ЛАБОРАТОРНАЯ РАБОТА №2 Управление системными службами и процессами Windows

1. Цель работы

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

2. Краткие теоретические сведения

Служба Windows – программа или процесс, который выполняется в фоновом режиме, т.е. без прямого общения с пользователем, и обеспечивает поддержку других программ. Службы могут запускаться при загрузке операционной системы и находиться в оперативной памяти вплоть до завершения работы. Каждая служба имеет определённые характеристики: тип запуска, условия восстановления и другие, которые будут рассмотрены ниже.

Параметры настройки служб хранятся в peecrpe Windows.

Процесс services.exe, запущенный от имени пользователя SYSTEM, отвечает за запуск, остановку и управление службами. Services.exe автоматически запускает службы во время загрузки ОС и останавливает все службы при завершении работы Windows. Другое название этого процесса – диспетчер управления службами (Service control manager, SCM).

Отдельные службы запускаются в процессе svchost.exe, который является дочерним для services.exe. На компьютере может быть запущено несколько экземпляров процесса svchost.exe, при этом каждый из них содержит различные службы. Один экземпляр процесса svchost.exe может содержать одну службу для программы, а другой – несколько служб, относящихся к работе Windows.

Не только система, но и сам пользователь может управлять службами. В Windows предусмотрено управление службами через графический интерфейс и через командную строку, а также при помощи изменения ключей реестра.

3. Ход работы 3.1. Управление службами

Запустите диспетчер задач, нажав Ctrl+Alt+Del. Перейдите на вкладку «Службы» (рис. 1), чтобы увидеть все службы, установленные в операционной системе.

ј∰ Диспетчер задач Файл Параметры Вид				-	U	×
Производительность Жури	нал прилож	ений Автозагрузка Поле	взователи Подр	обности	Служ	••
Имя	ИД п	Описание	Состояние	Группа	a^	
🛱 WSearch	3612	Windows Search	Выполняется			- 1
WMPNetworkSvc		Служба общих сетевы	Остановлено			- 1
🔍 wmiApSrv		Адаптер производител	Остановлено			
WinDefend		Антивирусная програ	Остановлено			
WdNisSvc		Служба проверки сет	Остановлено			
wbengine		Служба модуля архив	Остановлено			
Q, VSS		Теневое копирование	Остановлено			
🔍 vds		Виртуальный диск	Остановлено			
AultSvc	544	Диспетчер учетных да	Выполняется			
G UI0Detect		Обнаружение интерак	Остановлено			
UevAgentService		Служба виртуализаци	Остановлено			
TrustedInstaller		Установщик модулей	Остановлено			
TieringEngineService		Управление уровнями	Остановлено			
🖓 sppsvc		Защита программног	Остановлено			
Spooler	1520	Диспетчер печати	Выполняется			
0 spectrum		Служба восприятия W	Остановлено			
SNMPTRAP		Ловушка SNMP	Остановлено			
SensorDataService		Служба данных датчи	Остановлено			
Sense		Служба Advanced Thr	Остановлено			
SecurityHealthService	1200	Служба Центра безоп	Выполняется			

Рис. 1. Просмотр установленных служб в диспетчере задач

Для каждой службы в диспетчере задач показывается её имя, идентификатор процесса, в рамках которого она запущена (если такой имеется), краткое описание, текущее состояние и группа.

Диспетчер задач позволяет запускать и останавливать службы, если это возможно. Щёлкните правой кнопкой на службе из списка, чтобы увидеть возможные действия (рис. 2).

Запустите и остановите службу Parental Controls (WPCSvc). Приложения, выполняющие функции, аналогичные диспетчеру задач, также зачастую позволяют просматривать, запускать и останавливать службы. Например, эти возможности доступны в Process Explorer.

Оснастка !Службы! – другое средство управления службами, имеющее графический интерфейс, но обладающее большими возможностями, чем диспетчер задач. Оснастка «Службы» представляет собой оснастку консоли ММС.

Оснастку «Службы» можно запустить из диспетчера задач (начиная с Windows 7). Для этого нужно нажать кнопку «Открыть службы» на вкладке «Службы» (рис. 3).

Чтобы запустить оснастку «Службы» из командной строки, нужно выполнить services.msc. Окно оснастки представлено на рис. 4.

WMPNetworkSvc	- i -	Cmarks abuun coronu
🗟 wmiApSrv		Запустить
🔍 WinDefend		Остановить
G WdNisSvc		Перезапустить
kwbengine WSS		Открыть службы
🔍 vds		Поиск в Интернете
🔍 VaultSvc	54	Подробно
Рис. 2. Действия со	службами	и в диспетчере задач

Меньше | 🧠 <u>Открыть службы</u> Рис. 3. Вызов оснастки из диспетчера задач

6 1					
🗼 Службы (локалы	Имя	Описание	Состояние	Тип запуска	Вход от имени
	🖗 BranchCache	Эта служб		Вручную	Сетевая служба
	CoreMessaging	Manages c	Выполняется	Автоматиче	Локальная слу
	Q DevicesFlow_1fcf7	Обнаруже		Вручную	Локальная сис
	Ф. DHCP-клиент	Регистрир	Выполняется	Автоматиче	Локальная слу
	dmwappushsvc	Служба м		Вручную (ак	Локальная сис
	🖏 DNS-клиент	Служба D	Выполняется	Автоматиче	Сетевая служба
	🍓 КtmRm для координатора	Координи	оордини	Вручную (ак Сетев	Сетевая служба
	MessagingService_1fcf7	Служба, о		Вручную (ак	Локальная сис
	Alicrosoft App-V Client	Manages A		Отключена	Локальная сис
	🖏 Office Source Engine	Saves insta		Вручную	Локальная сис
	🖏 Plug and Play	Позволяет	Выполняется	Вручную	Локальная сис
	Reprinter Extensions and Notif	This servic		Вручную	Локальная сис
	Quality Windows Audio Vid	Quality Wi		Вручную	Локальная слу
	Shared PC Account Manager	Manages p		Отключена	Локальная сис
	🤹 SMP дисковых пространст	Служба уз		Вручную	Сетевая служба
	🖏 Superfetch	Поддержи	Выполняется	Автоматиче	Локальная сис
	🖏 TokenBroker	<Не удает	Выполняется	Вручную	Локальная сис
	🖏 Update Orchestrator Service	Управляет		Вручную	Локальная сис
	10 Windows Audio	Vananacu	Purponuncerco	Antoniationo	

Рис. 4. Оснастка «Службы»

Если два раза щёлкнуть левой кнопкой мыши по любой из доступных служб, откроется окно свойств этой службы (рис. 5).

0.000000000	Вход в с	истему	Восстановление	Зависимости	
Имяс	пужбы:	Dhcp			
Отобра имя:	ажаемое	DHCP	клиент		
Описа	ние:	Регистрирует и обновляет IP-адреса и DNS- записи для этого компьютера. Если данная служба остановлена, этот компьютер не сможет получать динамические IP-адреса и			
Испол	няемый ф	айл:			
C:\Win	dows\syst	em32\sv	chost.exe -k LocalS	erviceNetwork Re	stricted
Тип за	пуска:	Автом	атически		~
Состоя	ние:	Выпол	няется		
	устить	Оста	новить Приост	гановить Про	должить
3an		ать пара	аметры запуска, пр	оименяемые при	1 запуске
Зап Вы мо: службы	жете указ ы из этого	диалог	ового окна.		

Рис. 5. Окно свойств службы

Служба может находиться в одном из следующих состояний: работает, приостановлена и остановлена. Соответственно, для службы доступно 4 команды: запустить, остановить, приостановить, продолжить. Эти команды для выбранной службы отображаются в оснастке слева от списка доступных служб (при выборе «расширенного» вида внизу окна), либо в окне свойств выбранной службы на вкладке «Общие». Команды также отображаются, если щёлкнуть правой кнопкой на службе в списке.

Не все службы могут быть приостановлены – некоторые могут быть только запущены и остановлены. Некоторые службы нельзя ни приостановить, ни остановить.

Остановите службу «Windows Audio» и попробуйте запустить звуковой файл. Затем запустите службу и убедитесь, что файл проигрывается.

Служба может зависеть от других служб и при этом могут быть службы, зависящие от неё. Если служба, от которой зависит данная

служба, не запущена, то данная служба может работать некорректно или вообще не запуститься.

Одна служба может иметь несколько зависимых служб. Также сама служба может быть зависима от нескольких служб. Службы могут зависеть не только от других служб, но и от некоторых драйверов. Зависимые службы можно просмотреть на вкладке «Зависимости» окна свойств службы (рис. 6).

Некотор или спис неправи службах Рабочая Данная	ые службы зави жа загрузки гру пьно работает, з станция служба зависит Драйвер подде; Мини-реренапра	исят от других служ пп служб. Если ко это может отразит от следующих ком	кб, системных драй мпонент остановле ься на зависимых о понентов:	веров н или эт нее
Рабочая Данная Народанная	станция служба зависит Драйвер подде; Мини-перенапо	от следующих ком	понентов:	
Данная	служба зависит Драйвер поддер Мини-перенапра	от следующих ком ожки браузера	понентов:	
	Драйвер поддер Мини-деренарр;	ожки браузера		
E. Chi	Служба интерфе	авитель SMB 2.0 ейса сохранения с	ети	
Следуюц	цие компоненты Браузер компьн Настройка сере Сетевой вход в	зависят от данной отеров зера удаленных раб систему	й службы: бочих столов	

Рис. 6. Просмотр зависимостей службы

Остановите службу «Система событий СОМ+», которая имеет зависимую службу «Служба уведомления о системных событиях». Система выведет предупреждение о том, что зависимые службы будут также остановлены (рис. 7).



Рис. 7. Попытка остановить службу с зависимостями

Каждая служба может иметь один из следующих типов запуска: – автоматически: служба запускается при загрузке Windows;

- вручную: служба запускается пользователем в оснастке «Службы» или любым другим способом;

– отключена: служба не может быть запущена, пока тип запуска не будет сменён на другой.

Кроме того, имеются также два дополнительных типа запуска: первый – запуск на этапе загрузке ядра Windows (низкоуровневые драйверы), второй – запуск сразу после инициализации ядра. Для таких служб сменить тип запуска в оснастке нельзя (например, служба «Удалённый вызов процедур»).

Примечание: начиная с Windows Vista, у служб присутствует ещё один тип запуска – «Автоматически (отложено)». Он аналогичен типу «Автоматически», но запускает службу через некоторое время после загрузки для оптимизации запуска Windows.

Тип запуска можно сменить на вкладке «Общие» окна свойств службы. Для службы «Темы» установите тип запуска «Вручную», перезагрузите компьютер и убедитесь, что окна Windows имеют «классический» вид, так как служба не запущена.

Если работа службы была некорректно завершена, Windows может перезапустить её или выполнить другие действия. Настройка параметров восстановления находится на вкладке «Восстановление» окна свойств службы (рис. 8).

