Лекция 7

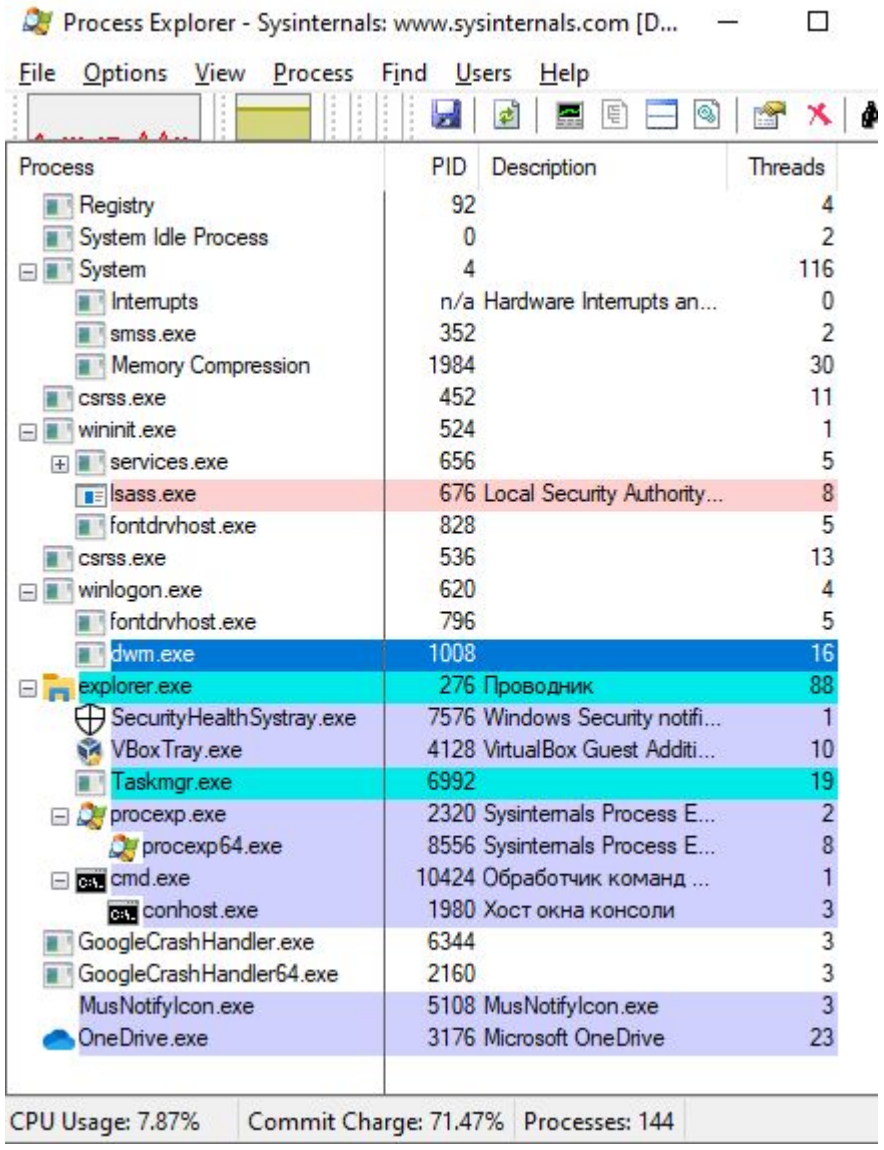
Системные процессы Windows

Основные системные файлы

Имя файла	**Компоненты**
Ntoskrnl.exe	Исполнительная система и ядро
Hal.dll	HAL
Win32k.sys	Часть подсистемы Windows режима ядра (GUI)
Hvix64.exe (Intel), Hvax64.exe (AMD)	Гипервизор
.sys les in \SystemRoot\System32\Drivers	Основные файлы драйверов: Direct X, Volume Manager, TCP/IP, TPM и поддержка ACPI
Ntdll.dll	Внутренние вспомогательные функции и заглушки диспетчеризации системных сервисных функций
Kernel32.dll, Advapi32.dll, User32.dll, Gdi32.dll	DLL основных подсистем Windows

