1 Введение

Цель работы: освоение способов управления службами в ОС Windows 10, изучение специфики работы планировщика задач, а также ознакомление со структурой и особенностями работы процессов и потоков в операционных системах.

Задание для лабораторной работы:

1. Задать через командную строку перезагрузку компьютера через минуту после первого сбоя;
2. Назначить автоматический запуск калькулятора после входа в Windows;
3. Заменить стандартный диспетчер задач на Process Explorer;
4. Определить какой раздел реестра «Сапер» делает записи о рекордах;
5. Вывести информацию о Cookies при работе Internet Explorer;
6. Определить какие файлы реестра открывает косынка;
7. Определить какие системные файлы читает при работе WMPlayer;
8. Определить какой процесс запускается при открытии “Установки и удаления программ”;
9. Определить в какой файл записываются данные при работе с калькулятором.
   1. Ход работы
      1. Управление службами

Запустим диспетчер задач, нажав комбинацию клавиш ctrl+alt+del. Откроем в вкладку «Службы». Диспетчер задач с открытой вкладкой представлен на рисунке 1.

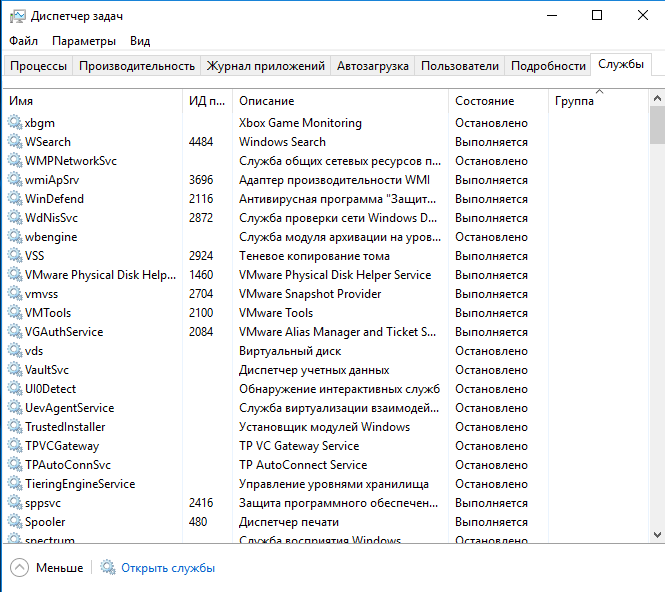


Рисунок 1 – Диспетчер задач.

Чтобы увидеть возможные действия, нужно щелкнуть правой кнопкой по службе из списка. Запустим родительский контроль. Запущенная служба представлена на рисунке 2.

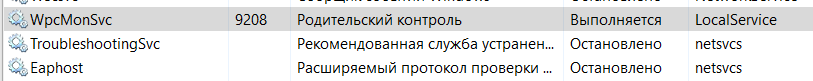


Рисунок 2 – Запущенная служба.

Запустим оснастку «Службы». Для этого нужно нажать на кнопку

«Открыть службы» на вкладке «Службы». Для запуска оснастки из командной строки, необходимо выполнить services.msc. На рисунке 3 показана оснастка

«Службы».

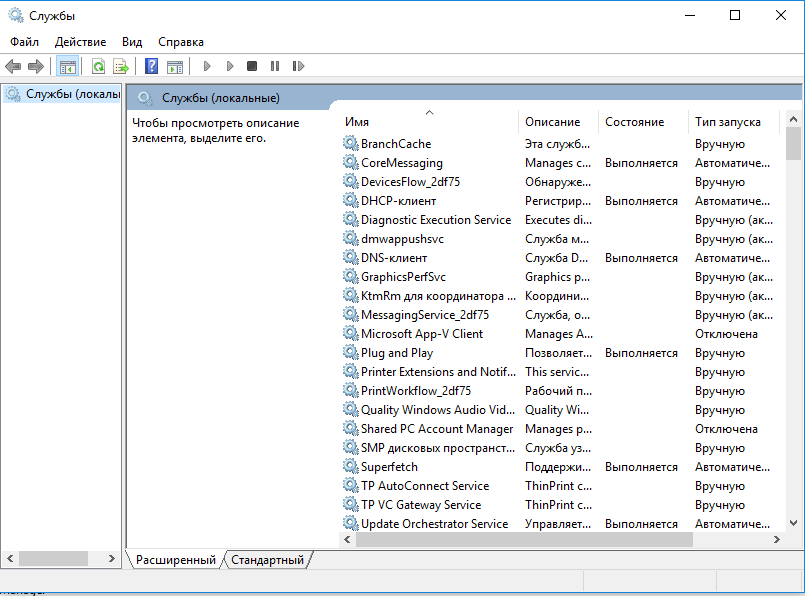


Рисунок 3 – Оснастка «Службы».

Откроем свойства службы «Windows Audio» и отключим ее. Чтобы открыть свойства службы, необходимо нажать два раза на службу и откроется окно свойств. Далее нажимаем на кнопку «Остановить». Ниже на рисунке 4 представлено окно свойств.

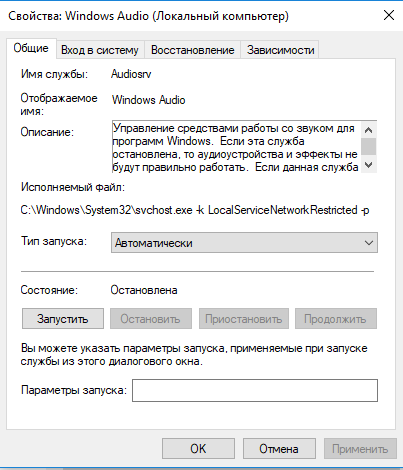


Рисунок 4 – Окно свойств для Windows Audio.

Далее посмотрим зависимые службы «Система событий COM+» и попробуем ее отключить. Чтобы посмотреть зависимости службы, откроем вкладку «Зависимости». На рисунке 5 показана вкладка «Зависимости».

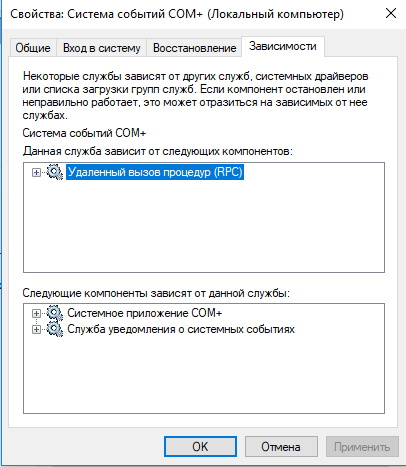


Рисунок 5 – Зависимости службы «Система событий СОМ+».

Пробуем отключить службу. Нам выдает предупреждение о том, что зависимые службы будут отключены. Предупреждение представлено на рисунке 6.

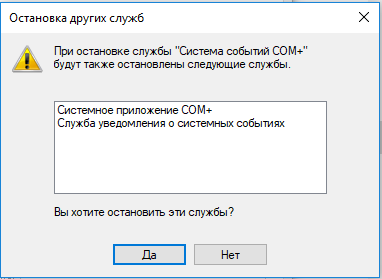


Рисунок 6 – Предупреждение.

Далее для службы «Темы» установим тип запуска «Вручную». Для этого в типе запуска выберем пункт «Вручную». На рисунке 7 показано окно свойств.

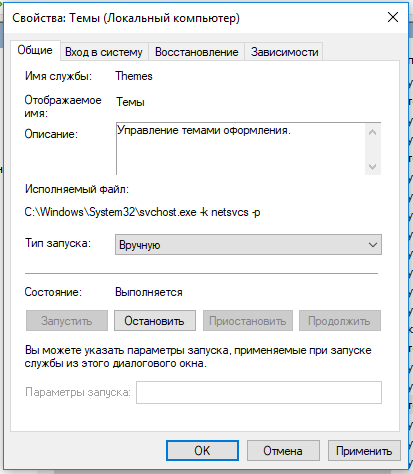


Рисунок 7 – Установка типа запуска «Вручную».

Установим параметры восстановления для службы «Диспетчер печати» Для этого выберем раздел «Восстановление» и при первом сбое установим пункт «Перезагрузка службы» а при втором сбое установим пункт

«Перезагрузка компьютера» с выводом сообщения через 2 минуты. На рисунке 8 представлен раздел «Восстановление».

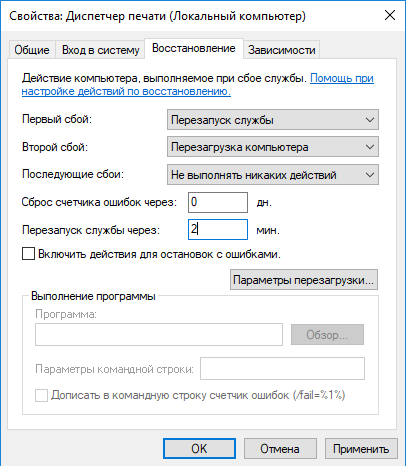


Рисунок 8 – Раздел «Восстановление»

Завершим процесс spoolsv.exe При первом завершении процесс должен перезапуститься, при втором завершении через 2 минуты Windows должна выдать сообщение о перезагрузке. На рисунке 9 показано сообщение.

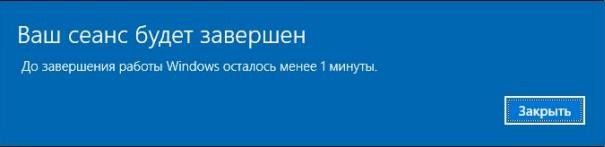


Рисунок 9 – Сообщение о завершении сеанса.

Чтобы сменить права службы, необходимо в свойствах выбрать вкладку

«Вход в систему». На рисунке 10 показана вкладка службы.