Јощие	Вход в систему	Восста	новление	Зависимости	
Дейст настро	вие компьютера, в ойке действий по в	зыполня зосстани	аемое при о овлению	сбое службы. Помощь пр	
Первь	ій сбой:	Пе	Перезапуск службы		
Второ	й сбой:	Пе	резапуск с	лужбы	
После	дующие сбои:	He	выполнять	» никаких действий	
Сброс	счетчика ошибок ч	через:	1	дн.	
Перез	апуск службы чере	es:	2	мин.	
🗌 Вкл	ючить действия д	ля остан	новок с ош	— ибками.	
			П	араметры перезагрузки	
Вып	олнение программ	ы			
Про	грамма;				
				Обзор	
Dec		vi orteorie	ard I		
110	аметры команцно	и строк	и.		
				ик оцийбок (/fail=%1%)	
	Дописать в коман,	дную ст	року счетчи	in omnoon frain- is they	

Рис. 8. Параметры восстановления службы

Можно задать действия, которые будут выполняться при первом, втором и последующих сбоях службы. Среди доступных действий:

– перезапуск службы: перезапускает службу через указанное время после сбоя;

 запуск программы: запускает выбранную ниже программу с заданными параметрами командной строки. Можно включить в параметры командной строки номер очередного сбоя службы;

 перезагрузка компьютера: перезагружает компьютер немедленно или по истечении заданного времени. При этом можно вывести на экран сообщение о неминуемой перезагрузке;

– не выполнять никаких действий: никакие действия после сбоя выполнены не будут.

Некоторые службы, например «Plug'n'play», не поддерживают параметры восстановления. Обычно при сбое этих служб компьютер перезагружается.

Установите параметры восстановления для службы «Диспетчер печати» («Диспетчер очереди печати») следующим образом: при первом сбое служба должна мгновенно перезапускаться, при втором – перезагружать компьютер с выводом сообщения через 2 минуты.

Завершите процесс spoolsv.exe, в котором запущена эта служба. Убедитесь, что процесс тут же запускается снова. Завершите процесс второй раз и убедитесь, что Windows выводит сообщение о неминуемой перезагрузке и через 2 минуты компьютер перезагружается.

Каждая служба имеет определённые права при запуске. Служба может запускаться:

- с системной учётной записью;

- как локальная служба;
- как сетевая служба;

- с правами какого-либо пользователя.

Права службы можно сменить на вкладке «Вход в систему» окна свойств службы (рис. 9).

Ортив	Вход в систему	Восстановление	Зависимости	
Входв	систему:			
ОСси	стемной учетной	і записью		
F	азрешить взаим	юдействие с рабочі	им столом	
		75		12/2
C y4	етной записью:	Сетевая служба		Обзор
⊚Суч –	етной записью:	Сетевая служба		Обзор
⊚Суч Пар	етной записью: оль:	Сетевая служба	••	Обзор

Рис. 9. Права службы при входе в систему

Чтобы выбрать вход с системной учётной записью, выберите соответствующий вариант вверху окна. Для выбора локальной службы нужно ввести в качестве имени пользователя «NT AUTHORITY / LocalService» («Локальная служба» в Windows Vista и 7) без кавычек, а пароль не вводить.

Для выбора сетевой службы – «NT AUTHORITY/NetworkService» («Сетевая служба» в Windows Vista и 7) и пароль так же не вводить.

Для работы со службами из командной строки предусмотрены команды семейств net и sc. Семейство net в основном используется для

других целей и имеет базовые команды работы со службами. Семейство sc, введённое в Windows XP, целиком посвящено работе со службами.

Запустите командную строку, выбрав «Пуск > Выполнить» и набрав cmd.

Для просмотра запущенных на данный момент служб введите команду net start. Обратите внимание, что она выводит список отображаемых имён служб, а не сами имена служб (рис. 10).





Рис. 10. Выполнение команды net start

Чтобы запустить службу, введите команду net start с последующим именем службы. Запустите службу SysmonLog (pla начиная с Windows 7) – «Журналы и оповещения производительности» (рис. 11).



Если служба имеет тип запуска «Отключена» или уже запущена, об этом будет выведено соответствующее сообщение.

Для остановки службы используется команда net stop с последующим именем службы. Если служба не запущена или не может быть остановлена, об этом будет выведено сообщение. Остановите службу MpsSvc – «Брандмауэр Windows». Зайдите в панель управления и убедитесь, что брандмауэр Windows отключен.

Команды семейства net не позволяют, например, выводить все установленные в системе службы. Для этого используются команды семейства sc.

Семейство sc позволяет просматривать и изменять подробную информацию о каждой службе, а также регистрировать в системе новые службы и удалять установленные. Если ввести sc без параметров, можно просмотреть справку по этому семейству. То же самое относится к большинству команд этого семейства.

Для вывода списка служб используются команды sc query и sc queryex. Первая команда выводит такие данные о службе, как имя (SERVICE_NAME), отображаемое имя (DISPLAY_NAME), состояние (STATE) и другие данные, не рассматриваемые в данной работе. Вторая команда дополнительно выводит идентификатор процесса (PID), в рам-ках которого запущена служба (рис. 12).

C:\Users\Администратор>sc c	jueryex
Имя службы: AudioEndpointBu	ilder
Выводимое имя: Средство пос	троения конечных точек Windows Audio
Тип	: 20 WIN32 SHARE PROCESS
Состояние	: 4 RUNNING
	(STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
Код_выхода_Win32	: 0 (0x0)
Код_выхода_службы	: 0 (0x0)
Контрольная_точка	: 0x0
Ожидание	: 0x0
ID_процесса	: 8
Флаги	

Рис. 12. Команды sc query и sc queryex

Команды позволяют использовать фильтр для вывода списка служб. Фильтр задаётся в виде параметров, введённых после команды. Среди параметров:

– type: имеет значение driver (драйвер), service (служба), interact (интерактивная служба, которая обменивается информацией с пользователем) или all (и то, и другое). По умолчанию – service;

 – state: имеет значение inactive (незапущенные службы) или all (и запущенные, и остановленные службы). Если параметр не задан, он принимается равным значению active (запущенные службы).

Таким образом, чтобы, например, вывести список незапущенных служб драйверов, нужно ввести команду sc query type= all state= inactive.

Соответственно, если не задано никаких параметров, выводятся все запущенные службы.

Если после команды sc query или sc queryex ввести имя службы, будет выведена информация только об этой службе.

Выведите список всех установленных интерактивных служб. Затем выведите расширенную информацию об одной из запущенных служб из этого списка.

Кроме перечисленных команд, для вывода информации о конкретной службе используются также команды sc qc, sc qdescription, sc qfailure и другие. После команды пишется имя соответствующей службы (рис. 13).

C:\Users\Администр [SC] QueryService(атор>sc qc Spoole Config: ycnex	r
Имя службы: Spoole	۱ ۲	
Тип Тип_запусл Управление Имя_двоичн Группа_зап Тег Выводимое_ Зависимост	. : 110 а : 2 _ошибками : 1 юго_файла : С:\W юска : Spoo : 0 .имя : Дисп и : RPCS	WIN32_OWN_PROCESS (interactive) AUTO_START NORMAL lindows/System32\spoolsv.exe ergroup erчeр печати is
Начальное	: http имя службы : Loca	- JSystem
C:\Users\Администр [SC] QueryService(arop≻sc qdescript config2: ycnex	ion Spooler
Имя_службы: Spoole Описание: Эта слу ствие с принтером. ры.	р жба позволяет ста Если ее отключит	вить задания печати в очередь и обеспечивает взаимодей ъ, вы не сможете выполнять печать и видеть свои принте
C:\Users\Администр [SC] QueryService(атор>sc qfailure Config2: успех	Spooler
Имя_службы: Spool€ Период_сбр Сообщение_ Командная_ Лайстрия г	ег юса (в секундах) при_перезагрузке строка пом сбое	: 3600 : : : перезалиск залелика - 5000 мс
PI	с 13 Команлы	просмотра информации о службах

Рис. 13. Команды просмотра информации о службах

sc qc выводит такую информацию: тип запуска службы (START TYPE), имя исполняемого файла (BINARY PATH NAME), отображаемое имя (DISPLAY NAME), зависимости (DEPENDENCIES) и имя учётной записи, правами которой обладает служба при запуске (или начальное имя службы, SERVICE START NAME).

sc qdescription выводит описание службы (DESCRIPTION).

sc qfailure выводит действия при сбое службы (FAILURE ACTIONS), период сброса счётчика сбоев в секундах (RESET_PERIOD), сообщение при неминуемой перезагрузке (REBOOT_MESSAGE) и путь к файлу программы для запуска (COMMAND_LINE).

Кроме того, можно вывести список служб, зависящих от данной службы. Для этого используется команда sc enumdepend.

Выведите информацию с помощью этих команд о службе CryptSvc – «Службы криптографии».

Для изменения состояния службы используются следующие команды:

- sc start: запуск службы;

- sc pause: приостановка службы, если возможно;

- sc continue: продолжение работы службы, если она была приостановлена;

- 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. Эта команда также позволяет, в частности, изменять имя учётной записи для службы, отображаемое имя, путь к исполняемому файлу и даже зависимости, что недоступно в диспетчере управления службами.

Для изменения типа запуска используется параметр start. Его значения:

- boot: запуск при инициализации ядра Windows;

- system: запуск сразу после инициализации ядра Windows;

- auto: запуск сразу после загрузки Windows (соответствует типу «Автоматически» в диспетчере управления службами);

- demand: запуск по требованию пользователя (соответствует типу «Вручную» в диспетчере управления службами);

- disabled: служба отключена (соответствует типу «Отключена» в диспетчере управления службами).

Примечание: для Windows Vista и выше, типу «Автоматически (отложено)» соответствует значение параметра delayed-auto.

Примечание: как и в оснастке «Службы», первые два типа запуска изменять не допускается.

Таким образом, чтобы, например, установить службе «DNSклиент» тип запуска «Вручную», нужно ввести sc config Dnscache start= demand.

С помощью этой команды измените тип запуска службы Themes – «Темы» на «Автоматически». Перезагрузите компьютер и убедитесь, что окна Windows имеют обычный вид.

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

– 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:

– run: запуск программы. При использовании этого значения должен быть задан параметр command;

- reboot: перезагрузка компьютера. Используется совместно с параметром reboot;

– restart: перезапуск службы.

Чтобы при сбое не выполнялось никаких действий, просто не вводите следующее действие и его задержку.

К примеру, если службу при первом и втором сбое нужно перезапустить через 2 секунды, а при следующих сбоях – перезагрузить компьютер через 30 секунд, значение параметра actions будет равно restart/2000/restart/2000/reboot/30000;

- reset: продолжительность периода (в секундах), после которого счётчик сбоев сбрасывается. Если значение равно INFINITE, счётчик никогда не сбрасывается;

- reboot: сообщение, выводимое перед перезагрузкой;

- command: путь и параметры командной строки для файла запускаемой при сбое программы.

Для службы Spooler установите следующие параметры восстановления: при первом сбое служба должна перезапуститься через 5 секунд, при втором

- через 10 секунд, при третьем – компьютер должен перезагрузиться через 20 секунд с выводом соответствующего сообщения. Счётчик сбоев должен быть сброшен через 1 час.

Завершите процесс spoolsv.exe три раза, чтобы убедиться в правильности введённой команды.

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. Откройте оснастку «Службы». Остановите с помощью sc stop службу TapiSrv – «Телефония», а затем обновите её состояние в оснастке с помощью sc interrogate и убедитесь в том, что в оснастке её состояние показывается правильно.

Для регистрации новой службы в реестре используется команда 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.

Создайте новую службу, выбрав в качестве исполняемого файла Notepad.exe (блокнот) (рис. 14). Задайте ему автоматический тип запуска и произвольное отображаемое имя. Пусть служба обладает правами пользователя «Система» (LocalSystem).

C:\U	sers\Администратор>sc	creat	e Notepad	binPath=(:\Windows\	notepad.exe	start=
auto	DisplayName= Блокност	obj=	LocalSys	tem			
[SC]	CreateService: ycnex						

Рис. 14. Создание новой службы

Откройте оснастку «Службы» и убедитесь, что созданная служба отображается в списке.