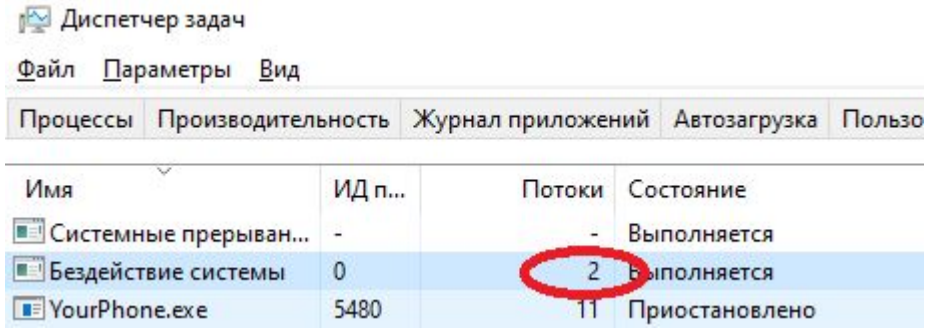
Основные системные процессы

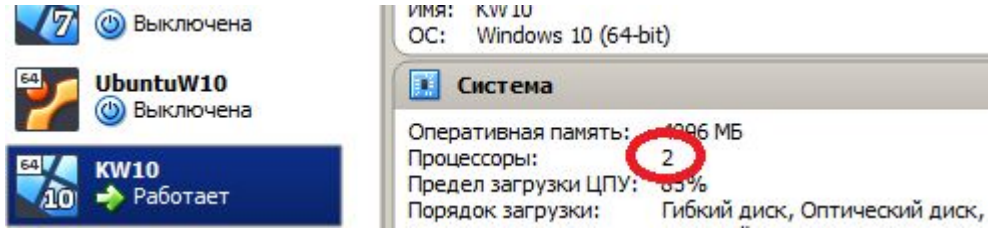
- Процесс **Idle** (включает по одной нити на процессор для учета времени простоя процессора)
- Процесс **System** (содержит большинство системных потоков режима ядра)
- Диспетчер сеансов (**Smss.exe**)
- Подсистема Win32 (**Csrss.exe**) – 2 экземпляра
- Инициализация сеанса 0 (**wininit.exe**)
- Процесс входа в систему (**Winlogon.exe**)
- Диспетчер управления сервисами (**Services.exe**) и дочерние процессы сервисов (**Svchost.exe**)
- Серверный процесс локальной аутентификации (**Lsass.exe**)



Процесс простоя системы

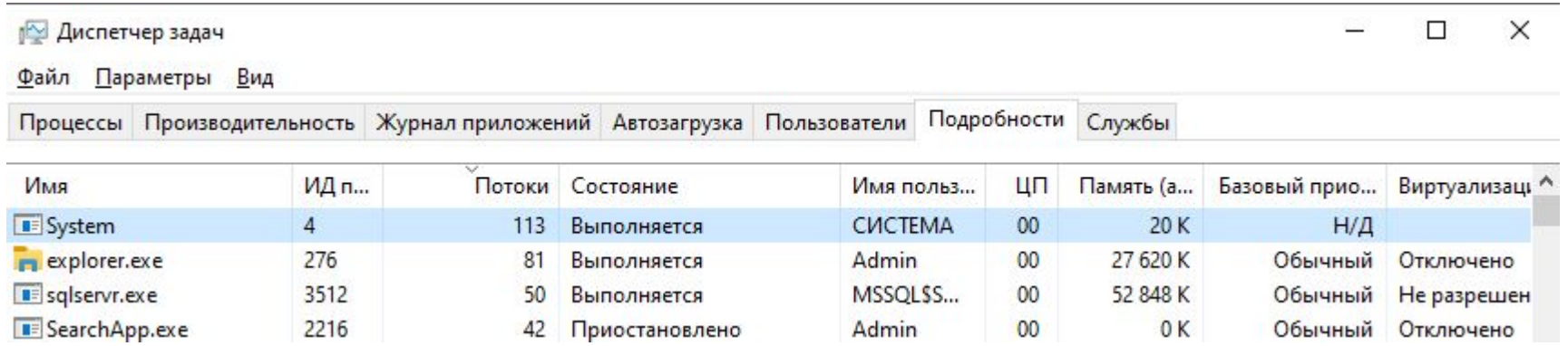
- этот процесс с идентификатором 0 не выполняет реальный код пользовательского режима
- учитывает время бездействия процессора в системе, имеет по одному потоку на процессор
- имена отличаются в разных утилитах:
  - Task Manager **System Idle Process**
  - Process Viewer (Pviewer.exe) **Idle**
  - Process Explode (Procexp.exe) **System Idle Process**
  - Task List (Tlist.exe) **System Idle Process**