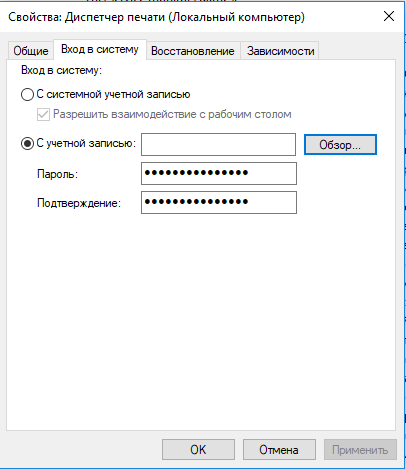


Рисунок 10 – Вход в систему.

Запустим командную строку. Чтобы увидеть запущенные службы, введем команду net start. На рисунке 11 представлена командная строка с запущенными службами.

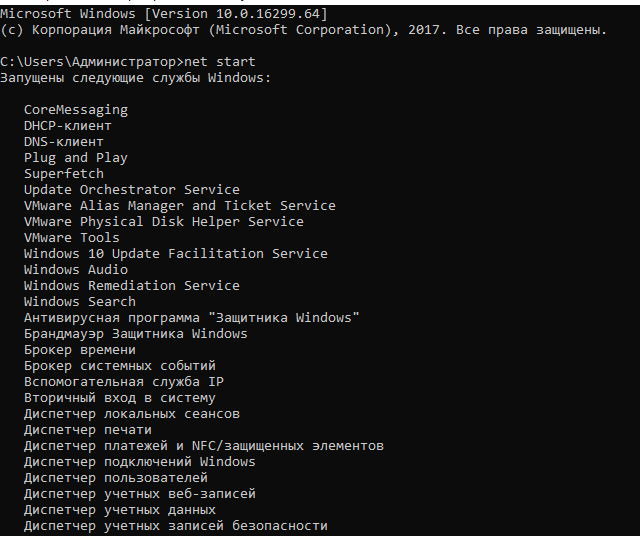


Рисунок 11 – Запущенные службы.

Запустим команду «Журналы и оповещения производительности». Для этого введем команду net start pla. Также возможно остановить службу, для этого нужно ввести команду net stop. Результат представлен на рисунке 12.

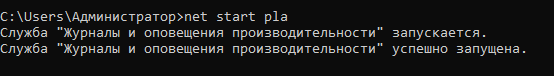


Рисунок 12 – Запуск команды.

Выведем список служб, используя команду sc query и sc queryex. Команда sc query выводит такие данные о службе, как имя (SERVICE\_NAME), отображаемое имя (DISPLAY\_NAME), состояние (STATE) и другие данные, не рассматриваемые в данной работе. Команда sc queryex дополнительно выводит идентификатор процесса (PID), в рамках которого запущена служба. На рисунках 13 и 14 представлено выполнение команд.

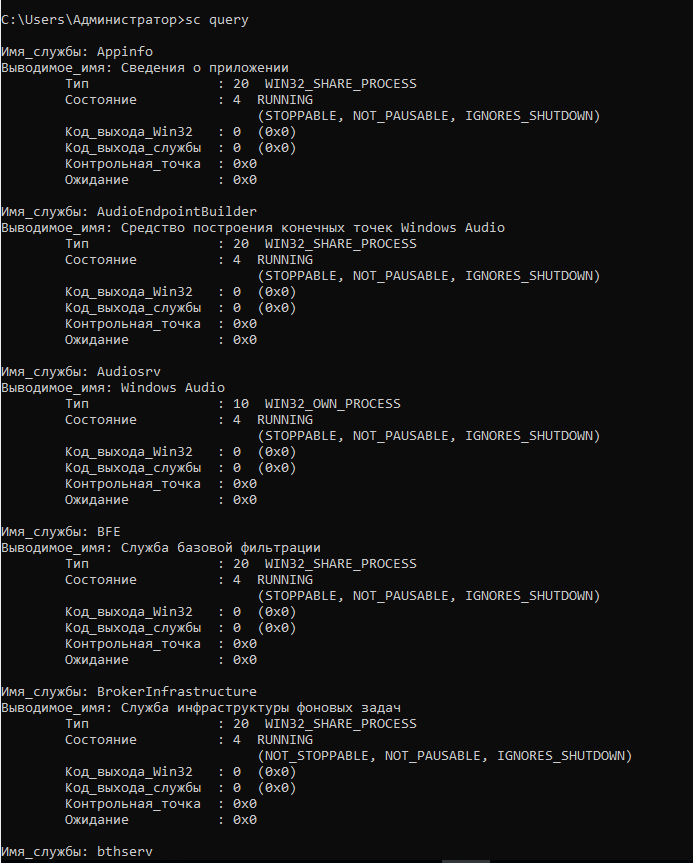


Рисунок 13 – Выполненная команда sc query.

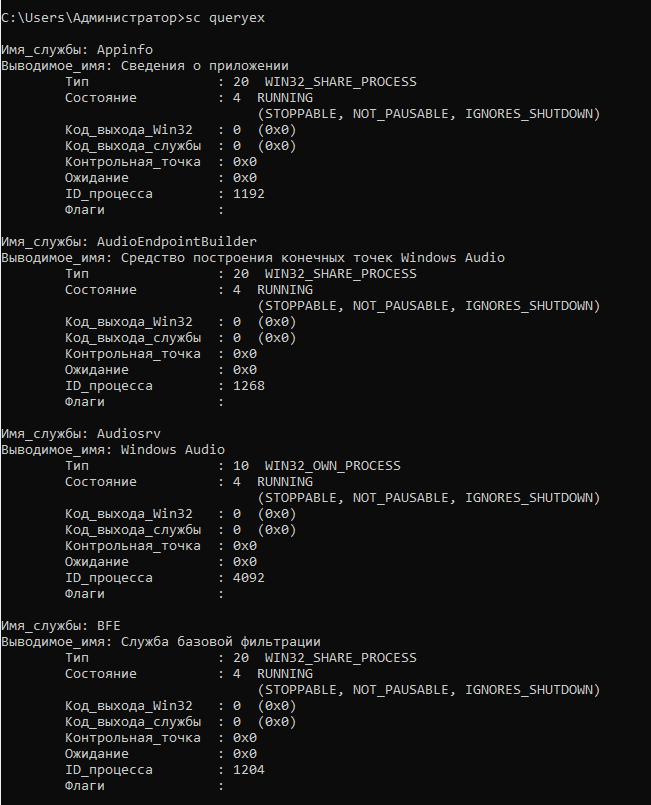


Рисунок 14 – Выполненная команда sc query.

Выведем список установленных интерактивных служб. Для этого введем команду sc query type=all state=inactive. На рисунке 15 представлено выполнение команды.

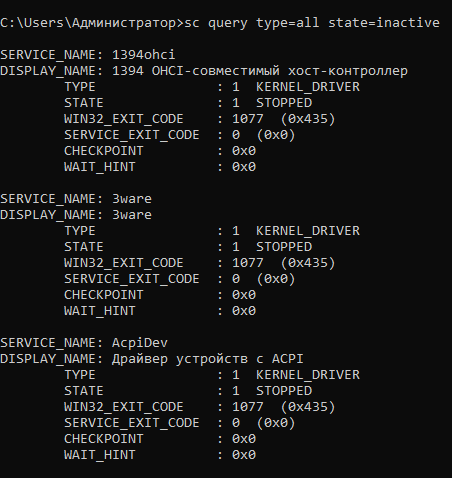


Рисунок 15 – Список установленных интерактивных служб.

Выведем расширенную информацию о запущенной службе. Для вывода информации о конкретной службе используются также команды sc qc, sc qdescription, sc qfailure и другие. После команды пишется имя соответствующей службы. На рисунке 16 показана расширенная информация о службе.

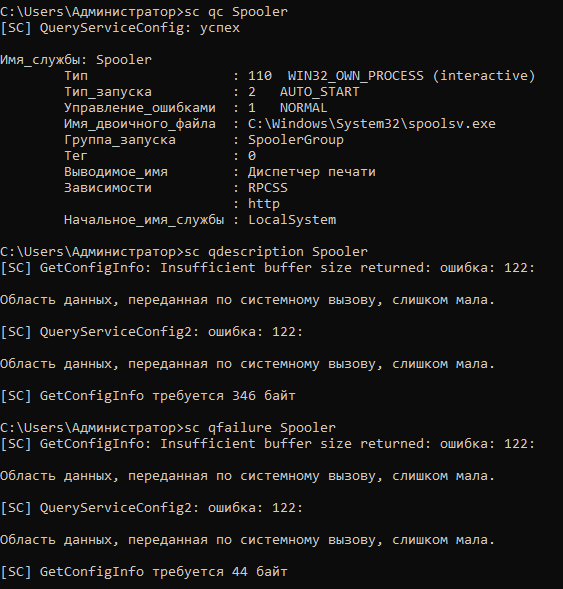


Рисунок 16 – Расширенная информация о службе.

Также можно вывести список служб, зависящих от данной службы. Для этого используется команда sc enumdepend. Выведем информацию с помощью этих команд о службе CryptSvc – «Службы криптографии». На рисунке 17 показана информация о «Службы криптографии».

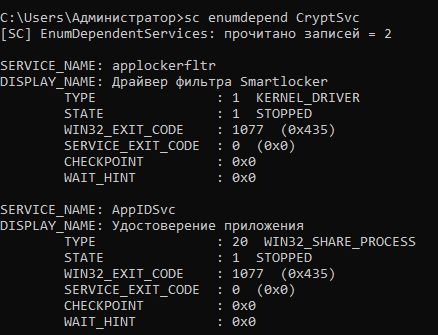


Рисунок 17 - Информация о «Службы криптографии».

Для изменения состояния службы используются следующие команды:

1. sc start: запуск службы;
2. sc pause: приостановка службы, если возможно;
3. sc continue: продолжение работы службы, если она была приостановлена;
4. sc stop: остановка службы, если возможно.

