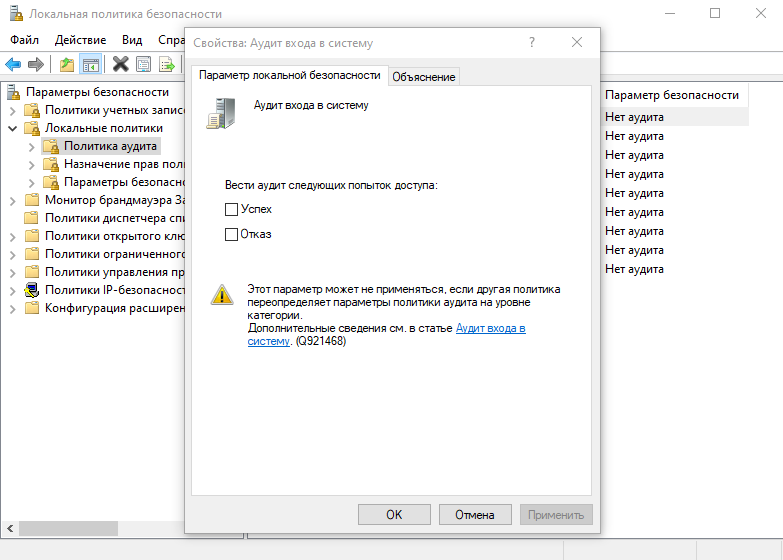


Рисунок 8.2 – «Политика аудита»

8.2.2 Чтобы отследить пользователей, открывающих документ, необходимо выполнить следующие действия:

1. Щелкнуть правой кнопкой мыши документ, контроль за которым нужно установить, и выбрать из контекстного меню пункт Свойства.
2. На вкладке Безопасность нажать кнопку Дополнительно и перейти на вкладку Аудит.
3. Нажать кнопку Продолжить. Если отображается запрос на ввод пароля администратора или его подтверждения, указать пароль или предоставить подтверждение.
4. Щелкнуть кнопку Добавить. В поле Введите имена выбираемых объектов ввести имя пользователя или группы, за которыми нужно установить наблюдение и нажать ОК в последующих четырех диалоговых окнах.