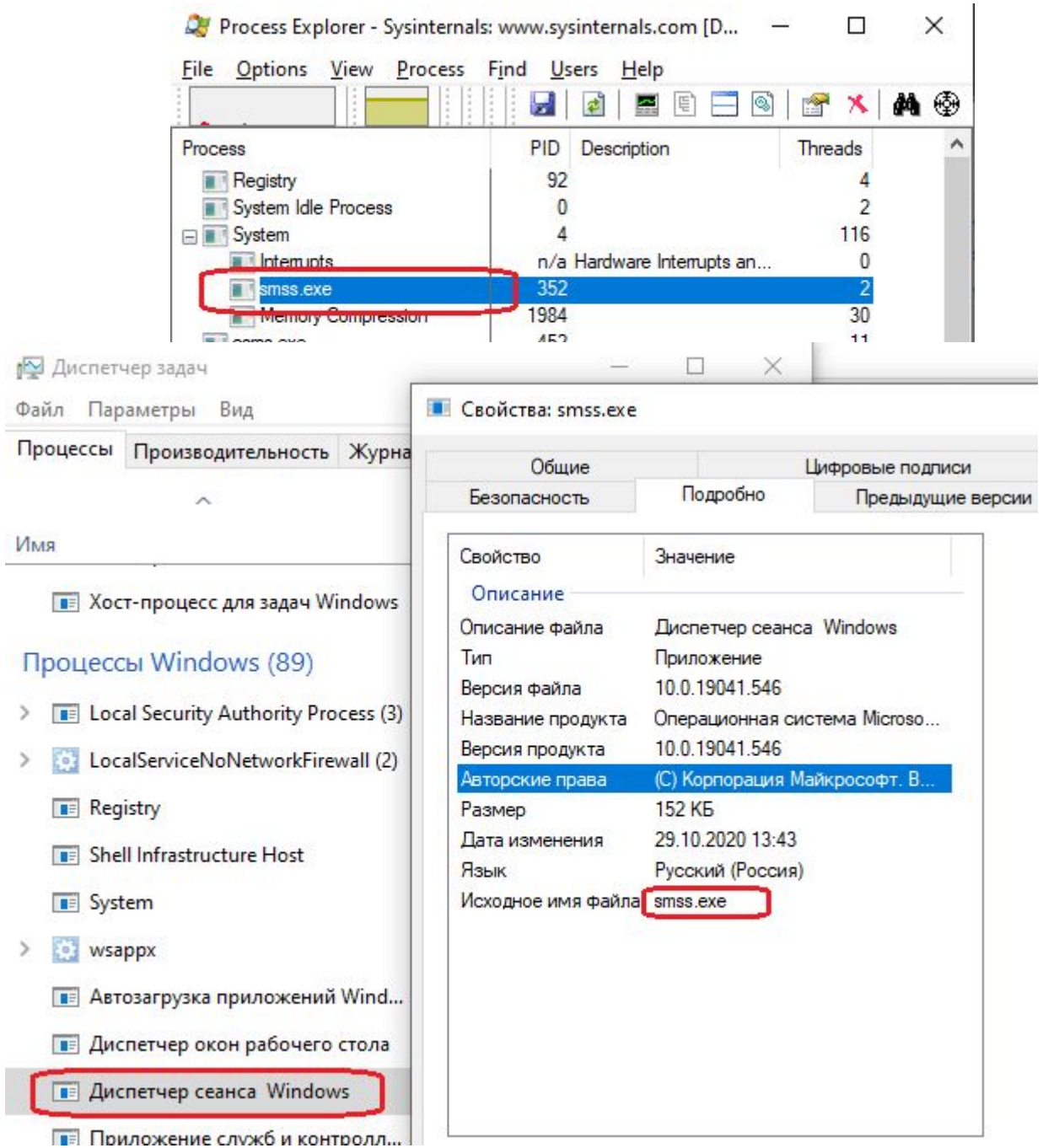
Процесс System и его нити

- Процесс **System** (PID 4) служит носителем особых нитей, работающих только в режиме ядра, — **системных нитей режима ядра (kernel-mode system threads).**
- У них имеются все атрибуты и контексты обычных потоков пользовательского режима (например, контекст оборудования, приоритет и т. д.), но они отличаются тем, что выполняются только в режиме ядра внутри системного кода, загруженного в системное пространство, — будь то Ntoskrnl.exe или какой-либо драйвер устройства.
- У системных потоков нет адресного пространства пользовательского процесса, и поэтому нужная им динамическая память выделяется из куч памяти операционной системы, например из **пула подкачиваемых или неподкачиваемых страниц**