Примечание: не пытайтесь запустить созданную службу. Она не отвечает требованиям, предъявляемым к службам, и приведена только в качестве примера.

Чтобы удалить службу, используется команда sc delete с последующим именем службы. Если служба запушена или используется другим процессом, она будет помечена для удаления и удалена позже.

Удалите только что созданную службу. Перейдите в оснастку «Службы», выберите «Действие > Обновить» и убедитесь, что служба в списке отсутствует.

Приведём описание некоторых системных служб Windows:

– DHCP-клиент: управляет конфигурацией сети посредством регистрации и обновления IP-адресов и DNS-имен.

– DNS-клиент: разрешает для данного компьютера DNS-имена в адреса и помещает их в кэш. Если служба остановлена, не удастся разрешить DNS-имена и разместить службу каталогов Active Directory контроллеров домена.

– Plug'n'play: позволяет компьютеру распознавать изменения в установленном оборудовании и подстраиваться под них, либо не требуя вмешательства пользователя, либо сводя его к минимуму.



– Windows audio: управление звуковыми устройствами для Windows-программ.

– Автоматическое обновление: загрузка и установка обновлений Windows. Если служба отключена, то на этом компьютере нельзя будет использовать возможности автоматического обновления или веб-узел Windows Update.

- Веб-клиент: позволяет Windows-программам создавать, получать доступ и изменять файлы, хранящиеся в Интернете.

– Диспетчер логических дисков: обнаружение и наблюдение за новыми жесткими дисками и передача информации о томах жестких дисков службе управления диспетчера логических дисков.

– Журнал событий: обеспечивает поддержку сообщений журналов событий, выдаваемых Windows-программами и компонентами системы, и просмотр этих сообщений.

– Обозреватель компьютеров/браузер компьютеров: обслуживает список компьютеров в сети и выдает его программам по запросу.

– Планировщик заданий: позволяет настраивать расписание автоматического выполнения задач на компьютере.

– Поставщик поддержки безопасности NT LM: аутентификация на серверах NT и доступ к ресурсам домена.

– Рабочая станция: обеспечивает поддержку сетевых подключений и связь. Если служба остановлена, программа, данные подключения будут недоступны.

– Сервер: обеспечивает поддержку общий доступ к файлам, принтерам и именованным каналам для данного компьютера через сетевое подключение.

- Сетевые подключения: управляет объектами папки «Сеть и удаленный доступ к сети», отображающей свойства локальной сети и подключений удаленного доступа.

– Служба восстановления системы: выполняет функции восстановления системы.

– Службы криптографии: предоставляет три службы управления: службу баз данных каталога, которая проверяет цифровые подписи файлов Windows; службу защищенного корня, которая добавляет и удаляет сертификаты доверенного корня центра сертификации с этого компьютера; и службу ключей, которая позволяет подавать заявки на сертификаты с этого компьютера. Начиная с Windows Vista, предоставляет также четвёртую службу: службу автоматического обновления корневых сертификатов, которая получает корневые сертификаты из центра обновления Windows и разрешает сценарии, такие как SSL.

 – Теневое копирование тома: управляет созданием теневых копий (контрольных точек состояния) дисковых томов, которые используются для архивации и восстановления или для иных целей.

– Удалённый вызов процедур: выполняет запросы активации объектов, разрешение экспортера объектов и распределенный сбор мусора для серверов СОМ и DCOM.

– Управление приложениями: обеспечивает службы установки программного обеспечения, такие как назначение, публикация и удаление.

– Центр обеспечения безопасности: ведет наблюдение за настройками и параметрами безопасности системы.

3.2. Автоматизация выполнения административных задач

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

Планировщик заданий содержит библиотеку всех назначенных заданий, обеспечивая возможность быстрого просмотра и удобного управления заданиями. Из библиотеки можно запустить, отключить, изменить и удалить задание.

Для того чтобы запустить планировщик задач, необходимо проверить, включена ли данная служба, как показано на рис. 15.

Службы Файл Действие В С С С С С С С С С С С С С С С С С С С	Вид Справка				
Службы (локалы	Имя Диспетчер печати Определение оборудован Служба уведомления о си Служба центра безопасно	Описание Эта служб Предостав Ведет наб Служба Ц	Состояние Выполняется Выполняется Выполняется Выполняется	Тип запуска Автоматиче Автоматиче Автоматиче Автоматиче	Вход от имені Локальная си Локальная си Локальная си Локальная си
	 Планировщик заданий Диспетчер учетных записе Удаленный вызов процеду Сопоставитель конечных Сопоставитель конечных Служба профилей пользо Питание 	Позволяет Запуск это Служба R Обеспечи Эта служб Управляет	Выполняется Выполняется Выполняется Выполняется Выполняется Выполняется	Автоматиче Автоматиче Автоматиче Автоматиче Автоматиче Автоматиче	Локальная си Локальная си Сетевая служ Сетевая служ Локальная си Локальная си

Рис. 15. Службы

Если служба Планировщик задач не включена, нужно вызвать контекстное меню, кликнув правой кнопкой мыши на данную службу и выбрать Свойства. Во вкладке Общее, если в поле Состояние стоит статус «Работает», значит служба планировщик задач запущена. Если нет, необходимо нажать кнопку «Запустить», тип запуска выбрать «Автоматически» и сохранить настройки (рис. 16).

Общие	Вход в с	истему	Восстановление	Зависимо	сти			
Имя с.	пужбы:	Sched	ule					
Отобр имя:	ажаемое	Планировщик заданий						
Описание:		Позволяет настраивать расписание автоматического выполнения задач на этом компьютере. Данная служба также отвечает за выполнение нескольких критически важных						
Испол	няемый ф	айл:						
C:\Win	idows\syst	em32\sv	chost.exe +k netsvc	5				
Тип за	пуска:	Автоматически 🗸						
Состоя	ание:	Выпол	няется					
	устить	Оста	новить Приост	гановить	Продолжит	ь		
Заг	Construction of the							

После того, как служба запущена и тип запуска автоматический, служба будет стартовать при загрузке системы, и задания будут выполняться в соответствии с выбранным расписанием.



Рис. 17. Добавление оснастки

Чтобы создать задачу, потребуется сперва вызвать консоль управления ММС и добавить в нее оснастку «Планировщик заданий» (рис. 17). После чего в меню действий к данной оснастке выбрать пункт «Создать задачу...» или «Создать простую задачу...» (рис. 18).

🚟 Файл Действие Вид Избранное 🛙	Окно Справка
* • # 🖬 🖬 🖬	
🔛 Корень консоли	Сводка планировщика заданий (Последнее о
 Планировщик заданий (Локальный) Библиотека планировщика задан Мicrosoft 	Подключиться к другому компьютеру Создать простую задачу
in a substance of the s	Создать задачу
	Импортировать задачу
	Отображать все выполняемые задачи
	Включить журнал всех заданий

Рис. 18. Добавить задание

В случае выбора создания простой задачи – будет запущен «Мастер создания простой задачи», в котором по шагам будет предложено создать необходимое задание. Создайте задачу по запуску командной строки. Для удобства работы с создаваемыми задачами – каждой из них присваивается имя (рис. 19).

Мастер создания простой задачи		×
Оздать простую задачу		
Создание простой задачи Триггер	Этот мастер дополнител используйт	о используется для быстрого планирования обычных задач. Для выбора пьных возможностей, таких как многозадачные действия или триггеры, • команди, "Создать задачу" в области "Действия".
Действие Завершение	<u>И</u> мя:	Командная строка
	<u>О</u> писание:	
		< <u>Назад</u> алее > Отмена

Рис. 19. Задание имени задаче

Мастер предложить указать период запуска этого задания. Возможны следующие варианты периода запуска задания:

 – Ежедневно. Задание будет запускаться ежедневно, либо только по рабочим дням или через несколько дней в указанное время.
 48 – Еженедельно. Указывается, каждую ли неделю нужно запускать задание и выбирать дни недели, по которым задание будет запущено в определенное время.

– Ежемесячно. В какие месяцы года надо запускать задание и выбирать по каким числам месяца, либо по каким дням месяца в определенное время будет запущено задание.

– Однократно. Можно выбрать дату и время запуска задания. Больше это задание выполняться не будет.

– При загрузке компьютера. При таком типе запуска задание будет выполняться каждый раз при загрузке компьютера. Данный тип запуска не требует входа пользователя.

– При входе в Windows. Этот тип запуска похож на предыдущий с тем отличием, что задание будет выполнено только когда пользователь войдет в Windows, то есть введет свои логин и пароль.

Выберите «При входе в Windows» и нажмите «Далее» (рис. 20).

Мастер создания простой задачи					
Создание простой задачи	Когда вы хотите запускать задачу?				
Триггер	💭 Ежедневно				
Действие Завершение	🔘 Еженедельно				
	О Ежемесячно				
	🔘 Однократно				
	🔘 При запуске компьютера				
	При входе в Windows				
	При занесении в журнал указанного события				
	< Назад				

Рис. 20. Задание триггера запуска

Затем будет предложено выбрать действие, выполняемое задачей. Выберите «Запуск программы» (рис. 21). Будет предложено через «Проводник» указать файл программы, который будет необходимо запустить. Выберите из списка Командную строку (C:\Windows\System32\cmd.exe) и нажмите «Далее» (рис. 22).

Мастер создания простой задачи	
Создание простой задачи Григгер Действие	Выберите действие для задачи
Завершение	 Запустить программу Отправить сообщение электронной почты (не рекомендуется)
	О Вывести сообщение (не рекомендуется)

Рис. 21. Выбор действия

Мастер создания простой задачи		
Запуск программы		
Создание простой задачи		
Триггер	<u>П</u> рограмма или сценарий:	
Действие	C:\Windows\System32\cmd.exe	Обзор
Запуск программы Завершение	Добавить <u>а</u> ргументы (необязательно):	
	<u>Р</u> абочая папка (необязательно):	
	< <u>Н</u> азад Дале	ее > Отмена

Рис. 22. Выбор программы для запуска

После проделанных действий «Мастер создания простой задачи» предоставит информацию по заданной задаче. Убедитесь, что все соответствует выбранным параметрам и нажмите «Готово» (рис. 23).

В библиотеке планировщика заданий появится новая задача с указанным Вами именем. Выделите задачу правой кнопкой и в меню действий (рис. 24) выберите пункт «Выполнить». Убедитесь, что задача осуществляется, после чего откройте ее свойства (рис. 25).

Ознакомьтесь с содержимым вкладок свойств созданной задачи. После чего запустите через меню действий планировщика «Создать задачу...». В данном формате создания задачи – мастер отличается от меню свойств созданной задачи только отсутствием вкладки «Журнал». Создайте через данный мастер задачу по запуску «Блокнота».

Мастер создания простой задачи					>
Создание простой задачи		V			
Триггер	Имя:	командная строка			
Действие	Описание:				
Завершение					
	Триггер:	При входе в систему; Пр	ои входе WIN-BM43746	5MJJV\Админи	стратор
	Действие:	Запуск программы; С:\\	Windows\System32\cn	nd.exe	
	🗌 Открыть После наж. Windows.	окно "Свойства" для этой этия кнопки "Готово" нова	й задачи после нажаті ая задача создается и	ия кнопки "Гот добавляется в	ово" расписание
			< Назад	Готово	Отмена

Рис. 23. Завершение работы мастера создания простой задачи

Файл	Состояние	Триггеры
(B) AAct	Готово	В 8:00 каждые 2 дн.
🕒 OneDrive St	Готово	В 4:00 01.05.1992 - Частота повтора і
🕒 OneDrive St	Готово	В 4:00 01.05.1992 - Частота повтора і
🕒 OneDrive St	Готово	В 4:00 01.05.1992 - Частота повтора і
🕒 Командная	Готово	При Выполнить
<		Завершить
Действия Усло	вия Параме	етры Экспортировать
Действие Запуск програм	Подроб мы C:\Wind	бност Свойства dows [\] Удалить

Рис. 24. Выбор действий с созданной задачей.