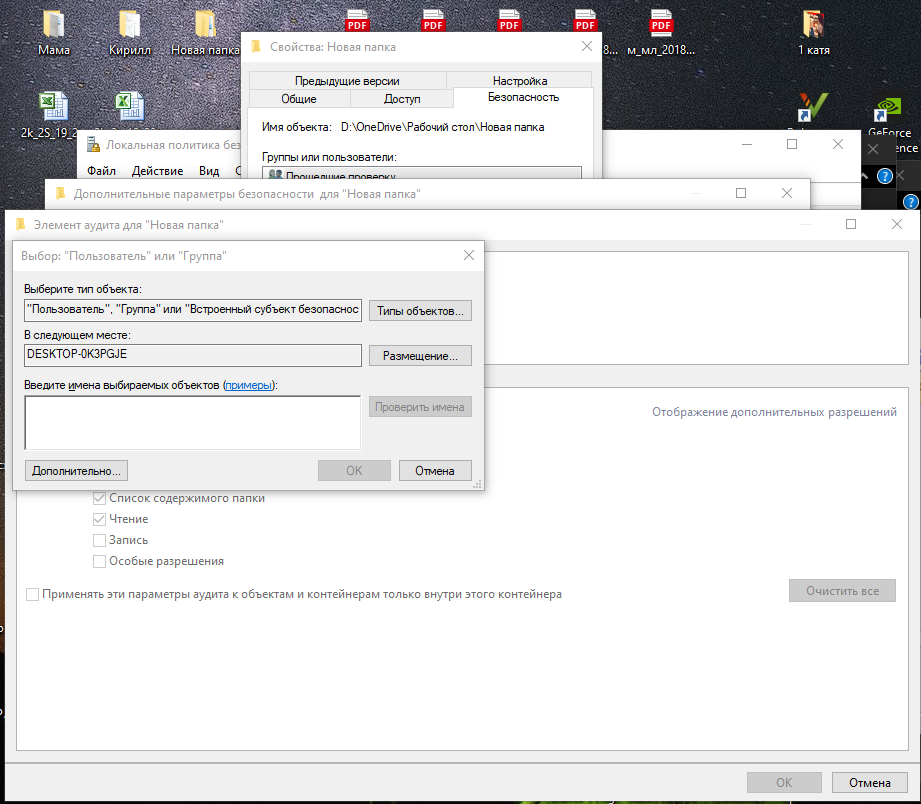


Рисунок 8.3 – Установление наблюдения за пользователями

8.2.3 Просмотр журнала аудита осуществляется в разделе «Просмотр событий». Для открытия раздела нажмём кнопку Пуск и введём Просмотр событий, затем откроем его, щёлкнув по нему левой кнопкой мыши.