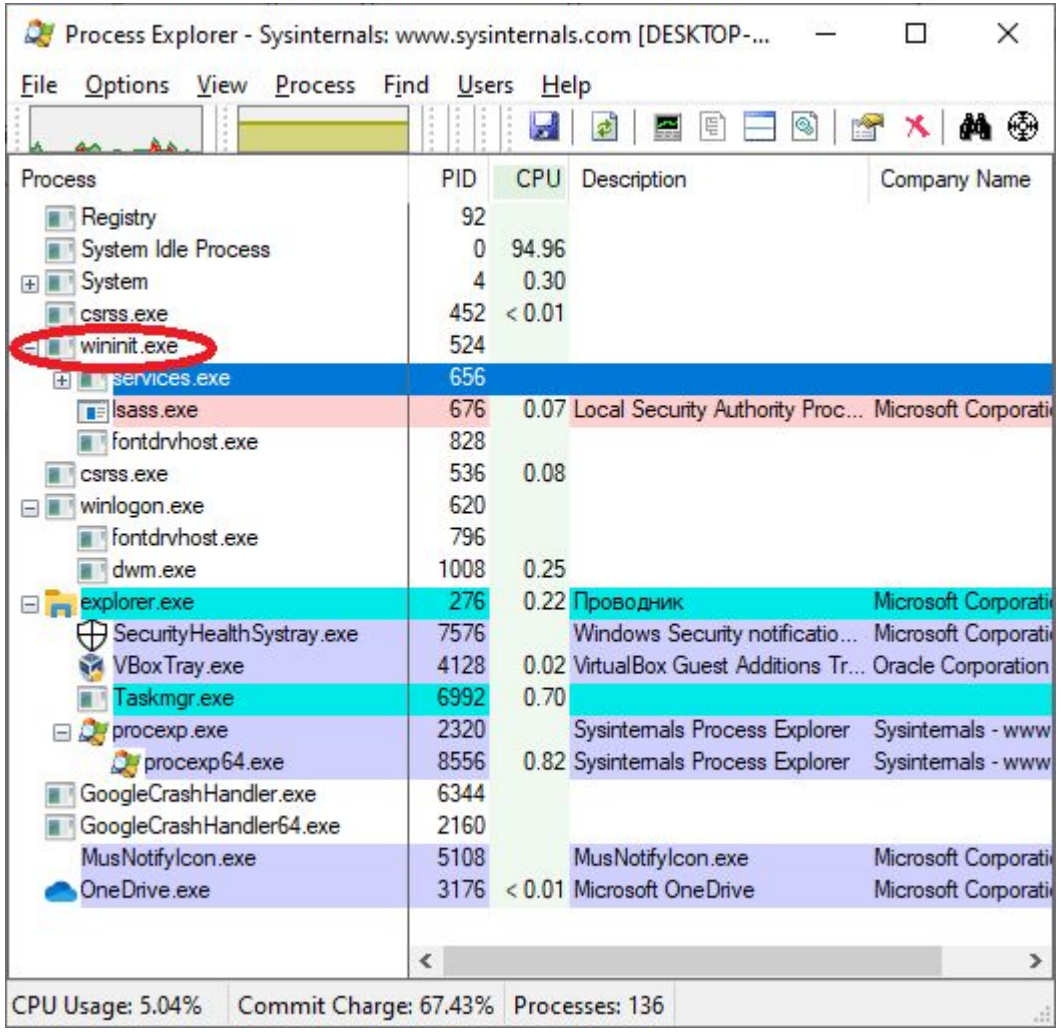


Диспетчер сеансов (Smss)