Добавьте в планировщик заданий Дефрагментацию диска. Для этого в Мастере планирования задания необходимо нажать Обзор и выбрать программу Defrag.exe, находящуюся в каталоге C:\Windows\System32\Defrag.exe (рис. 27). Выберите ежедневное выполнение задания.

) Коман	ідная строка	а (Локальнь	ій компью	тер) - свойств	a			>
Общие	Триггеры	Действия	Условия	Параметры	Журнал (откл	пючен)		
Имя:		Командна	я строка					
Размеш	цение:	N N						
Автор:		WIN-BM4	3746MJJV	Администрато	p			
Описан	ие:							
Парам	іетры безоп	асности						
При в	ыполнении	задачи исп	ользовать	следующую у	четную запись	о пользователя:		
Адми	нистратор						Изменить	
🖲 Вы	полнять тол	тько для по.	пьзователе	ей, вошедших	в систему			
⊖ Вы	полнять для	я всех польз	ователей					
12	Не сохраня	ть пароль.	Будут дост	упны ресурсы	только локал	ьного компьют	epa.	
🗌 Вы	полнить с н	аивысшим	и правами					
Скры	ытая задача	Настр	оить для:	Windows Vist	a™, Windows S	erver™ 2008		~
								1

Рис. 25. Свойства задачи

Общие	Триггеры	Лействия Условия	Параметры	
14	(principle)		, inspanie, par	
кімя:		L		
Размеь	цение:	1		
Автор:		WIN-BM43746MJJV	\Администратор	
Описан	ние:			
Парам	иетры безоп	асности		
Прин	выполнении	задачи использовать	ь следующую учетную запись пользо	ователя:
WIN-	BM43746MJJ	√Администратор		Изменить
🖲 Вь	полнять тол	ько для пользовател	ей, вошедших в систему	
О Вь	полнять для	всех пользователей		
1000	Не сохраня	ть пароль. Будут дос	тупны ресурсы только локального ко	омпьютера.
122	1	1		
		313 P C P F F F F F F F F F F F F F F F F F	и	
Вь	полнить с н	аивысшими правамі		

Рис. 26. Общие параметры создаваемой задачи



Укажите де	иствие для данной задачи.		
Действие:	Запуск программы		
Параметр	ы		
Програм	іма или сценарий:		
C:\Wind	ows\System32\Defrag.exe		Обзор
	ь аргументы (необязательно):		
Добавит			
Добавит Рабочая	папка (необязательно):	<u> </u>	

Рис. 27. Мастер планирования заданий

Ошибки при создании задачи, которые приводят к незапуску задачи в указанное время – неправильно введенный пароль, либо пароль не введен вообще. Путь к программе или скрипту, которые запускаются задачей, указан неправильно. Если в пути к запускаемой программе или скрипту есть пробелы, то путь должен быть заключен в кавычки. Еще необходимо проверить статус службы планировщика. Он должен быть запущен и режим запуска службы планировщик заданий должен быть «Авто».

3.3. Работа с процессами и потоками

Запустите «Process Explorer» (файл procexp.exe). В главном окне перечислены все работающие в системе процессы, представленные в виде древовидной структуры (рис. 28).

Двойной щелчок по имени процесса открывает окно его свойств (рис. 29). Свойства процесса предоставляют информацию о работе выбранного 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.

File Options View Process Fir	nd User	rs Help					_
	XM				A.		
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	
System Idle Process	77.25	24 K	4 K	0			
🖃 🔳 System	0.73	48 K	52 K	4	A REAL PLAN AND AND A REAL PLAN AND A		_
Interrupts	1.12	0 K	0 K	n/a	Hardware Interrupts and DPCs		
smss.exe		320 K	852 K	288			
Memory Compression	< 0.01	124 K	37 620 K	2004			
Csrss.exe		924 K	3 756 K	380			
🗉 🔳 wininit.exe		1 052 K	5 276 K	460			
🖃 🔳 services.exe	0.01	2 568 K	6 228 K	572			
svchost.exe	0.80	6 624 K	17 408 K	680	Хост-процесс для служб	Microsoft Corporation	
ShellExperienceHost	Susp	31 788 K	49 624 K	3584	Windows Shell Experience H	Microsoft Corporation	
SearchUI.exe	Susp	53 804 K	71 076 K	3616	Search and Cortana applicati	Microsoft Corporation	
RuntimeBroker.exe	0.04	9 412 K	21 516 K	4032	Runtime Broker	Microsoft Corporation	1
backgroundTaskHost	0.05	4 216 K	21 192 K	1620	Background Task Host	Microsoft Corporation	
backgroundTaskHost	0.19	7 860 K	22 684 K	2772	Background Task Host	Microsoft Corporation	
SkypeHost.exe	Susp	3 624 K	16 144 K	2936	Microsoft Skype Preview	Microsoft Corporation	ł
smartscreen.exe	0.0000000000	7 520 K	15 064 K	3264	SmartScreen	Microsoft Corporation	7
WmiPrvSE.exe		3 052 K	9 168 K	4480			
svchost exe	0.74	3 040 K	8 012 K	760	Хост-процесс для служб	Microsoft Corporation	

Рис. 28. Главное окно Process Explorer

Threads	TCP/IP	Security	Enviror	nment	Job	String
Image	Perform	nance	Performar	nce Graph		GPU Graph
CPU Usage	e 					
17.26% Private By	tes	4 40 - A 6- 40	kanana	maal		l
15.6 ME I/O	3					
0						

54

File Option	s View Process F	ind Han	dle Users H	elp		
	f 🗈 🗖 🖄 🗗	* 4	•			
Process		CPU	Private Bytes	Working Set	PID Description	Company Name
smss	.exe	0	320 K	740 K	288	
Mem	ory Compression		164 K	10 012 K	2004	
CSISS.exe	9		956 K	3 584 K	380	
🖃 🔳 wininit.ex	(e		1 052 K	5 028 K	460	
🖃 🔳 servi	ces.exe		2 644 K	6 192 K	572	
- II- S1	/chost.exe		6 664 K	17 440 K	680 Хост-процесс для служб	Microsoft Corporatio
	ShellExperienceHost	Susp	31 788 K	49 460 K	3584 Windows Shell Experience H.	Microsoft Corporatio
	SearchUI.exe	Susp	53 804 K	69 788 K	3616 Search and Cortana applicati.	Microsoft Corporatio
1	RuntimeBroker.exe		12 676 K	23 976 K	4032 Runtime Broker	Microsoft Corporatio
1	SkypeHost.exe	Susp	3 624 K	16 136 K	2936 Microsoft Skype Preview	Microsoft Corporatio
	WmiPrvSE.exe	1.2	1 944 K	7 412 K	6060	
	TiWorker.exe		2 116 K	8 484 K	5972	
1 = S	vchost.exe		3 272 K	8 156 K	760 Хост-процесс для служб	Microsoft Corporatio
T.== ^	News					
туре	Name					
ALPC Port	\Sessions\1\AppCo	ontainerNar	nedObjects\S-1-1	5-2-1861897761	-1695161497-2927542615	
ALPC Port	\Sessions\1\AppCo	ontainerNar	nedObjects\S-1-1	15-2-1861897761	-1695161497-2927542615	
ALPC Port	\Sessions\T\AppCo	ontainerNar	nedObjects\S-1-1	15-2-1861897761	-1695161497-2927542615	
Desktop	\Derault					
Directory	\KnownDils	unt nin or Mar	nadObicate\S_1_1	5 2 1001007701	1005101407 2027542015	
Dimeton	\Sessions \1\AppCo	ntainerNar	nedObjects \3-1-1	5.2-1001037701	-1055101457-2527542015	
Directory	1 The second sec	ant since Mar	nedObjects \3-1-1	5.2.1001037701	1005101407-2027542015	
Directory Event	\Sessions\1\AppCo					
Directory Event Event Event	\Sessions\1\AppCo	ontainerNar	pedObjects\S-1-1	5-2-1861897761	-1695161497-2927542615-	
Directory Event Event Event Event	\Sessions\1\AppCo \Sessions\1\AppCo \Sessions\1\AppCo	ontainerNar ontainerNar	nedObjects\S-1-1 nedObjects\S-1-1	15-2-1861897761	-1695161497-2927542615	
Directory Event Event Event Event Event	\Sessions \1 \AppCo \Sessions \1 \AppCo \Sessions \1 \AppCo \Sessions \1 \AppCo \Sessions \1 \AppCo	ontainerNar ontainerNar ontainerNar	nedObjects\S-1-1 nedObjects\S-1-1 nedObjects\S-1-1	15-2-1861897761 15-2-1861897761 15-2-1861897761	-1695161497-2927542615 -1695161497-2927542615 -1695161497-2927542615	
Directory Event Event Event Event Event Event	\Sessions \1 \AppCo \Sessions \1 \AppCo \Sessions \1 \AppCo \Sessions \1 \AppCo \Sessions \1 \AppCo \Sessions \1 \AppCo	ontainerNar ontainerNar ontainerNar ontainerNar	nedObjects\S-1-1 nedObjects\S-1-1 nedObjects\S-1-1 nedObjects\S-1-1	15-2-1861897761 15-2-1861897761 15-2-1861897761 15-2-1861897761	-1695161497-2927542615 -1695161497-2927542615 -1695161497-2927542615 -1695161497-2927542615	
Directory Event Event Event Event Event Event Event	Sessions \1 AppCo \Sessions \1 AppCo	ontainerNar ontainerNar ontainerNar ontainerNar ontainerNar	nedObjects\S-1-1 nedObjects\S-1-1 nedObjects\S-1-1 nedObjects\S-1-1 nedObjects\S-1-1 nedObjects\S-1-1	5-2-1861897761 5-2-1861897761 5-2-1861897761 5-2-1861897761 5-2-1861897761 5-2-1861897761	-1695161497-2927542615 -1695161497-2927542615 -1695161497-2927542615 -1695161497-2927542615 -1695161497-2927542615	
Directory Event Event Event Event Event Event Event Event	Sessions \\AppCc \Sessions\\AppCc \Sessions\\AppCc \Sessions\\AppCc \Sessions\\AppCc \Sessions\\AppCc \Sessions\\AppCc \Sessions\\AppCc	ontainerNar ontainerNar ontainerNar ontainerNar ontainerNar ontainerNar	nedObjects\S-1-1 nedObjects\S-1-1 nedObjects\S-1-1 nedObjects\S-1-1 nedObjects\S-1-1 nedObjects\S-1-1	5-2-1861897761 5-2-1861897761 5-2-1861897761 5-2-1861897761 5-2-1861897761 5-2-1861897761 5-2-1861897761	-1695161497-2927542615 -1695161497-2927542615 -1695161497-2927542615 -1695161497-2927542615 -1695161497-2927542615 -1695161497-2927542615	

Рис. 30. Режим отображения дескрипторов

В режиме дескрипторов (рис. 30), в нижнем окне, отображаются все открытые дескрипторы выбранного в верхнем окне процесса, в данном случае, посмотрим дескрипторы открытые процессом procexp.exe: Section – диспетчер памяти объект «Секция» для общей памяти. Semaphore – исполнительная система определяет объекты «семафор». File – диспетчер ввода/вывода определяет объект «файл» для представления открытых экземпляров ресурсов драйверов устройств, которые включают в себя файлы файловой системы. Кеу – «ключ» для представления открытого ключа системного реестра. Диспетчер процессов создает объекты «поток» (Thread) и «процесс» (Process). Mutant – «мутант» внутреннее название для мьютекса.