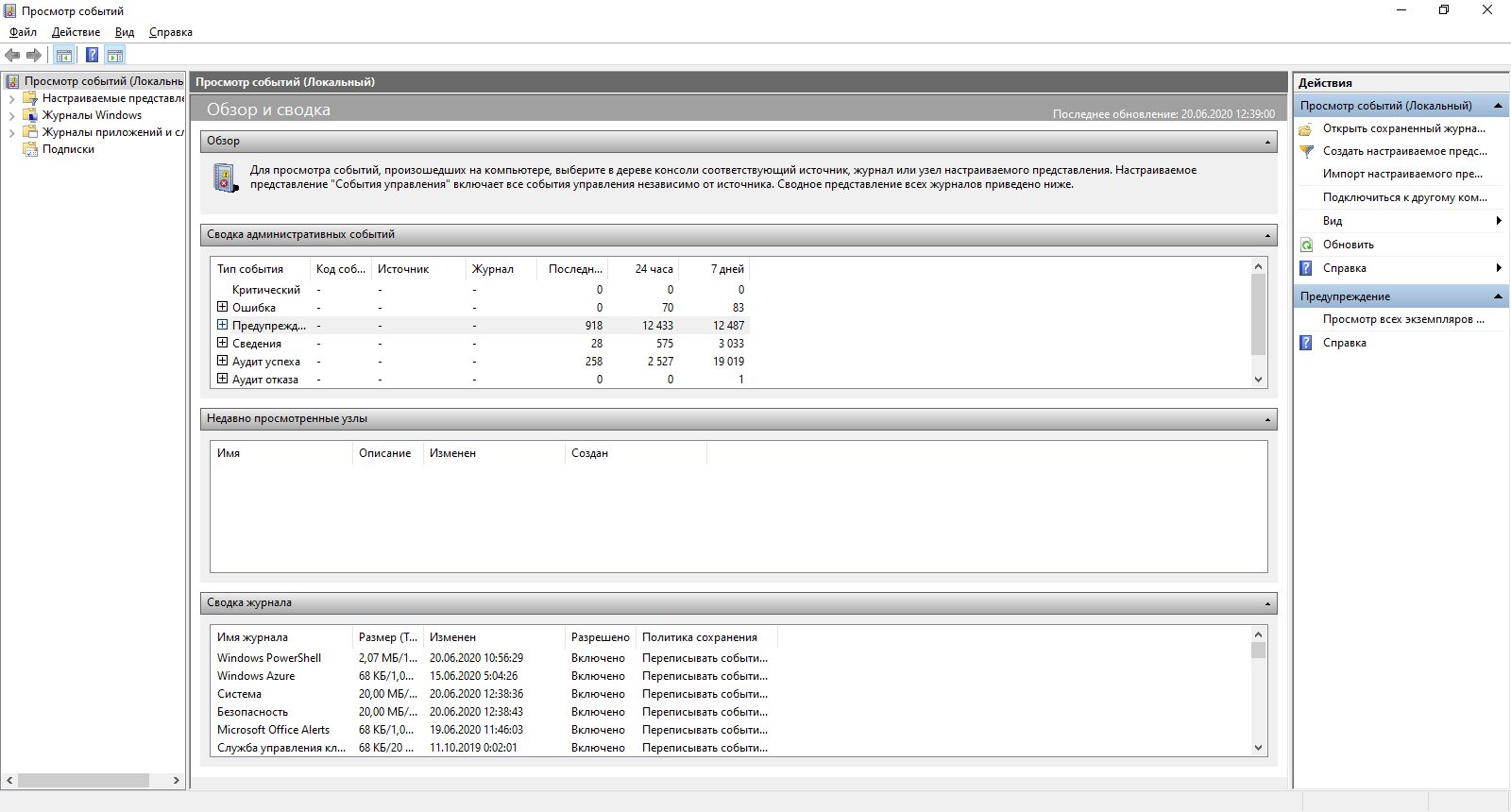


Рисунок 8.4 – Окно «Просмотр событий»

8.2.4 Чтобы настроить, просмотреть или изменить настройки аудита файлов и папок, нужно зайти в Свойства этого файла/папки. В окне свойств папки или файла перейти на вкладку Безопасность, нажмите кнопку Дополнительно и затем перейти на вкладку Аудит. И установить нужные параметры.

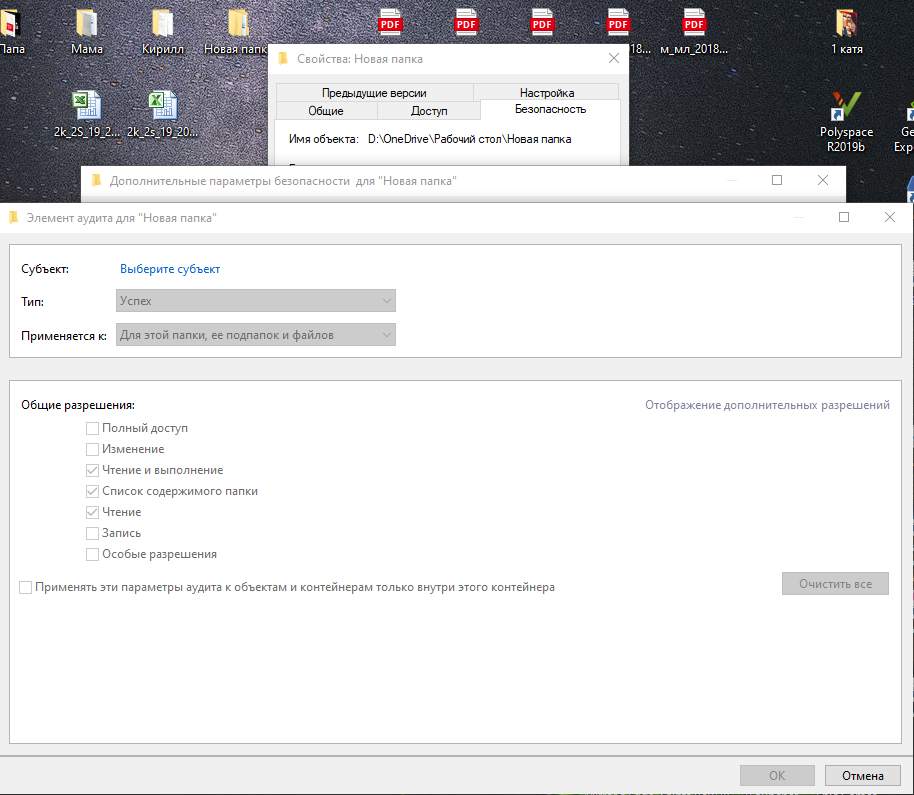


Рисунок 8.5 – Настройки аудита файлов\папки

**Вывод**

В ходе лабораторной работы ознакомились с встроенными средствами протоколирования событий ОС Windows.