- Диспетчер сеансов (**Session Manager**) (\Windows\System32\Smss.exe) является первым процессом пользовательского режима, создаваемым в системе.
- Он порождается системным потоком режима ядра, отвечающим за последний этап инициализации исполнительной системы и ядра
- запускает процессы подсистем (обычно только **Csrss.exe**) и **Winlogon**, который в свою очередь создает остальные системные процессы.
- при неожиданном завершении любого из них Smss вызывает **крах системы**
- Инициализирует файлы подкачки



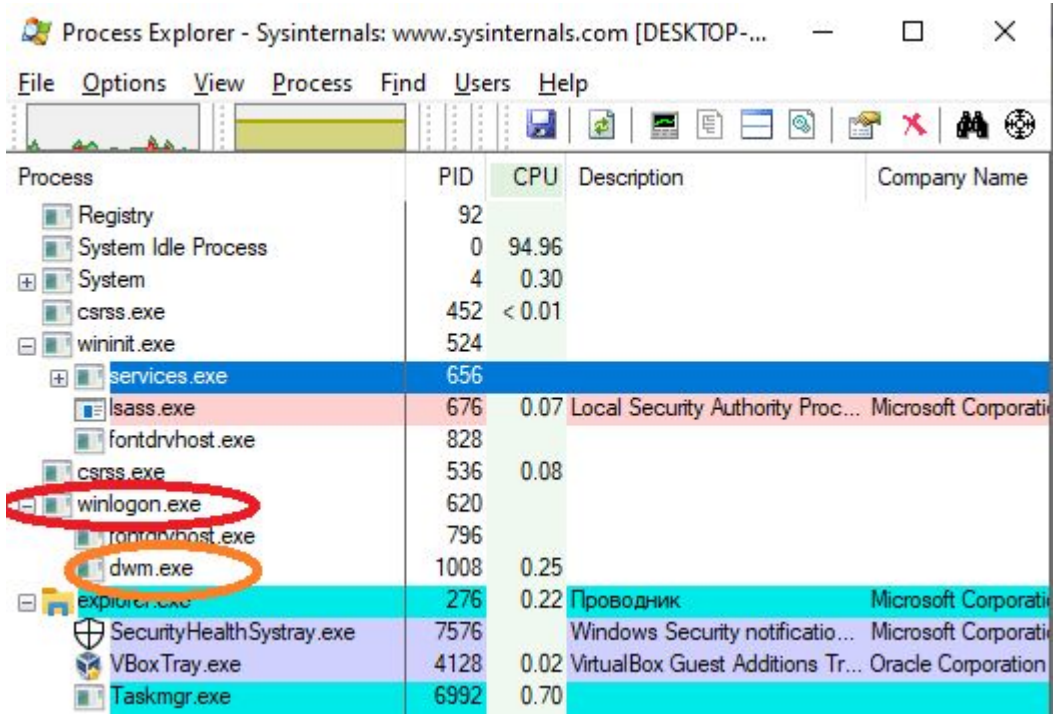
Процесс инициализации Wininit

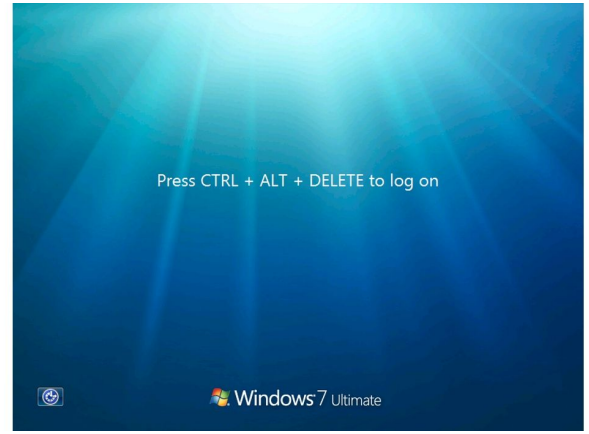


- Создает папку %windir%\Temp
- Запускает Services.exe (диспетчер управления службами — Service Control Manager или SCM)
- Запускает Lsass.exe (Local Security Authentication Subsystem Server — сервер проверки подлинности локальной системы безопасности)

WINLOGON

- Процесс входа в Windows %winroot%\System32\Winlogon.exe) обрабатывает интерактивный вход пользователя в систему и выход из нее
- SAS (secure attention sequence) =Ctrl+Alt+Del
- Интерфейсы аутентификации по умолчанию — пароли и смарт-карты
- Desktop Window Manager (dwm.exe) – это системный процесс в Windows 10, который управляет отображением окон приложения, он отвечает за визуальные, 3D-эффекты и темы Windows, он создает предварительный просмотр миниатюр окна на панели задач, поддерживает устройства с высоким разрешением и т. д.