В режиме библиотек DLL (рис. 31) отображаются все загруженные процессом динамические библиотеки и отображенные в память файлы.

File Options	View Process Fi	nd DLL	Users Help		_		1:	
		75 1 699	19					
Process		CPU	Private Bytes	Working Set	PID	Description	Company Name	^
exe.sams			320 K	740 K	288	3		1
Memory	Compression	0.01	164 K	7 764 K	2004	4		
CSrss.exe			956 K	3 576 K	380)		
🖃 🔳 wininit.exe			1 052 K	5 028 K	460)		
services.	exe		2 644 K	6 192 K	572	2		
= svcho	ost.exe	0.01	6 664 K	17 440 K	680) Хост-процесс для служб	Microsoft Corporation	
II S	ellExperienceHost	Susp	31 788 K	49 460 K	3584	4 Windows Shell Experience H	Microsoft Corporation	
Se Se	archUl.exe	Susp	53 804 K	69 796 K	3616	6 Search and Cortana applicati	Microsoft Corporation	
ILE R	untimeBroker.exe		12 552 K	22 808 K	4032	2 Runtime Broker	Microsoft Corporation	
- S	ypeHost.exe	Susp	3 624 K	16 140 K	2936	5 Microsoft Skype Preview	Microsoft Corporation	
III W	miPrvSE.exe	0.17	1 868 K	7 404 K	6060)		
svcho	st.exe	0.01	3 268 K	8 156 K	760) Хост-процесс для служб	Microsoft Corporation	
= svcho	st.exe		21 436 K	40 760 K	920) Хост-процесс для служб	Microsoft Corporation	¥
Name	Description	15	Comp	any Name		Path		~
ICAFOCOOF DEED A			(and the			N Deserver Detex Misses AVM/r		
(0AF0030E-D330-4					2	2. (Flogram Data (Microsoft (Wir	Mismost Windows Caches	
AFBF3F1A-0EE0-4	nuc Dise					2:\Dsers\Oser\+ppData\Loca 2:\ProgramData\Microsoft\Wir	down/Caches//DDE571E2	
advani32 dll	Расширенная би	блиотека	APLW Micros	off Comporation	6	?:\Windowe\Svetem32\advani	32 dll	
annhein dil	Клиентская библ		evec Micros	oft Corporation	0	Windows System 32 appha	n dl	
BCP47Langs dll	BCP47 Language	Classes	Micros	oft Corporation	0	Windows\System32\BCP47	i angs di	
borvot.dll	Библиотека криг	тографич	еских Містоз	oft Corporation	c	C:\Windows\System32\bcrypt.	dl	
bcryptprimitives.dll	Windows Cryptog	aphic Prim	tives Micros	oft Corporation	C	C:\Windows\System32\bcrypt	primitives.dll	
cfgmgr32.dll	Configuration Man	ager DLL	Micros	oft Corporation	C	C:\Windows\System32\cfgmgr	-32.dll	
clbcatq.dll	COM+ Configuration	on Catalog	Micros	oft Corporation	C	C:\Windows\System32\clbcat	q.dll	
combase.dll	Microsoft COM дл	s Windows	Micros	oft Corporation	C	C:\Windows\System32\comba	se.dll	
comctl32.dll	Библиотека элем	лентов упр	авле Micros	oft Corporation	C	C:\Windows\WinSxS\x86_mic	rosoft.windows.common-cont	
coml2.dll	Microsoft COM for	Windows	Micros	oft Corporation	C	C:\Windows\System32\coml2.	dll	
cryptbase.dll	Base cryptographi	c API DLL	Micros	oft Corporation	C	C:\Windows\System32\cryptba	ase.dll	
	Charles of the second sec			and the local sectors		1 1 1 1 1 0 1 00h	10	

Рис. 31. Режим отображения библиотек DLL

Ргосезя 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. Например, в процесс explorer.exe, входит процесс ргосехр.exe, можно уничтожить это дерево процессов (рис. 32). Приостановка работы процесса может временно освободить занятые им ресурсы для использования другими приложениями.

Ргосезя Explorer предоставляет в распоряжение пользователя удобный инструмент, с помощью которого очень просто определить то, каким процессом открыто определенное окно. Для этого следует перетащить с панели инструментов Process Explorer кнопку 😨 в любое место открывшегося окна. После этого в верхней части главного окна будет подсвечено имя искомого процесса (рис. 33).

При помощи пункта меню «Параметры – Вместо диспетчера задач» можно заменить стандартный Диспетчер задач Windows на Process Explorer (рис. 34). Информация о системе, вызываемая из Process Explorer более полная, чем аналогичная вкладка Диспетчера задач Windows.

Process		CPU	Private I	Bytes
5 (m) 5	Window		>	96 K 38 K
s s	Set Priority		>	14 K
	Kill Process		Del	36 K
	Kill Process Tree	Shi	ft+Del	18 K
2	Restart			52 K
III S	Suspend			56 K
Isas:	Create Dump		>	24 K
CSrss.ex	Check VirusTotal			40 K
🖃 🔳 winlogo	Properties			00 K 04 K
dwn	Search Online	C	Ctrl+M	84 K
🖃 📻 explorer.exe		0.08	4/ .	208 K
+ MSASCu	iL.exe		1.	432 K
VBox Tra	y.exe	0.01	21	056 K
Cone Drive	e.exe		5 -	484 K
Q procexp.	exe	6.90	13 (696 K

Рис. 32. Уничтожение дерева процессов

😺 Process Explorer - Sysinternals: w	/ww.sysi
File Options View Process Fin	nd DLL 🔨 🕺
Process	CPU
Memory Compression csrss.exe wininit.exe	
services.exe	0.01
ShellExperienceHost SearchUI.exe RuntimeBroker.exe	Susp Susp
WmiPrvSE.exe	Susp
Calculator.exe	

Рис. 33. Подсветка имени искомого процесса

При помощи пункта меню «Файл – Сохранить» (рис. 35), сохранить в текстовый файл список всех процессов с описаниями и объемом занятой каждым из них памяти.



Рис. 34. Замена стандартного диспетчера задач

File	Options	View	Process	Find	DLL	ι
	Run			Ct	rl+R	
	Run as Ad	minist	rator			
	Run as Lin	nited U	ser			
•	Show Deta	ails for	All Proces	ses		10
	Save			Ct	rl+S	
	Save As	6		Ct	rl+A	
	Shutdown	۴.			8	
	Exit					

Рис. 35. Сохранение в текстовый файл списка всех процессов

Можно рассчитать влияние приоритета процесса на количество выделяемого процессорного времени, а также задать приоритет (приоритет можно выбрать при помощи нажатия правой кнопки мыши по процессу). На рис. 36 видно, сколько выделяется суммарного времени за одну минуту при заданном приоритете «Реального времени: 24» и 4 соответственно.

Image Performance Per	formance Graph Disk and Network	Image Performance Performance G	Graph Disk and Network
CPU Priority 24 Kernel Time 0:00:03.093 User Time 0:00:01.250 Total Time 0:00:04.343 Cycles 11.544 795 121 Virtual Memory Private Bytes 15.192 K Peak Private Bytes 15.200 K Virtual Size 1.13.540 K Page Faults 176.806 Page Faults 176.806 Page Faults 176.806 15 Physical Memory Memory Memory Physical Memory 5 Working Set 3.6.808 K 36.808 K 36.808 K	I/O I/O Priority Normal Reads 76 Read Delta 0 Read Bytes Delta 0 Writes 37 Write Delta 0 Write Bytes Delta 0 Write Bytes Delta 0 Other 37 785 Other Delta 11 Other Bytes Delta 44 Handles 633 Peak Handles 633 Peak Handles 540 USER Handles 142	CPU I/O Priority 4 I/O P Kernel Time 0:00:05.546 Read User Time 0:00:02.109 Read Total Time 0:00:07.656 Read Cycles 20 856 949 120 Write Virtual Memory Write Private Bytes 15 256 K Page Faults 185 77K Other Page Faults 185 77K Other Physical Memory 1 Peak I Memory Priority 1 Peak Memory Priority 1 Peak	riority Very Low s 76 Delta 0 Bytes Delta 0 s 37 Delta 0 Bytes Delta 0 r 39 290 r Delta 11 r Bytes Delta 448 es 631 Handles 631 tandles 431
WS Private 11 728 K WS Shareable 25 076 K WS Shared 21 920 K Peak Working Set 36 816 K		WS Private 11 968 K USEK WS Shareable 25 132 K WS Shared 21 440 K Peak Working Set 37 168 K	nanues 330

Рис. 36. Влияние приоритета на выделяемые ресурсы

У потоков, также как и у процессов, существует возможность менять приоритет, приоритет потока изменяется путем изменения приоритета у процесса. Аналогично процессам, потокам выделяется процессорное время, также потоки можно приостановить и уничтожить.

Чтобы просмотреть потоки, исполняемые в рамках процесса, необходимо открыть вкладку потоки в окне свойств процесса (рис. 37).

Чтобы просмотреть стек потока процесса, необходимо нажать клавишу «Stack» (рис. 38).

Запустите «Process Monitor» (файл ProcmonRus.exe). Откроется главное окно утилиты (рис. 39). В этом окне можно отследить действия процессов во время их работы.

При помощи меню «Файл – Сохранить» можно сохранить информацию о процессах в журнал (рис. 40).

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» (рис. 41). В результате в колонке «Категория» можно увидеть действия процесса (рис. 42).

Image	Perfo	ormance	Perfor	rmance Graph		GPU Graph
Threads	TCP/IP	Securi	ty En	vironment	Job	String
Count: 5						
TID	ČPU	Cycles De	lta Start A	Address		
2976 4536 1948 2084 2512			Skypef ntdll.dll ntdll.dll combas	Host exe+Ux85 RtlUnicodeTo RtlCreateUser RtlUnicodeTo se.dll!CoDisab	MultiBy MultiBy Thread MultiBy IeCallCa	teN+0x470 +0x270 teN+0x470 incellation+.
Thread ID:		2976		Stack		Module
Thread ID: Start Time:		2976	20.09.2017	Stack		Module
Thread ID: Start Time: State: Yeared Time:		2976 17:25:09 Wait:Suspe	20.09.2017 nded	Stack Base Priority		Module 8
Thread ID: Start Time: State: Kernel Time: User Time:		2976 17:25:09 3 Wait:Suspe 0:00:00.01	20.09.2017 nded 5	Stack Base Priority Dynamic Prior	: rity:	Module 8 10 Normal
Thread ID: Start Time: State: Kernel Time: User Time: Context Switc	hes:	2976 17:25:09 Wait:Suspe 0:00:00.01 0:00:00.00	20.09.2017 nded 5 0	Stack Base Priority Dynamic Pric I/O Priority:	: rity:	Module 8 10 Normal 5
Thread ID: Start Time: State: Kernel Time: User Time: Context Switc Cydes:	hes:	2976 17:25:09 Wait:Suspe 0:00:00.01 0:00:00.00 124 63 133 637	20.09.2017 nded 5 0	Stack Base Priority Dynamic Prio I/O Priority: Memory Prio Ideal Proces	: vrity: rity: sor:	Module 8 10 Normal 5 0
Thread ID: Start Time: State: Kernel Time: User Time: Context Swite Cycles:	hes:	2976 17:25:09 Wait:Suspe 0:00:00.01 0:00:00.00 124 63 133 637 P	20.09.2017 nded 5 0	Stack Base Priority Dynamic Prio I/O Priority: Memory Prio Ideal Proces Kill	rity: sor:	Module 8 10 Normal 5 0 Resume