После команды пишется имя службы, состояние которой нужно изменить. Для изменения типа запуска определённой службы используется команда sc config с последующим именем службы и списком изменяемых параметров.

Для изменения типа запуска используется параметр start. Его значения:

* 1. boot: запуск при инициализации ядра Windows;
  2. system: запуск сразу после инициализации ядра Windows;
  3. auto: запуск сразу после загрузки Windows;
  4. demand: запуск по требованию пользователя;
  5. disabled: служба.

С помощью команд изменим тип запуска службы «Темы» на

«Автоматический». На рисунке 18 представлено выполнение команды.

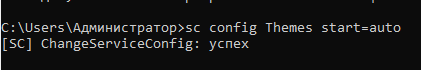


Рисунок 18 – Выполненная команда.

Для изменения параметров восстановления определённой службы используется команда sc failure с последующим именем службы и списком изменяемых параметров. Параметры следующие:

1. actions: действия, выполняемые при сбое и задержки перед их выполнением в миллисекундах. Сначала пишется действие при первом сбое, затем задержка, отделяемая от него косой чертой («/»). Если нужно задать действия при следующих сбоях, далее снова ставится косая черта и пишется следующее действие и задержка.

Возможные действия:

1. run: запуск программы;
2. reboot: перезагрузка компьютера. Используется совместно с параметром reboot;
3. restart: перезапуск службы.

Для службы Spooler установим следующие параметры восстановления:

1. при первом сбое служба должна перезапуститься через 5 секунд;
2. при втором − через 10 секунд;
3. при третьем – компьютер должен перезагрузиться через 20 секунд с выводом соответствующего сообщения.

Счётчик сбоев должен быть сброшен через 1 час. Выполнение команды представлено на рисунке 19.



Рисунок 19 – Выполненная команда

Команда sc interrogate используется совместно с открытой оснасткой

«Службы». При изменении состояния службы с помощью командной строки оно не сразу обновляется в оснастке. Чтобы принудительно обновить его, вводится эта команда с последующим именем службы.

В оснастке «Службы» остановим службу «Телефония». Для этого используем команду sc stop и обновим ее состояние с помощью команды sc interrogate. Состояние службы в оснастке показано на рисунке 20.

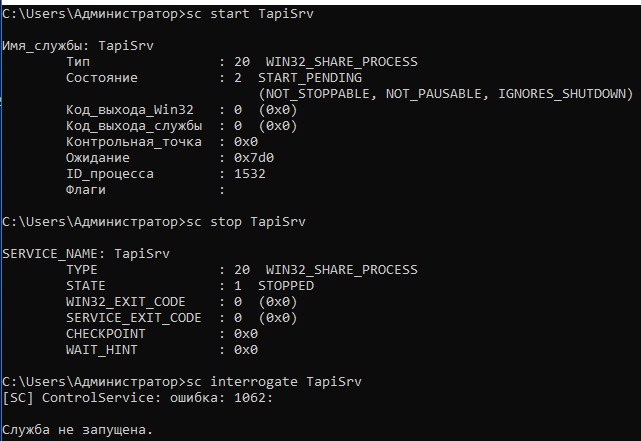


Рисунок 20 – Состояние службы в оснастке.

Создадим новую службу. В качестве исполняемого файла выберем блокнот. Зададим ему автоматический тип запуска и произвольное отображаемое имя. Служба будет обладать правами пользователя «Система».

Чтобы создать новую службу, необходимо воспользоваться командой sc create. При этом после команды требуется указать имя создаваемой службы и

путь к исполняемому файлу (параметр binPath). Дополнительно можно указать тип запуска (start), зависимости (depend), отображаемое имя (DisplayName), имя (obj) и пароль (password) учётной записи для входа и другое. Создание службы показано на рисунке 21.

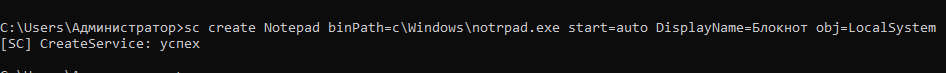


Рисунок 21 – Создание службы.

Убедимся, что созданная служба отображается в списке. На рисунке 22 показана служба.

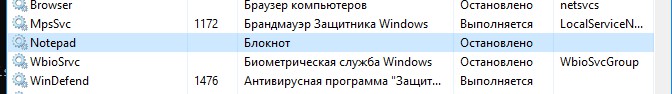


Рисунок 22 – Созданная служба в списке.

Чтобы удалить службу, используется команда sc delete с последующим именем службы. Удаление службы показано на рисунке 23.

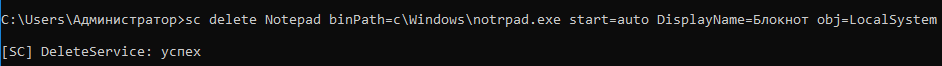


Рисунок 23 – Удаление службы.

* + 1. Автоматизация выполнения административных задач

Планировщик заданий - это оснастка MMC, позволяющая назначать автоматически выполняемые задания, запуск которых производится в определенное время или при возникновении определенных событий.

Запустим планировщик заданий, но сначала убедимся, что служба включена. На рисунке 24 представлена служба.

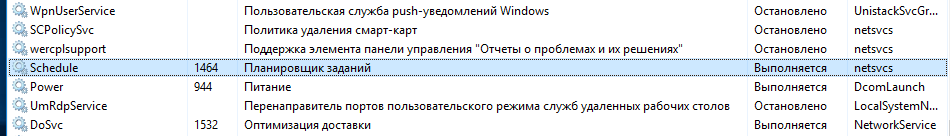


Рисунок 24 – Служба «Планировщик заданий».

Чтобы запустить задачу, нужно открыть консоль управления ММС и добавить в нее оснастку «Планировщик заданий» и после в меню действий к оснастке выбрать пункт «Создать задачу» На рисунках 25 и 26 показан процесс добавления оснастки и окно создание простой задачи.

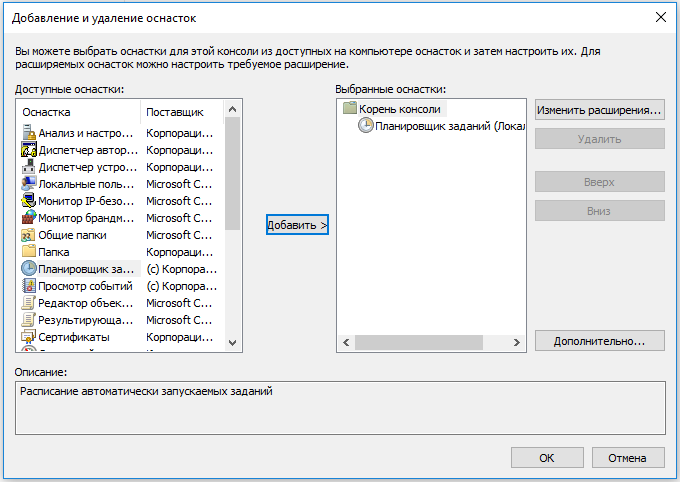


Рисунок 25 – Добавление оснастки.

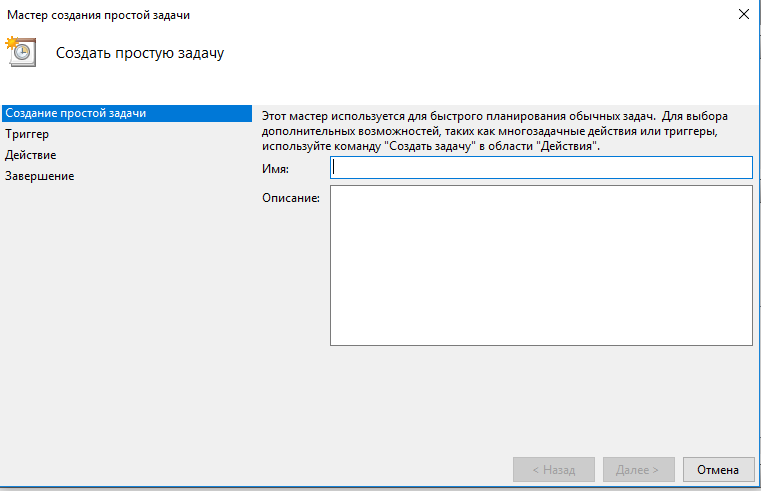


Рисунок 26 – Мастер создания простой задачи.

Создадим задачу по запуску командной строки. Сначала для задачи присвоим имя. На рисунке 27 показано присваивание имени.

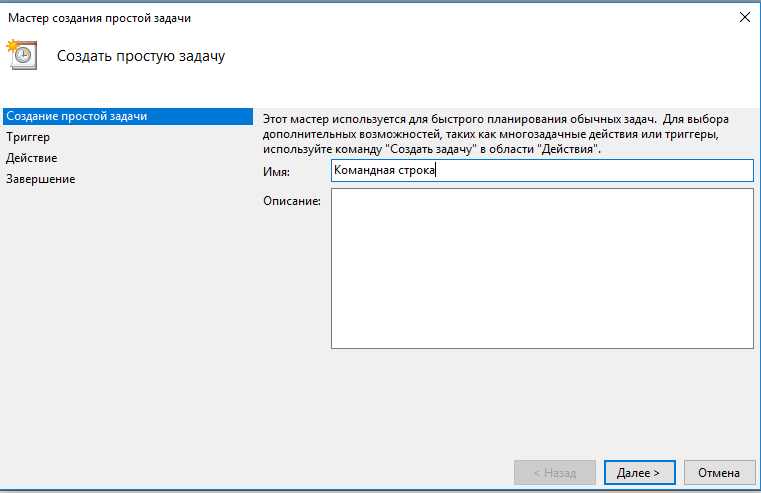


Рисунок 27 – Присваивание имени.

В разделе «Триггер задачи» выберем пункт «При входе в Windows». На рисунке 28 показан выбор пункта.

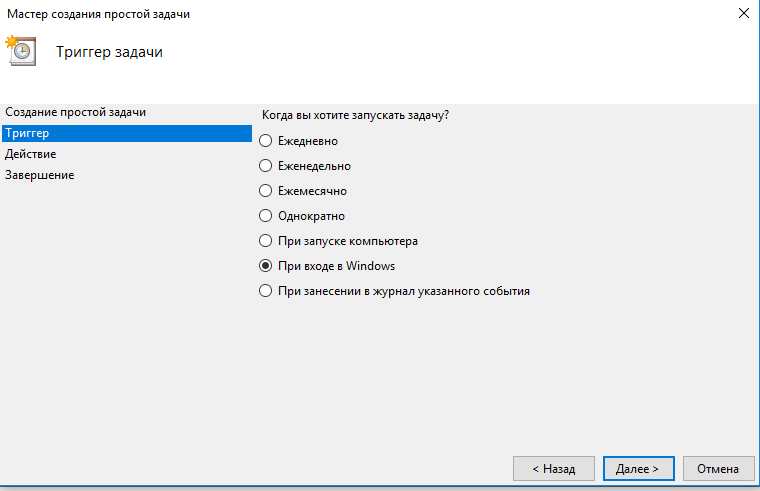


Рисунок 28 – Выбор триггера.

В разделе «Действие» выберем пункт «Запустить программу». На рисунке 29 показан выбор пункта.

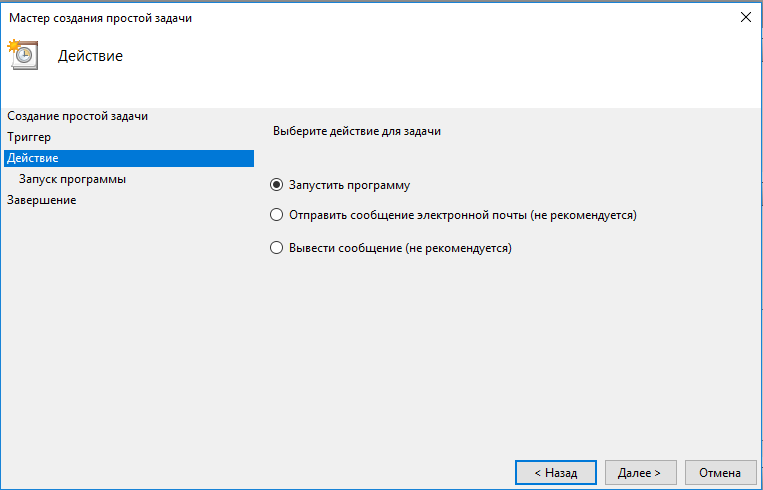


Рисунок 29 – Выбор действия.

Далее в разделе «Запуск программы» будет предложено через

«Проводник» указать файл программы. Выберем из списка командную строку. На рисунке 30 показан выбор программы.

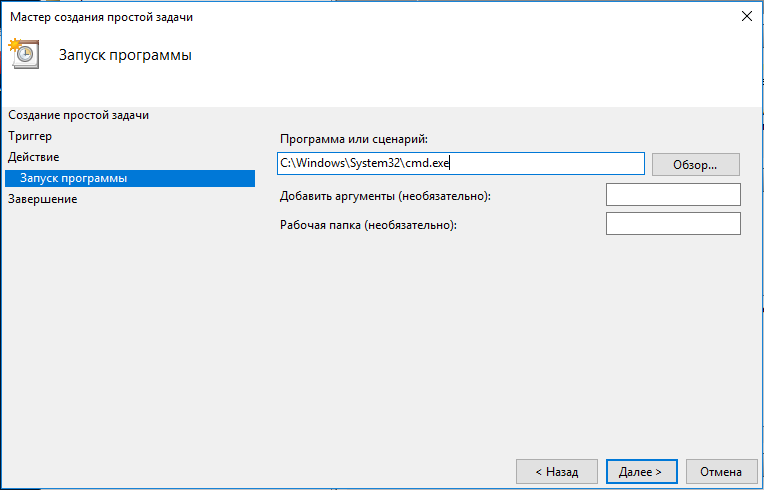


Рисунок 30 – Выбор программы.

В разделе «Завершение» проверяем все пункты и нажимаем кнопку

«Готово». На рисунке 31 показан раздел «Завершение.

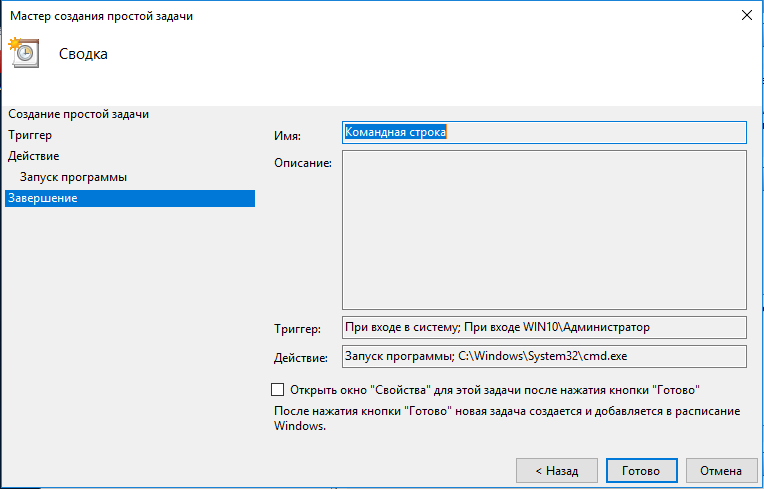


Рисунок 31 – Раздел «Завершение».

Проверим созданную задачу в библиотеке планировщика. Выделим задачу правой кнопкой и в меню действий выберем пункт «Выполнить». На рисунке 32 показана задача в библиотеке.

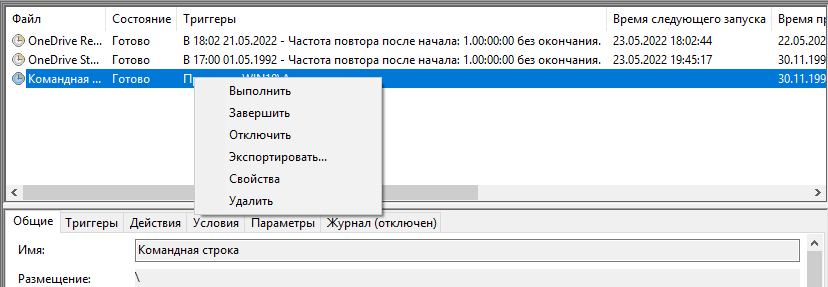


Рисунок 32 – Созданная задача в библиотеке.

Проверка, что задача выполняется представлена на рисунке 33.

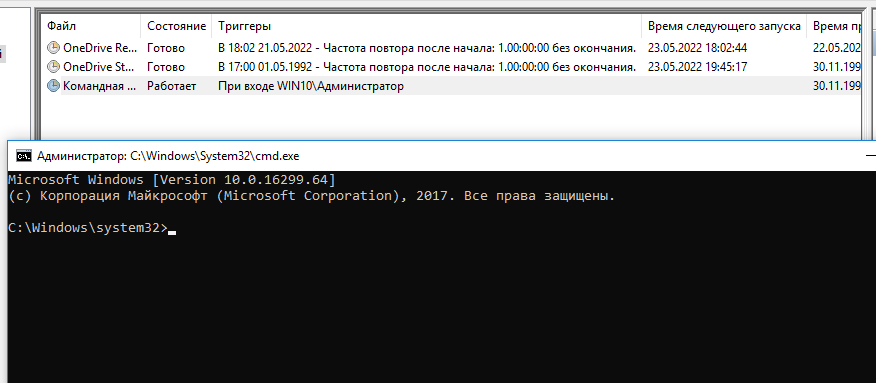


Рисунок 33 – Запущенная командная строка.

Свойства задачи представлены на рисунке 34.

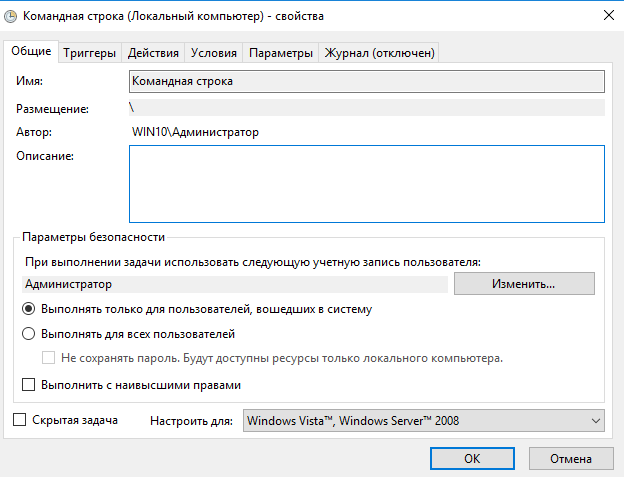


Рисунок 34 – Свойства задачи.

Добавим в планировщик заданий «Дефрагментация диска». Для этого в мастере планирования задания необходимо нажать «Обзор» и выбрать программу Defrag.exe. Выберем ежедневное выполнение задания. На рисунке 35 показана созданная задача.