Рис. 38. Стек потока



🚊 Process Monitor - Sysir	ternals: www.sysinternals	.com		- 0 >	×
File Edit Event Filter	Tools Options Help				
	> 🛆 🐵 🔳 🛤 🗏				
Time Process Name	PID Operation	Path	Result	Detail	-
19:11: Searchindexer	3436 CloseFile	C:\Windows\System32	SUCCESS		
19:11: RearchIndexer	3436 🗟 File SystemContro	blC:	SUCCESS	Control: FSCTL_R	
19:11: Explorer.EXE	2912 RegQueryKey	HKU\S-1-5-21-4268929865-406128885	SUCCESS	Query: Name	
19:11: Explorer.EXE	2912 RegOpenKey	HKU\S-1-5-21-4268929865-406128885	NAME NOT FOUND	Desired Access: R	
19:11: Explorer.EXE	2912 RegOpenKey	HKCR\Applications\Procmon.exe	NAME NOT FOUND	Desired Access: R	
19:11: Explorer.EXE	2912 CreateFile	C:\Users\User\Desktop\ProcessMonito	. SUCCESS	Desired Access: R	
19:11: Explorer.EXE	2912 QueryBasicInfor	C:\Users\User\Desktop\ProcessMonito	SUCCESS	Creation Time: 20.0	
19:11 Explorer EXE	2912 CloseFile	C:\Users\User\Desktop\ProcessMonito	SUCCESS		
19:11 Explorer EXE	2912 QueryStandard	C:\Users\User\AppData\Local\Microso	SUCCESS	AllocationSize: 32	
19:11: Explorer EXE	2912 QueryStandardl.	C:\Users\User\AppData\Local\Microso	SUCCESS	Allocation Size: 1 0	
19:11 Explorer EXE	2912 RegQuervKev	HKU\S-1-5-21-4268929865-406128885	SUCCESS	Querv: Name	
19.11 Explorer EXE	2912 RegOpenKey	HKU\S-1-5-21-4268929865-406128885	NAME NOT FOUND	Desired Access R	
19:11: Explorer.EXE	2912 RegOpenKey	HKCR\CLSID\{56AD4C5D-B908-4F85	NAME NOT FOUND	Desired Access: R	
19:11: Explorer EXE	2912 RegQuervKev	HKU\S-1-5-21-4268929865-406128885.	SUCCESS	Query: Name	
19:11 Explorer EXE	2912 RegOpenKey	HKU\S-1-5-21-4268929865-406128885	NAME NOT FOUND	Desired Access: R	
19.11 Explorer EXE	2912 RegOpenKey	HKCR\Applications\Procmon exe	NAME NOT FOUND	Desired Access: R	
19:11 Explorer EXE	2912 CreateFile	C:\Users\User\Deskton\ProcessMonito	SUCCESS	Desired Access: R	
19:11: Explorer EXE	2912 QueryBasicInfor	C:\Users\User\Desktop\ProcessMonito	SUCCESS	Creation Time: 20.0	
19:11 Explorer EXE	2912 CloseFile	C:\Users\User\Desktop\ProcessMonito	SUCCESS		
19.11 Teskhostwiexe	2584 RegOpenKey	HKI M\Software\Microsoft\Input	SUCCESS	Desired Access: R	
19:11: Teskhostw exe	2584 ReqQueryValue	HKI M\SOFTWARE\Microsoft\Input\En	SUCCESS	Type: REG_DWO	
19.11 Teskhostwiexe	2584 RegCloseKey	HKLM\SOFTWARE\Microsoft\Input	SUCCESS		
19:11 Explorer EXE	2912 QueryNameInfo	C:\LIsers\LIser\Deskton\ProcessMonito	SUCCESS	Name: \Users\Use	
19-11 Explorer EXE	2912 RegOpenKey	HKU\S-1-5-21-4268929865-406128885	NAME NOT FOUND	Desired Access: Q	
19.11 Explorer EXE	2912 CreateFile	C:\Users\User	NAME COLLISION	Desired Access: B	
19:11 Explorer EXE	2912 CreateFile	C:\Users\User	SUCCESS	Desired Access: R	
19:11 Explorer EXE	2912 QueryBasicInfor	C:\Users\User	SUCCESS	Creation Time: 16.0	
19:11: Explorer EXF	2912 CloseFile	C:\Users\User	SUCCESS	Contraction of the second s	
19:11: Explorer EXF	2912 CreateFile	C:\Users\User\AppData\Local	NAME COLLISION	Desired Access: R	
19.11 Explorer EXE	2912 CreateFile	C:\Users\User\AppData\Local	SUCCESS	Desired Access: R	
19:11 Explorer EXE	2912 QueryBasicInfor	C:\Users\User\AnnData\Local	SUCCESS	Creation Time: 16.0	1
Showing 31 656 of 123 300 e	vents (25%) Ba	icked by virtual memory			