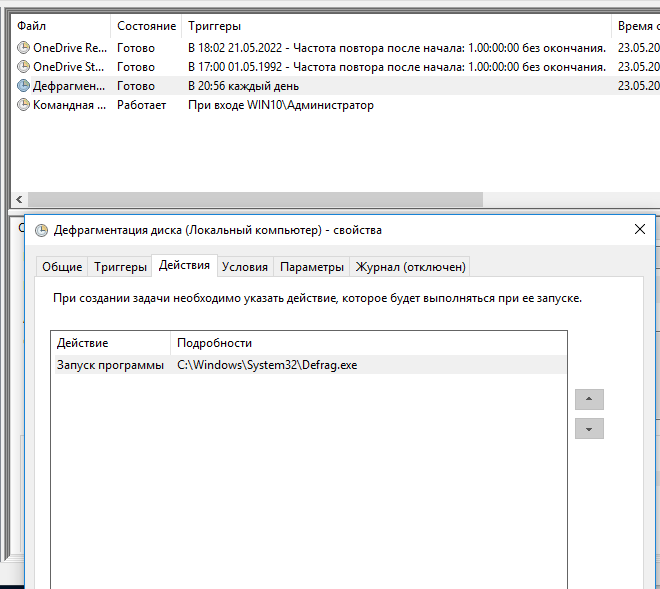


Рисунок 35 – Созданная задача.

* + 1. Работы с процессами и потоками

Запустим «Process Explorer». В окне перечислены все работающие в системе процессы, представленные в виде древовидной структуры. Чтобы посмотреть свойства процесса, нужно щелкнуть два раза правой кнопкой мыши. На рисунках 36 и 37 показано главное окно и свойства процесса.

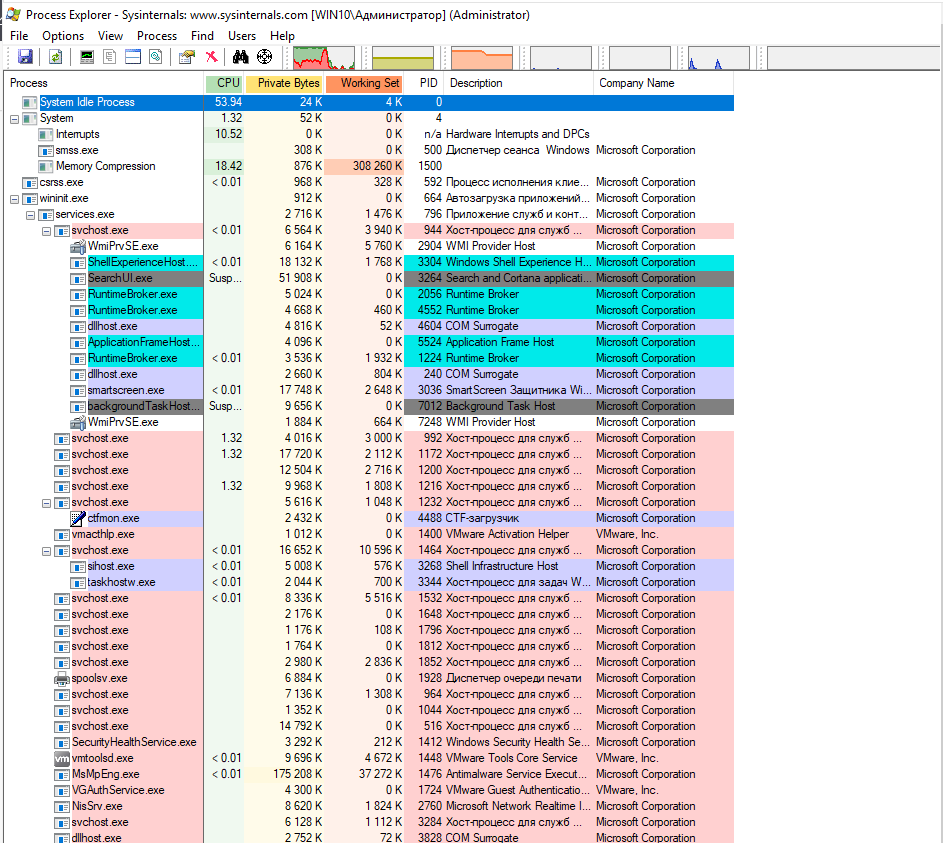


Рисунок 36 – Главное окно.

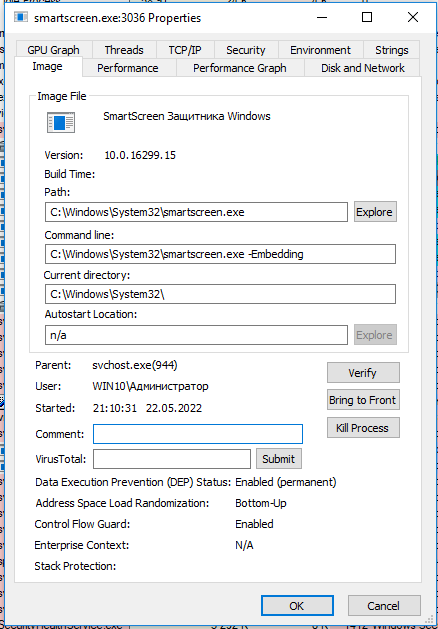


Рисунок 37 – Свойства процесса.

На вкладке «Образ» указаны путь к программе, родительский процесс, текущий рабочий каталог, предоставляется возможность уничтожения процесса и др. На вкладке «Производительность» выводится информация об использовании процессора, описание процесса, объем занятой памяти, на основе которых на вкладке «График производительности» построены графики.

Существует два режима работы программы. В режиме дескрипторов и в режиме библиотек DLL, переключение между режимами осуществляется с помощью сочетания клавиш Ctrl+H – переключение в режим отображения описателей и Ctrl+D – переключение в режим отображения DLL.

В режиме дескрипторов отображаются все открытые дескрипторы выбранного в верхнем окне процесса. На рисунке 38 показан режим отображения дескрипторов.

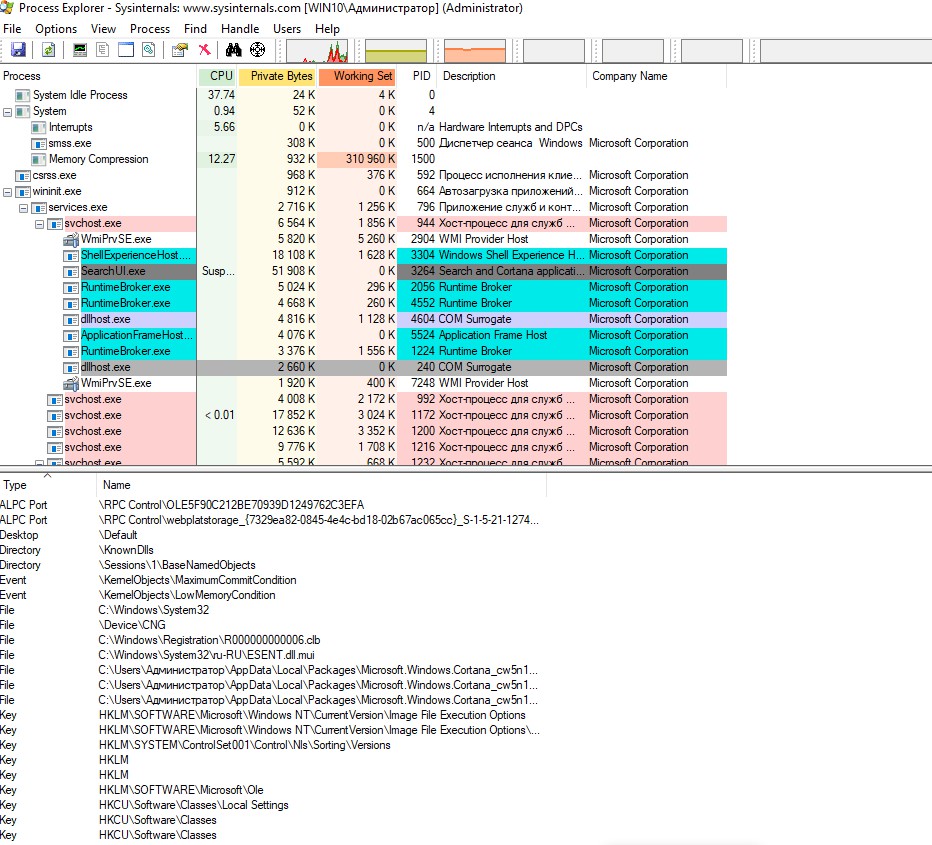


Рисунок 38 – Режим отображения дескрипторов.

В режиме библиотек DLL отображаются все загруженные процессом динамические библиотеки и отображенные в память файлы. На рисунке 39 показан режим отображения библиотек DLL.

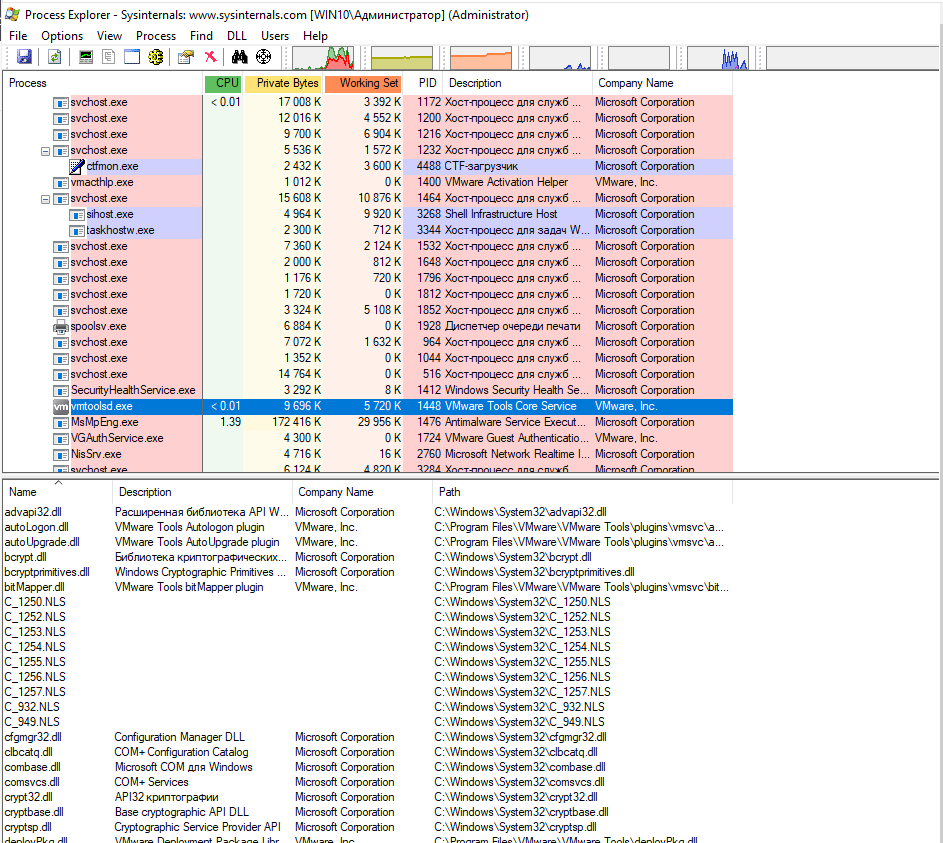


Рисунок 39 – Режим отображения библиотек DLL.

Process Explorer позволяет приостановить/возобновить работу процесса, изменить приоритет, уничтожить процесс или уничтожить процесс и его дерево. Для этого необходимо щелкнуть на нужный процесс правой кнопкой мыши и в открывшемся контекстном меню выбрать необходимое действие.

Процесс explorer.exe, входит процесс procexp.exe, можно уничтожить это дерево процессов. На рисунке 40 показано уничтожение дерева процессов.

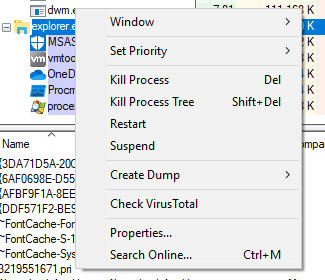


Рисунок 40 – Уничтожение дерева процессов.

При помощи пункта меню «Параметры – Вместо диспетчера задач» можно заменить стандартный Диспетчер задач Windows на Process Explorer. Замена диспетчера задач показана на рисунке 41.

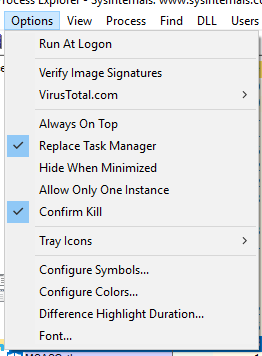


Рисунок 41 – Замена диспетчера задач.

Далее сохраним в текстовый файл список всех процессов с описаниями и объемом занятой каждым из них памяти. На рисунке 42 показано сохранения файла.

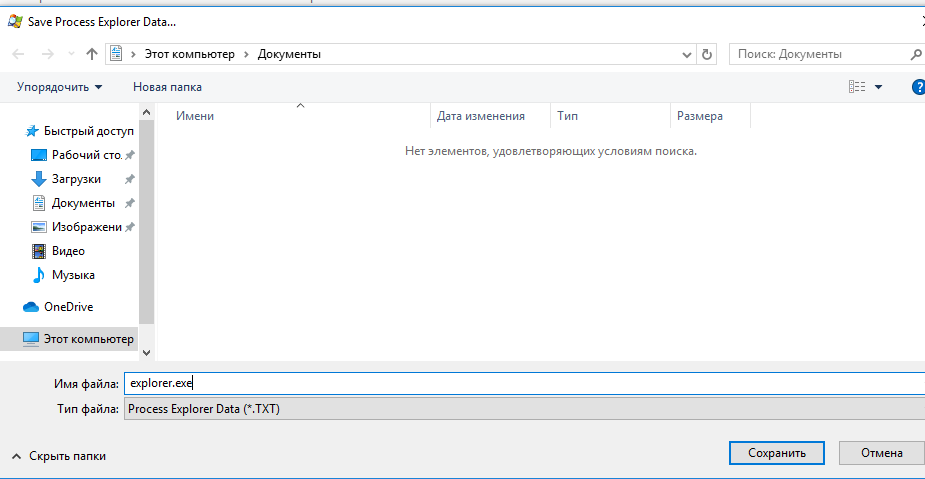


Рисунок 42 – Сохранение файла.

Можно рассчитать влияние приоритета процесса на количество выделяемого процессорного времени, а также задать приоритет. На рисунке 43 показана установка приоритета.

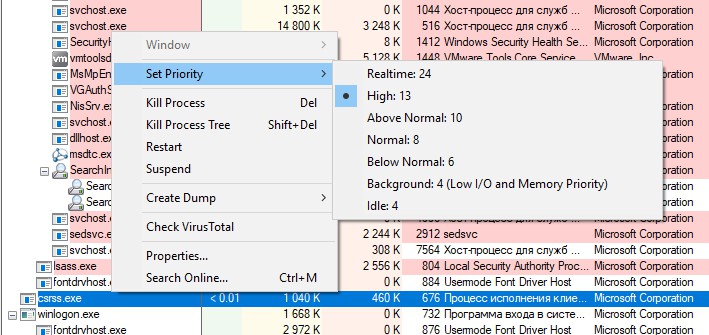


Рисунок 43 – Установка приоритета.

На рисунке 44 показано, сколько выделяется суммарного времени за одну минуту при заданном приоритете на 24 и 4 часа.

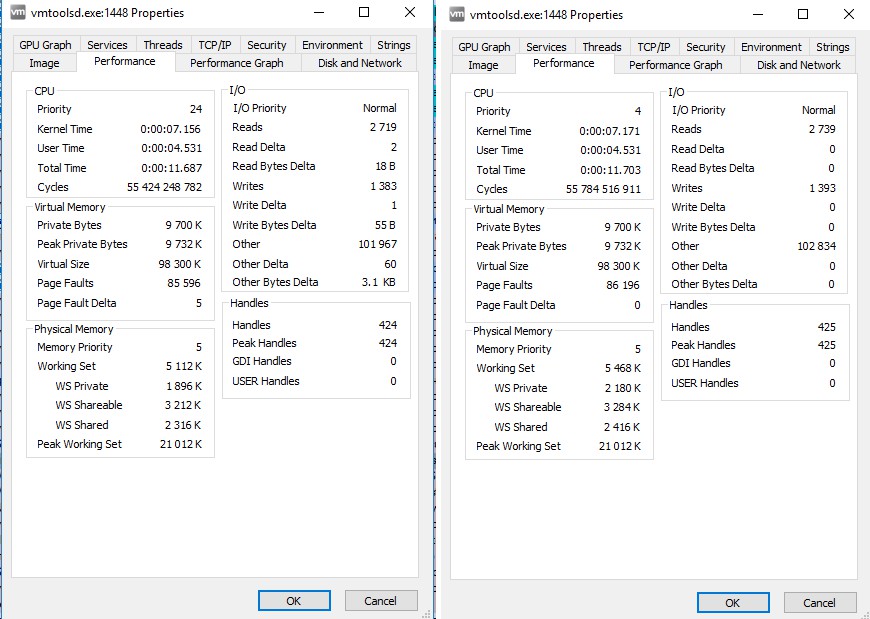


Рисунок 44 – Влияние приоритета на выделяемые ресурсы.

Чтобы просмотреть потоки, исполняемые в рамках процесса, необходимо открыть вкладку потоки в окне свойств процесса. Чтобы просмотреть стек потока процесса, необходимо нажать клавишу «Stack». На рисунках 45 и 46 показаны потоки и стек потока.

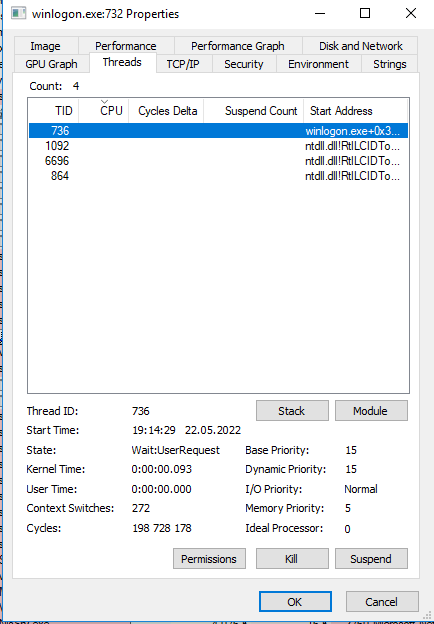


Рисунок 45 – Потоки.

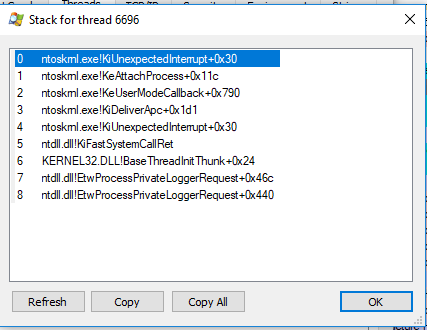


Рисунок 46 – Стек потока.

Запустим «Process Monitor». В главном окне можно отследить действия процессов во время их работы. На рисунке 47 показано главное окно.