Рис. 39. Главное окно Process Monitor



Рис. 40. Сохранение в журнал

	1 1 22 24					
	Select columns to a Application Detail	ppear in the Process Mo s	nitor window:			
	Process Nan	ne Descri	iption			
	Command Li	ne Archite	ecture			
	Company Na	ame				
	Event Details	- m <u>ra_2</u> 3598				
	Sequence N	umber ⊡Path ☑Detail				
	Operation	Result	ť.			
	Date &Time		ve Time			
	✓ Time of Day ✓ Category	Durati	ion letion Time			
	Process Manager	hent				
	User Name	Proces	ss ID			
	Session ID		d ID			
	Authenticat	on ID Paren Virtual	t PID lized			
		, <u> </u>	innel .			
		ОК	Cancel			
				_		
	Рис. 4	 Выбор коло 	нок			
	Рис. 4	1. Выбор коло	нок		N-1. 111	
ब) Process Monitor - Sysi	Рис. 4	1. Выбор коло	нок		- 0	×
 Process Monitor - Sysi File Edit Event Filter Process Monitor - Sysi 	Рис. 4 nternals: www.sysinternals.com Tools Options Help Ф A (8) (1) А (8) (2)	1. Выбор коло А а Б	онок		- 0	×
Process Monitor - Sysi File Edit Event Filter Image: I	Рис. 4 nternals: www.sysinternals.com Tools Options Help → ▲ ④ 『 ▲ 馬 盧 風 PID Operation Path	1. Выбор коло <u>А а</u> п	PHOK	Detail	- Category	×
 Process Monitor - Sysi File Edit Event Filter File Que to the system Time Process Name 19:11: Searchindeser 19:11: Searchindeser 	Puc. 4	1. Выбор коло <u>А 27</u> 🖪	Result SUCCESS	Detail	Category	×
Process Monitor - Sysi File Edit Edit Event File Q Ime Process Name 19:11: SearchIndexer 19:11: SearchIndexer 19:11: SearchIndexer	Рис. 4 nternals: www.sysinternals.com Tools Options Help ▲ ④ ① ▲ 承 政政 PID Operation Path 3436 ∯ FileSystemControlC: 2912 @RegQueryKey HKU/S-1-5	 Выбор коло А 27 В NSystem 32 21-4268929965-406128885 	Result SUCCESS SUCCESS SUCCESS	Detail Control: FSCTL_R Query: Name	Category Read Metadata Read	×
Process Monitor - Sysi File Edit Event Filter Time Process Name 19-11:	Рис. 4 nternals: www.sysinternals.com Tools Options Help PID Operation Path 345 @\	1. Выбор коло <u>А</u> 27 музет 21-4268929865-406128885 21-4268929865-406128885	Result SUCCESS SUCCESS SUCCESS NAME NOT FOUN	Detail Control: FSCTL_R Query: Name D Desired Access: R.	Category Read Metadata Read	×
Process Monitor - Sysi File Edit Event Filter Process Name 19.11	Рис. 4 nternals: www.sysinternals.com Tools Options Help ▲ ④ ① ▲ ▲	 Выбор коло Выбор коло Вабор коло Кузtem32 4268929865-406128885 14268929865-406128885 Ications/Procono.ese Decharo Procono.ese 	Result SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS NAME NOT FOUN NAME NOT FOUN	Detail Control: FSCTL_R Query: Name Desired Access: R. Desired Access: R.	Category Read Metadata Read Read Read	×
Process Monitor - Sysi File Edit Event Filter Time Process Name 19:11	PIC. 4	1. Выбор коло А 27 В NSystem 32 21-4268929865-406128885 21-4268929865-406128885 cations ProcessMonto ser/Desktop ProcessMonto	Result SUCCESS SUCCESS SUCCESS SUCCESS NAME NOT FOUN SUCCESS SUCCESS SUCCESS	Detail Control: FSCTL_R Query: Name Desired Access: R. Desired Access: R. Creation Time: R.	Category Read Metadata Read Read Read	×
Process Monitor - Syst File Edit Event Filter Process Name Process Nam Process Name Process Process Name Process Nam	PHC. 4 nternals: www.sysinternals.com Tools Options Help	1. Выбор коло А. Д. Б. System32 21.4268929865-40612885 сайон Рюссено Ароссевиона ser/Desktop ProcessMonto ser/Desktop ProcessMonto	Result SUCCESS SUCCESS SUCCESS SUCCESS NAME NOT FOUN SUCCESS SUCCESS SUCCESS	Detail Control: FSCTL_R. Query: Name Desired Access: R. Desired Access: R. Creation Time: 20.0.	Category Read Metadata Read Read Read Read	×
Process Monitor - Syss File Edit Event Filter Searchindeser 19.11	Рис. 4 nternals: www.sysinternals.com Tools Options Help ▲ ▲ ④ ⑥ ▲ ゅ ω ω ω PID Operation Path 3436 %HeSystemControlC: 2912 @ RegOpenKey HKU/S-15- 2912 @ RegOpenKey HKCR-Vpg 2912 @ RegOpenKey HKCR-Vpg 2912 @ RegOpenKey HKCR-Vfg 2912 @ Re	1. Выбор коло	PHOK Result SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	Detail Control: FSCTL_R Query: Name Desired Access: R. Desired Access: R. Creation Time: 20.0. Allocation Size: 32	Category Read Metadata Read Read Read Read Read Read Read Metadata	×
Process Monitor - Sysi File Edit Event Filter Process Name 19:11 Searchindexer. 19:11 Searchindexer. 19:11 Explorer EXE 19:11	PHC. 4	1. Выбор коло А сл с. С. С. С. С. С. С. С. С. С. С. С. С. С. С	Result SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS NAME NOT FOUN SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	Detail Control: FSCTL_R Query: Name Desired Access: R. Desired Access: R. Creation Time: 20.0 AllocationSize: 32. AllocationSize: 10.	Category Read Metadata Read Read Read Read Read Metadata Read Metadata	×
Process Monitor - Sysi File Edit Event Filter Process Name 19.11	PHC. 4	1. Выбор коло А. Д. В. А. Д. В. A. System 32 21.4268929865-406128885 Calions V. Process Monto ser/Desktop ProcessMonto ser/Desktop ProcessMonto ser/Desktop ProcessMonto ser/Desktop ProcessMonto ser/Desktop Cocal Microso 21.4268929865-406128885 21.4268929865-406128885 21.4268929865-406128885 21.4268929865-406128885	Result SUCCESS SUCCESS SUCCESS SUCCESS NAME NOT FOUN NAME NOT FOUN SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	Detail Control: FSCTL_R. Query: Name Desired Access: R. Desired Access: R. Creation Time: 20.0. AllocationSize: 32. AllocationSize: 20. Query: Name Desired Access: R.	Category Read Metadata Read Read Read Read Metadata Read Metadata Read Metadata Read Metadata Read	×
Process Monitor - Sysi File Edit Event Filter Filter	Рис. 4 nternals: www.sysinternals.com Tools Options Help	1. Выбор коло	PHOK Result SUCCESS SUCCES	Detail Control: FSCTL_R. Query: Name Desired Access: R. Creation Time: 20.0. Allocation Size: 32. Allocation Size: 10. Query: Name Desired Access: R. Desired Access: R.	Category Read Metadata Read Read Read Read Metadata Read Metadata Read Read Read	×
Process Monitor - Syss File Edit Event Filter Process Name 19:11	PHC. 4 nternals: www.sysinternals.com Tools Options Help	1. Выбор коло А сл с. С. С. С. С. С. С. С. С. С. С. С. С. С. С	Result SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS NAME NOT FOUN SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	Detail Control: FSCTL_R Query: Name Desired Access: R. Desired Access: R. Creation Time: 20.0 AllocationSize: 32. AllocationSize: 32. AllocationSize: 32. Desired Access: R. Desired Access: R. Desired Access: R.	Category Read Metadata Read Read Read Read Read Metadata Read Metadata Read Read Read	×
Process Monitor - Sysi File Edit Event Filter Process Name Process	PHC. 4 nternals: www.sysinternals.com Tools Options Help ▲ ④ ① ▲ ▲ ← ▲ ← ▲ PID Operation Path 3436 Al-DaseFile C:/Window 3436 Al-DaseFile C:/Window 3446 Al-DaseFi	1. Выбор коло А. 20 21.426892965.40612885 21.426892965.40612885 21.426892965.40612885 21.426892965.40612885 21.426892965.40612885 21.426892965.40612885 21.42692965.40612885 21.42692965.40612885 21.42692965.40612885 21.42692965.40612885 21.42692965.40612885 21.42692965.40612885 21.42692965.40612885 21.42692965.40612885 21.42692965.40612885 21.42692965.40612885 21.42692965.40612885 21.42692965.40612885	Result SUCCESS	Detail Control: FSCTL_R. Joarney: Name Desired Access: R. Desired Access: R. Creation Time: 20.0 AllocationSize: 32. AllocationSize: 32. Desired Access: R. Desired Access: R. Desired Access: R. Desired Access: R.	Category Read Metadata Read Read Read Read Metadata Read Metadata Read Read Read Read Read Read Read Rea	×
Process Monitor - Syst File Edit Event Filter Time Process Name 19:11	Рис. 4 nternals: www.sysinternals.com Tools Options Help ▲ ④ ① ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲ ▲	1. Выбор коло А. Д. Б. A. Д. Б. A. System 32 21.4268929865.40612885 21.4268929865.40612885 cations /ProcessMonto ser/Desktop ProcessMonto ser/Desktop ProcessMonto ser/Desktop ProcessMonto ser/Desktop ProcessMonto z1.4268929865.40612885 z1.4268929865.406128885 z1.4268929865.406128885 z1.4268929865.406128885 z1.4268929865.406128885 z1.426892966.406128885 z1.426892966.406128885 z1.426892966.406128885 z1.426892966.406128885 z1.426892966.406128885 z1.426892966.406128885 z1.426892966.406128885 z1.426892966.40612885	Result SUCCESS SUCCESS SUCCESS SUCCESS NAME NOT FOUN SUCCESS S	Detail Control: FSCTL_R. Desired Access: R. Desired Access: R. Creation Time: 20.0. AllocationSize: 32. AllocationSize: 32. AllocationSize: 32. Query: Name Desired Access: R. Query: Name Desired Access: R. Desired Access: R. Desired Access: R. Desired Access: R.	Category Read Metadata Read Read Read Read Metadata Read Metadata Read Read Read Read Read Read Read Rea	×
Process Monitor - Systems File Edit Event Filter Searchindeser Searchind	Рис. 4 nternals: www.sysinternals.com Tools Options Help ▲ ▲ ④ ⑥ ▲ ▲ ▲ ▲ ▲ PID Operation Path 3436 %HoSystemControlC: 2912 & RegOuenkey HKU\S-15- 2912 & RegOpenkey HKU\S-15- 2914 & RegOpenkey HKU\S-15- 2915 & RegOpenkey HKU\S-15- 2916 &	1. Выбор коло	PHOK Pesuit SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS NAME NOT FOUN SUCCESS NAME NOT FOUN SUCCESS NAME NOT FOUN SUCCESS	Detail Control: FSCTL_R Query: Name Desired Access: R. Creation Time: 20.0 AllocationSte: 32. AllocationSte: 32. AllocationSte: 32. Desired Access: R. Desired Access: R.	Category Read Metadata Read Read Read Read Read Metadata Read Read Read Read Read Read Read Rea	×
Process Monitor - Sysi File Edit Event Filter Process Name Pr	PHC. 4	1. Выбор коло А. 20 21.4268929865-40612885 21.42689	Result SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS NAME NOT FOUN NAME NOT FOUN NAME NOT FOUN NAME NOT FOUN SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	Detail Control: FSCTL_R. Guery: Name Desired Access: R. Desired Access: R. Creation Time: 20.0 AllocationSize: 32. AllocationSize: 32. Desired Access: R. Desired Access: R. Creation Time: 20.0	Category Read Metadata Read Read Read Read Metadata Read Metadata Read Read Read Read Read Read Read Rea	×
Process Monitor - Syst File Edit Event Filter Process Name Pr	Рис. 4 nternals: www.sysinternals.com Tools Options Help	1. Выбор коло А. Д. Б. A. Д. Б. A. System 32 21.4268929865.406128885 21.4268929865.406128885 Call Data Local Microso ser/Desktop ProcessMonto ser/Desktop ProcessMonto ser/Desktop ProcessMonto ser/Desktop ProcessMonto ser/Desktop ProcessMonto z1.4268929865.406128885 D1056AD4C5D-B908.4785 z1.4268929665.406128885 z1.	Result SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS NAME NOT FOUN SUCCESS SUCCESS SUCCESS SUCCESS NAME NOT FOUN SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	Detail Control: FSCTL_R. Desired Access: R. Desired Access: R. Desired Access: R. Creation Time: 20.0. AllocationSize: 32. AllocationSize: 32. AllocationSize: 32. Desired Access: R. Desired Access: R. Creation Time: 20.0. Desired Access: R. Creation Time: 20.0. Desired Access: R.	Category Read Metadata Read Read Read Read Metadata Read Metadata Read Read Read Read Read Read Read Rea	×
Process Monitor - Syst File Edit Event Filter Searchindeser Searchindese	Рис. 4 nternals: www.sysinternals.com Tools Options Help	1. Выбор коло	Result SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS NAME NOT FOUN NAME NOT FOUN SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	Detail Control: FSCTL_R Guery: Name Desired Access: R. Desired Access: R. Creation Time: 20.0 AllocationSter: 32. AllocationSter: 32. AllocationSter: 32. Desired Access: R. Desired Access: R. Desired Access: R. Desired Access: R. Creation Time: 20.0 Bearde Access: R. Creation Time: 20.0 Bearde Access: R. Type: REG_DWO	Category Read Metadata Read Read Read Read Read Read Read Rea	×
Process Monitor - Sysi File Edit Event Filter Process Name Pr	PHC. 4 nternals: www.sysinternals.com Tools Options Help	1. Выбор коло А. 20 В A. 20 В Alsystem 32 21-4268929865-40612885 21-4268929865-40612885 Catalons Process Monto ser/Desktop Process Monto Ser/Desktop Process Monto ser/Desktop Process Monto Ser/Desktop Process Monto 21-4268929665-40612885 21-4268929665-40612885 21-4268929665-40612885 21-426892966-40612885 21-426892966-406128885 21-426892966-406128885 21-426892966-40612885 21-426892966-40612885 21-426892966-40612885 21-426892966-40612885 21-426892966-40612885 21-426892966-40612885 21-426892966-40612885 21-426892966-40612885 21-426892966-40612885 21-426892966-40612885 21-426892966-40612885 21-426892966-40612885 21-426892966-40612885 21-426892966-40612885 21-426892966-40612885 21-426892966-40612885 21-426892966-40612885 21-426892966-40612885 21-426892966-40612885 21-426892966-40612885 21-426892966-40612885 21-426892966-40612885 <	Result SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS NAME NOT FOUN NAME NOT FOUN NAME NOT FOUN NAME NOT FOUN SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS	Detail Control: FSCTL_R. Guery: Name Desired Access: R. Desired Access: R. Creation Time: 20.0. AllocationSize: 32. AllocationSize: 32. Desired Access: R. Desired Access: R. Desired Access: R. Desired Access: R. Creation Time: 20.0. Desired Access: R. Creation Time: 20.0. Desired Access: R. Creation Time: 20.0. Desired Access: R. Creation Time: 20.0. Desired Access: R. Type: REG_DWO.	Category Read Metadata Read Read Read Read Read Metadata Read Read Read Read Read Read Read Rea	×
Process Monitor - Syst File Edit Event Filter Process Name Pr	Рис. 4 nternals: www.sysinternals.com Tools Options Help	1. Выбор коло А. Д. Ш. A. Д. Ш. A. System 32 21.4269329865.406128885 21.4269329865.406128885 1.7000000000000000000000000000000000000	Result SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS NAME NOT FOUN SUCCESS SUCCESS SUCCESS SUCCESS SUCCESS NAME NOT FOUN NAME NOT FOUN NAME NOT FOUN SUCCESS	Detail Control: FSCTL_R. Quey: Name Desired Access: R. Desired Access: R. Creation Time: 20.0. AllocationSize: 3.0. Quey: Name Desired Access: R. Desired Access: R. Desired Access: R. Creation Time: 20.0. Desired Access: R. Creation Time: 20.0. Desired Access: R. Creation Time: 20.0. Desired Access: R. Type: REG_DWO Name: Users'Uses	Category Read Metadata Read Read Read Read Read Metadata Read Metadata Read Read Read Read Read Read Read Rea	×
Process Monitor - Syst File Edit Event Filter Process Name Process Name Process Name Process Name Process Name Search Indexer Search Indexer Process Name Process Process Name	Рис. 4 nternals: www.sysinternals.com Tools Options Help	1. Выбор коло А. С.	Result SUCCESS	Detail Control: FSCTL_R Query: Name Desired Access: R. Desired Access: R. Creation Time: 20.0 AllocationSize: 32. AllocationSize: 32. AllocationSize: 32. Desired Access: R. Desired Access: R. Desired Access: R. Desired Access: R. Creation Time: 20.0 Beired Access: R. Creation Time: 20.0 Beired Access: R. Type: REG_DWO Name: \Users\User Desired Access: R.	Category Read Metadata Read Read Read Read Read Read Read Rea	×
Process Monitor - Sysi File Edit Event Filter Process Name Pr	PHC. 4	1. Выбор коло А. 20 В a\System 32 21.4268929865-40612885 21.4268929865-40612885 21.4268929865-40612885 21.4268929865-40612885 21.4268929865-40612885 21.4268929865-40612885 21.426929865-40612885 21.426892965-40612885 21.426892965-40612885 21.426892965-40612885 21.426892965-40612885 21.426892965-40612885 21.426892965-40612885 21.426892965-40612885 21.426892965-40612885 21.426892965-40612885 21.426892965-40612885 21.426892965-40612885 21.426892965-40612885 21.426892965-40612885 21.426892965-40612885 21.426892965-40612885 21.426892965-40612885 21.426892965-40612885 21.426892965-40612885 21.426892965-40612885 21.426892965-40612885	Result SUCCESS	Detail Control: FSCTL_R. Desired Access: R. Desired Access: R. Creation Time: 20.0. AllocationSize: 32. AllocationSize: 32. AllocationSize: 32. Desired Access: R. Desired Access: R. Desired Access: R. Creation Time: 20.0. Desired Access: R. Creation Time: 20.0. Desired Access: R. Type: REG_DWO. Desired Access: R. Type: REG_DWO. Desired Access: Q. Desired Access: Q. Desired Access: Q. Desired Access: R. Type: REG_DWO.	Category Read Metadata Read Read Read Read Read Metadata Read Read Read Read Read Read Read Rea	×
Process Monitor - Syst File Edit Event Filter Time Process Name 19:11	Рис. 4 nternals: www.sysinternals.com Tools Options Help	1. Выбор коло А. Д. П. A. Уузtен 32 21.4268929865-406128885 21.4268929865-406128885 12.126929865-406128885 12.126929865-406128885 ser/Desktop ProcessMonto ser/Desktop ProcessMonto ser/Desktop ProcessMonto ser/Desktop ProcessMonto ser/Desktop ProcessMonto 21.4268929865-406128885 12.4268929865-406128885 12.1268929865-406128885 12.1268929865-406128885 12.1268929865-406128885 ser/Desktop ProcessMonto ser ser	Result SUCCESS	Detail Control: FSCTL_R. Desired Access: R. Desired Access: R. Desired Access: R. Creation Time: 20.0. AllocationSize: 3.2. AllocationSize: 3.2. Desired Access: R. Desired Access: R. Desired Access: R. Creation Time: 20.0. Desired Access: R. Creation Time: 20.0. Desired Access: R. Creation Time: 20.0. Desired Access: R. Creation Time: 20.0. Desired Access: R. Creation Access: R. Desired Access: R. State Access: R. Creation Time: 20.0. Desired Access: R. Creation Time: 20.0. Desired Access: R. Creation Time: 20.0. Desired Access: R. Creation Time: 16.0.	Category Read Metadata Read Read Read Read Metadata Read Metadata Read Read Read Read Read Read Read Rea	×
Process Monitor - Syst File Edit Event Filter Process Name Pr	Рис. 4 nternals: www.sysinternals.com Tools Options Help	1. Выбор коло А. Д. Б. (1) Кузtem 32 21 426892965406128885 21 426892965406128885 21 426892965406128885 21 426892965406128885 21 426892965406128885 21 42692965406128885 21 42692965406128885 21 42692965406128885 21 42692965406128885 21 42692965406128885 21 42692965406128885 21 42692965406128885 21 42692965406128885 21 42692965406128885 21 42692965406128885 21 42692965406128885 21 42692965406128885 21 42692965406128885 21 42692965406128885 21 42692965406128885 24 62692965406128885 24 62692965406128885 24 62692965406128885 24 62692965406128885 24 62692965406128885 24 62692965406128885 24 62692965406128885 24 62692965406128885 24 62692965406128885 24 62692965406128885 24 62692965406128885 24 626929654	Result SUCCESS	Detail Control: FSCTL_R Query: Name Desired Access: R. Creation Time: 20.0 AllocationSize: 32. AllocationSize: 32. AllocationSize: 32. Query: Name Desired Access: R. Desired Access: R. Creation Time: 20.0 Desired Access: R. Creation Time: 20.0 Name: \Users\User Desired Access: R. Desired Access: R. Desired Access: R. Desired Access: R. Desired Access: R. Desired Access: R. Desired Access: R.	Category Read Metadata Read Read Read Read Read Metadata Read Read Read Read Read Read Read Rea	×
Process Monitor - Sysi File Edit Event Filter Time Process Name 19:11	Рис. 4 nternals: www.sysinternals.com Tools Options Help ▲ ④ ④ ① ▲ ▲ ▲ ▲ ▲ ▲ ▲ PID Operation Path 3436 AlcoseFile C.Window 3436 AlcoseFile C.Window 3436 AlcoseFile C.Window 3436 AlcoseFile C.Window 3436 AlcoseFile C.Window 2912 AlcreyBasicInfor. C.Users W 2912 AlcrestFile C.Users W 2913 AlcrestFile C.Users W 2914 AlcrestFile C.Users W 2914 AlcrestFile C.Users W 2915 AlcrestFile C.Users W 2915 AlcrestFile C.Users W 2916 C.CrestFile C.Users W 2917 AlcrestFile C.Users W 2918 AlcrestFile C.Users W 2919 AlcrestFile C.Users W 2919 AlcrestFile C.Users W 2919 AlcrestFile C.Users W 2910 AlcrestFile	1. Выбор коло А. 20 A. 20 A. 20 A. 20 A. 20 A. 20 A. 21 21-426892965-40612885 21-426892965-40612885 21-426892965-40612885 21-426892965-40612885 21-42692965-40612885 21-42692965-40612885 21-42692965-40612885 21-42692965-40612885 21-42692965-40612885 21-42692965-40612885 21-42692965-40612885 21-42692965-40612885 21-42692965-40612885 21-42692965-40612885 21-42692965-40612885 21-42692965-40612885 21-42692965-40612885 21-42692965-40612885 21-42692965-40612885 21-42692965-40612885 21-42692965-40612885 21-9000000000000000000000000000000000000	Result SUCCESS	Detail Control: FSCTL_R. Desired Access: R. Desired Access: R. Creation Time: 20.0. AllocationSize: 32. AllocationSize: 32. AllocationSize: 32. Desired Access: R. Desired Access: R. Desired Access: R. Desired Access: R. Desired Access: R. Creation Time: 20.0. Desired Access: R. Creation Time: 20.0. Desired Access: R. Creation Time: 20.0. Desired Access: R. Desired Access: R. Desired Access: R. Desired Access: R. Desired Access: R. Creation Time: 16.0. Desired Access: R. Creation Time: 16.0. Desired Access: R. Creation Time: 16.0. Desired Access: R.	Category Read Metadata Read Read Read Read Metadata Read Metadata Read Read Read Read Read Read Read Rea	×