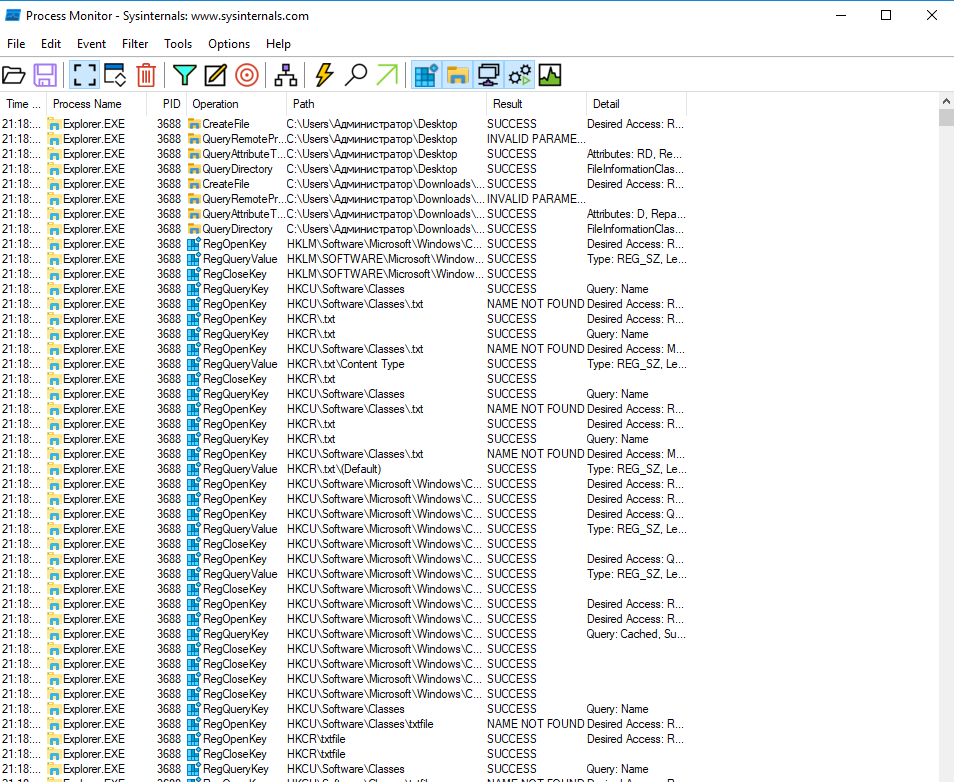


Рисунок 47 – Главное окно Process Monitor.

При помощи меню «Файл – Сохранить» можно сохранить информацию о процессах в журнал. На рисунке 48 показано окно сохранения.

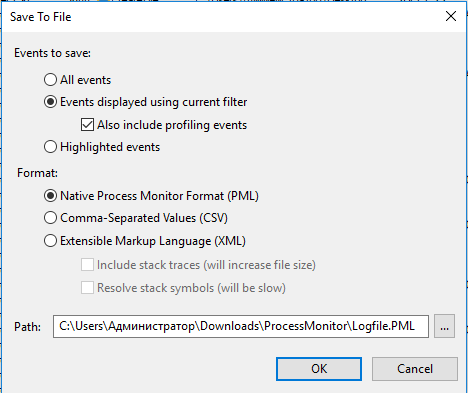


Рисунок 48 – Окно сохранения.

С помощью утилиты Process Monitor можно отследить действия (включая «чтение» и «запись») процесса с файлами, реестром, сетью. Для этого необходимо зайти в меню «Настройки – Выбор колонок» и выбрать колонку «Категория». В результате в колонке «Категория» можно увидеть действия процесса. На рисунке 49 представлен выбор колонок.

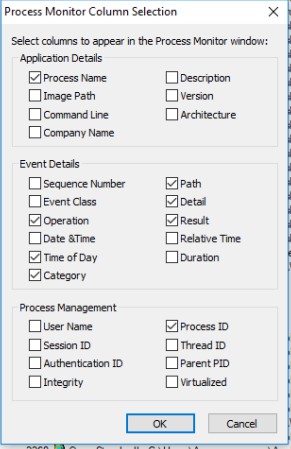


Рисунок 49 – Выбор колонок.

На рисунке 50 представлено отслеживание процесса.

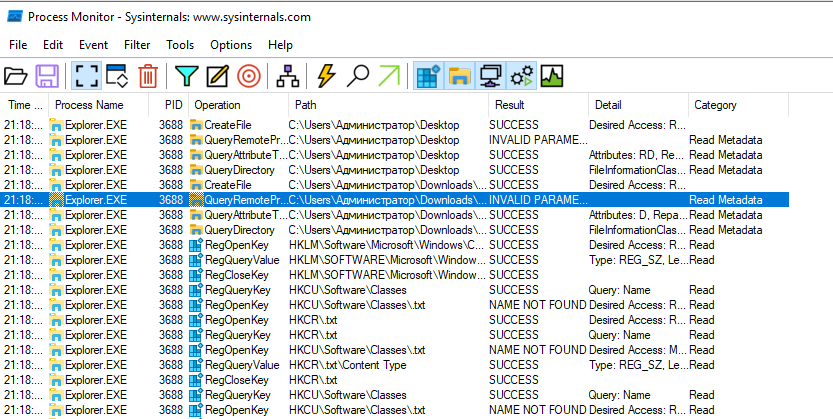


Рисунок 50 – Отслеживание процесса.

Также можно отследить активность процессов при помощи меню

«Инструменты – Лог активных процессов». На рисунке 51 представлена активность процессов.

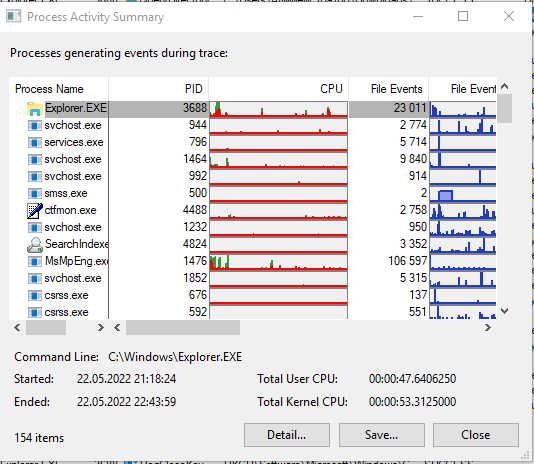


Рисунок 51 – Активность процессов.

Process Monitor предоставляет возможность создавать фильтры, позволяющие делать выборки из журналов. Попасть в меню фильтров можно нажатием сочетания клавиш Ctrl+L. Создадим фильтр, который делает выборку процессов по операции записи в файл. На рисунках 52 и 53 представлено создание фильтра и результат.

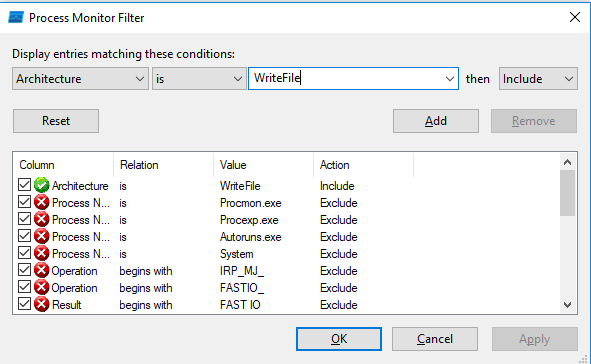


Рисунок 52 – Создание фильтра.



Рисунок 53 – Результат выполнения фильтра.

Также можно отследить работу процессов с файловой системой и реестром при установке программного обеспечения. Рассмотрим данную функцию на примере установки 7-zip. Создадим фильтр, который делает выборку процессов по операции записи в RegCreateFile. На рисунке 54 показан результат поиска.

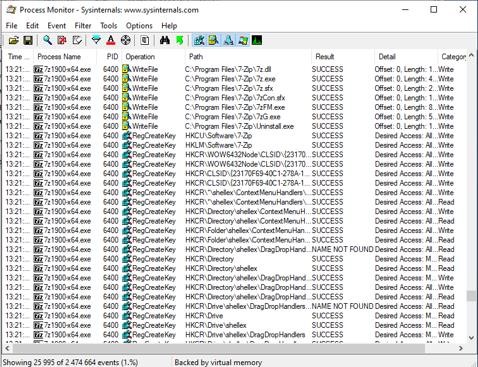


Рисунок 54 – Результат поиска.

* + 1. Задания для лабораторной работы

1. Задать через командную строку перезагрузку компьютера через минуту после первого сбоя.

На рисунке 55 показан результат.



Рисунок 55 – Настройка первого сбоя.

1. Назначить автоматический запуск калькулятора после входа в Windows.

Для выполнения этого задания необходимо в планировщике задач добавить новую задачу. Создание простой задачи и результат представлены на рисунках 56 и 57.

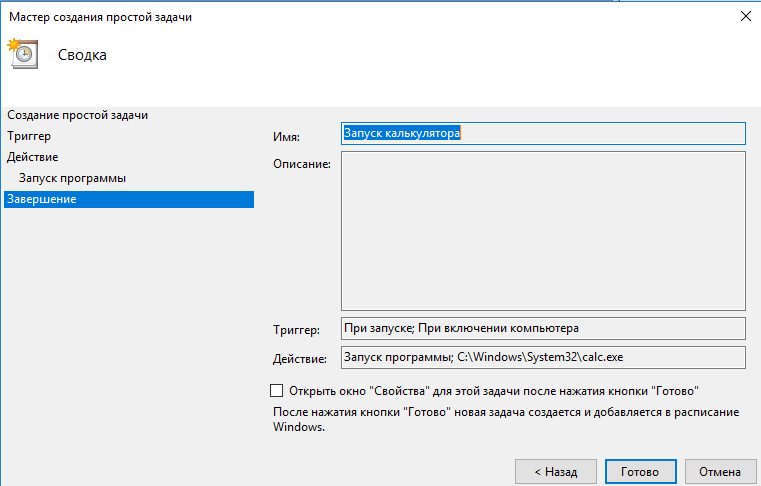


Рисунок 56 – Создание новой простой задачи.