62

Рис. 42. Отслеживание действий процесса

Process Name	PID	CPU	File E
🚑 SearchIndexer.exe	3436		
services.exe	572		
smss.exe	288		
Explorer.EXE	2912		
Csrss.exe	380		
wininit.exe	460		
🔳 taskhostw.exe	2584		
svchost.exe	920	a	
Csrss.exe	468		
winlogon.exe	544		
Isass.exe	580		2
< > <	C.1	k	>
Command Line: C:\Windows\Expl	orer.EXE		
Started: 20.09.2017	Total User (CPU: 00:00:09.265	6250
inded: 20.09.2017	Total Kerne	CPU: 00:00:19.218	7500
i3 items	Detail	Save	Close

Также можно отследить активность процессов при помощи меню «Инструменты – Лог активных процессов» (рис. 43).

Рис. 43. Лог активных процессов

Ргосезя Monitor предоставляет возможность создавать фильтры, позволяющие делать выборки из журналов. Попасть в меню фильтров можно нажатием сочетания клавиш Ctrl+L. Фильтры можно создавать по многим параметрам, например, по имени процесса, времени, категории, операций и др. Создадим фильтр, который делает выборку процессов по операции записи в файл (рис. 44).

Также можно отследить работу процессов с файловой системой и реестром при установке программного обеспечения. Рассмотрим данную функцию на примере установки 7-zip. Установите программу. После установки выведите на экран информацию о записи ключей в реестр при установке программы. Для этого необходимо создать фильтр, который делает выборку процессов по операции записи в RegCreateFile. Определите, в каких разделах реестра 7-zip сохранил свою информацию. По аналогии определите, в каких каталогах диска были созданы новые данные.

isplay enules match	ing these conditio	ins:			
Operation	∼ is	✓ WriteFile	×	then	Include 🗸
Reset			Add		Remove
Column	Relation	Value	Action	1	^
🗹 🍪 Operation	is	WriteFile	Include		
🗹 🔕 Process N	is	Procmon.exe	Exclude		
🗹 🐼 Process N	is	Procexp.exe	Exclude		
🗹 🐼 Process N	is	Autoruns.exe	Exclude		
Process N	is	System	Exclude		
🗹 🐼 Operation	begins with	IRP_MJ_	Exclude		
C 🖸 Operation	beains with	FASTIO	Exclude		~

Рис. 44. Создание фильтра

🚊 Process Monitor - Sysinter	rnals: www.sysinter	nals.com			-
File Edit Event Filter To	ools Options H	elp			
	A 🐵 🗊 🗚				
Time Process Name	PID Operation	Path	Result	Detail	Category
19:22: 4 OneDrive.exe 3	3884 🗒 WriteFile	C:\Users\User\AppData\Local\Micro	so SUCCESS	Offset: 183 226, L	eWrite
19:22: 🐔 One Drive.exe 3	3884 🗟 WriteFile	C:\Users\User\AppData\Local\Micro	so SUCCESS	Offset: 183 340, L	eWrite
19:22: 4 OneDrive.exe 3	3884 🗟 WriteFile	C:\Users\User\AppData\Local\Micro	so SUCCESS	Offset: 183 458, L	eWrite
19:22: 4 OneDrive.exe 3	3884 🗟 WriteFile	C:\Users\User\AppData\Local\Micro	so SUCCESS	Offset: 183 610, L	eWrite
19:23: ConeDrive.exe 3	3884 🗟 WriteFile	C:\Users\User\AppData\Local\Micro	so SUCCESS	Offset: 183 720, L	eWrite
19:23: ConeDrive.exe 3	3884 🗟 WriteFile	C:\Users\User\AppData\Local\Micro	so SUCCESS	Offset: 183 834, L	eWrite
19:23: ConeDrive.exe 3	3884 🖳 WriteFile	C:\Users\User\AppData\Local\Micro	so SUCCESS	Offset: 183 952, L	eWrite
19:23: 🐔 One Drive.exe 3	3884 🖳 Write File	C:\Users\User\AppData\Local\Micro	so SUCCESS	Offset: 184 104, L	eWrite
19:23: 4 OneDrive.exe 3	3884 🗟 WriteFile	C:\Users\User\AppData\Local\Micro	so SUCCESS	Offset: 184 214, L	eWrite
19:23: ConeDrive.exe 3	3884 🖳 WriteFile	C:\Users\User\AppData\Local\Micro	so SUCCESS	Offset: 184 328, L	eWrite
19:23: 4 OneDrive.exe 3	3884 🗟 WriteFile	C:\Users\User\AppData\Local\Micro	so SUCCESS	Offset: 184 446, L	eWrite
19:23: ConeDrive.exe 3	3884 🕃 WriteFile	C:\Users\User\AppData\Local\Micro	so SUCCESS	Offset: 184 598, L	eWrite
Showing 12 of 115 733 events (0.0%)	Backed by virtual memory			

Васкеd by virtual memory Рис. 45. Результат действия фильтра

4. Задание на лабораторную работу

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.

5. Контрольные вопросы

1. Что такое служба Windows?

2. Какие средства для управления службами предусмотрены в Windows?

3. В каких состояниях может находиться служба?

4. Какие действия могут применяться при сбое службы?

5. Правами каких учётных записей может обладать служба при запуске?

6. Чем отличаются команды для управления службами семейств net и sc?

7. Какие команды используются для изменения состояния и типа запуска служб?

8. Чем отличается процесс от потока?

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

10. По каким параметрам можно создавать фильтры в Process Monitor?