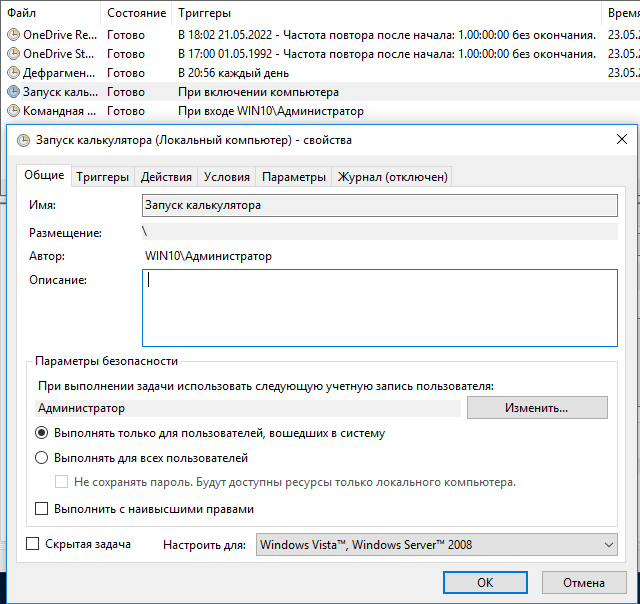


Рисунок 57 – Результат.

1. Заменить стандартный диспетчер задач на Process Explorer.

Для выполнения этого задания необходимо выполнить действия: Options – Replace Task Manager. На рисунке 58 показана замена диспетчера задач.

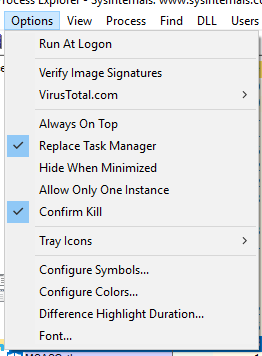


Рисунок 58 – Замена диспетчера задач.

1. Определить какой раздел реестра «Сапер» делает записи о рекордах. На рисунке 59 представлен раздел реестра с записями о рекордах.

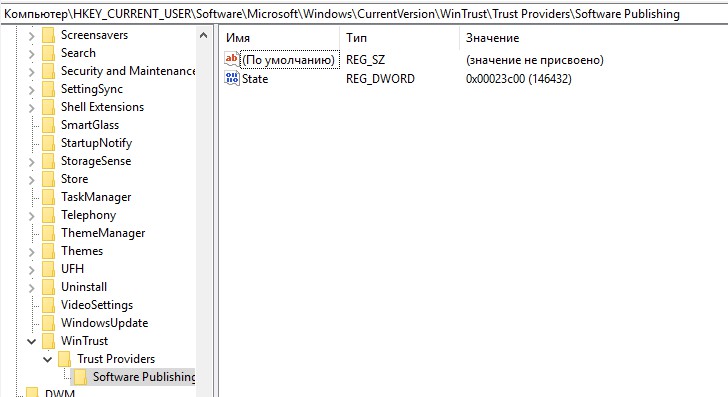


Рисунок 59 – Раздел реестра с записями о рекордах.

1. Вывести информацию о Cookies при работе Internet Explorer.

На рисунке 60 показаны файлы, которые записываются программой

«Internet Explorer».

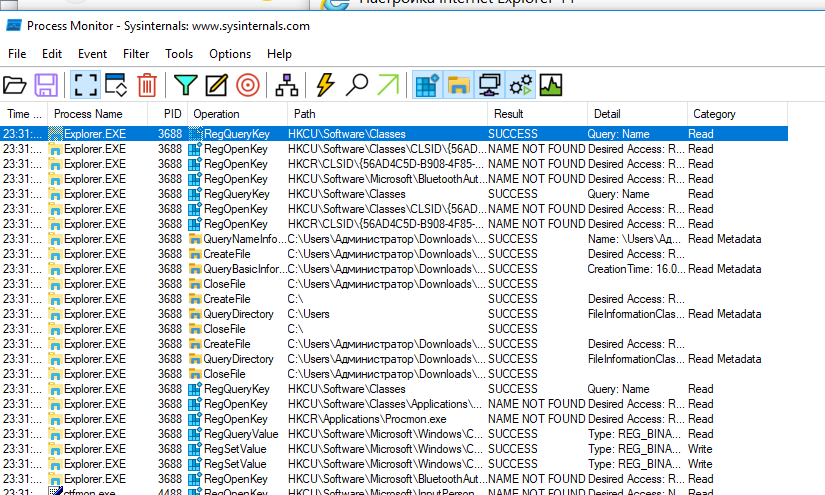


Рисунок 60 – Информация о cookies.

1. Определить какие файлы реестра открывает косынка

На рисунке 61 показаны файлы, которые открывает косынка.

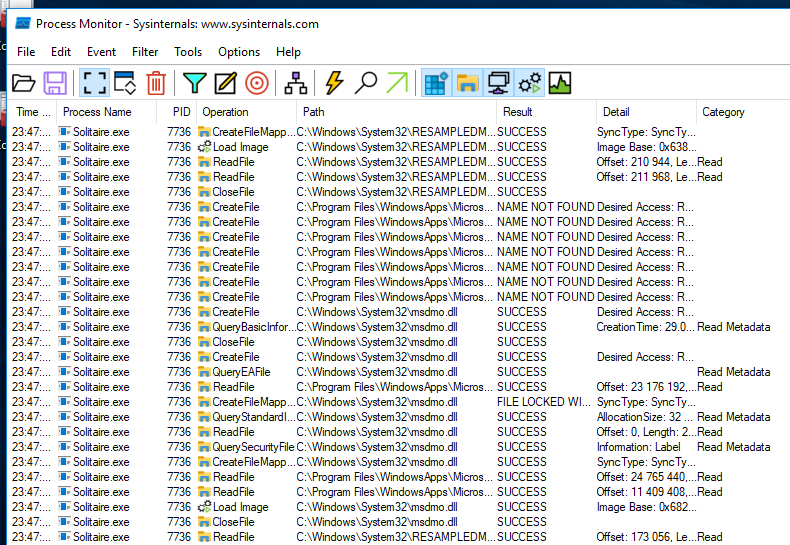


Рисунок 61- Файлы.

1. Определить какие системные файлы читает при работе WMPlayer. На рисунке 62 показаны системные файлы при работе WMPlayer.

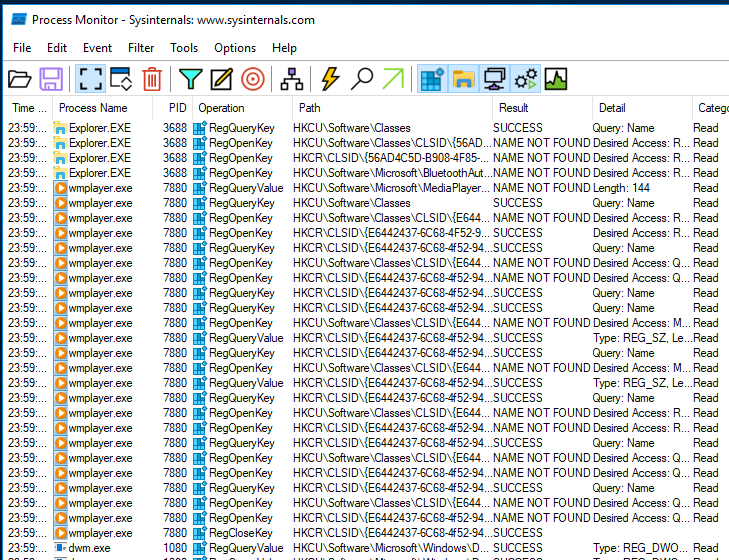


Рисунок 62 - Cистемные файлы при работе WMPlayer.

1. Определить какой процесс запускается при открытии “Установки и удаления программ”.

При открытии «Установка и удаление программ» открывается explorer.exe.

1. Определить в какой файл записываются данные при работе с калькулятором

При работе с калькулятором данные записываются в оперативную память.

Контрольные вопросы

1. Что такое служба Windows?

Служба Windows – программа или процесс, который выполняется в фоновом режиме, т.е. без прямого общения с пользователем, и обеспечивает поддержку других программ

1. Какие средства для управления службами предусмотрены в Windows? Диспетчер задач, оснастка «Службы», управление службами с помощью командной строки.
2. В каких состояниях может находиться служба? Служба может находиться в состояниях Inactive и all.
3. Какие действия могут применяться при сбое службы?

Перезапуск службы, запуск службы, перезагрузка компьютера, не выполнять никаких действий.

1. Правами каких учётных записей может обладать служба при запуске? С системной учетной записью, как локальная служба, как сетевая служба, с правами какого-либо пользователя.
2. Чем отличаются команды для управления службами семейств net и sc? Команда net используется не только для служб, но и для большей части сети, пользователей, входа в систему и т.д. Sc предназначен для служебных команд и превосходит команду net тем, что может запускать отключенные службы.
3. Какие команды используются для изменения состояния и типа запуска служб?

Boot, system, auto, demand, disabled.

1. Чем отличается процесс от потока?

Процесс - это всего лишь способ сгруппировать взаимосвязанные данные и ресурсы, а потоки - единица выполнения, которая распределяется и выполняется на процессоре. Процессы сменяться на процессоре не могут, сменяются и выполняются на процессоре именно потоки.

1. Как с помощью Process Explorer определить, каким процессом открыто определенное окно?

Для этого следует перетащить с панели инструментов Process Explorer кнопку Кнопка в любое место открывшегося окна. После этого в верхней части главного окна Process Explorer будет подсвечено имя искомого процесса.

1. По каким параметрам можно создавать фильтры в Process Monitor? По имени процесса, времени, категории, операции и т.д.

3 Заключение

В ходе данной работы были освоены способы управления службами в OC Windows 10, изучена специфика работы планировщика задач, а также произошло ознакомление со структурой и особенностями работы процессов и потоков в операционных системах, так же выполнены необходимые задания на заданную лабораторную работу.

Отчёт был написан согласно ОС ТУСУР 2013.