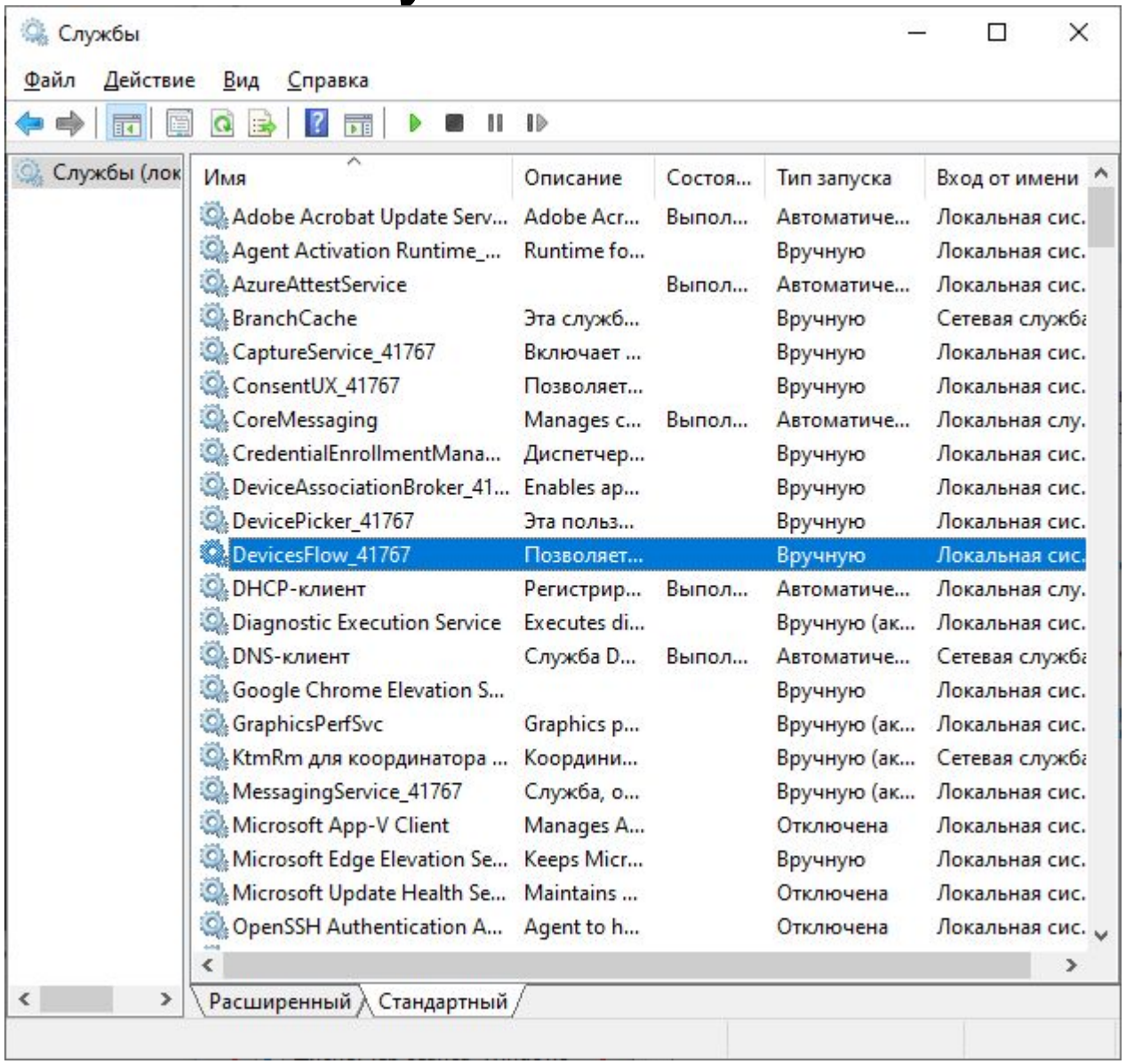




Winlogon, LSASS и Userinit

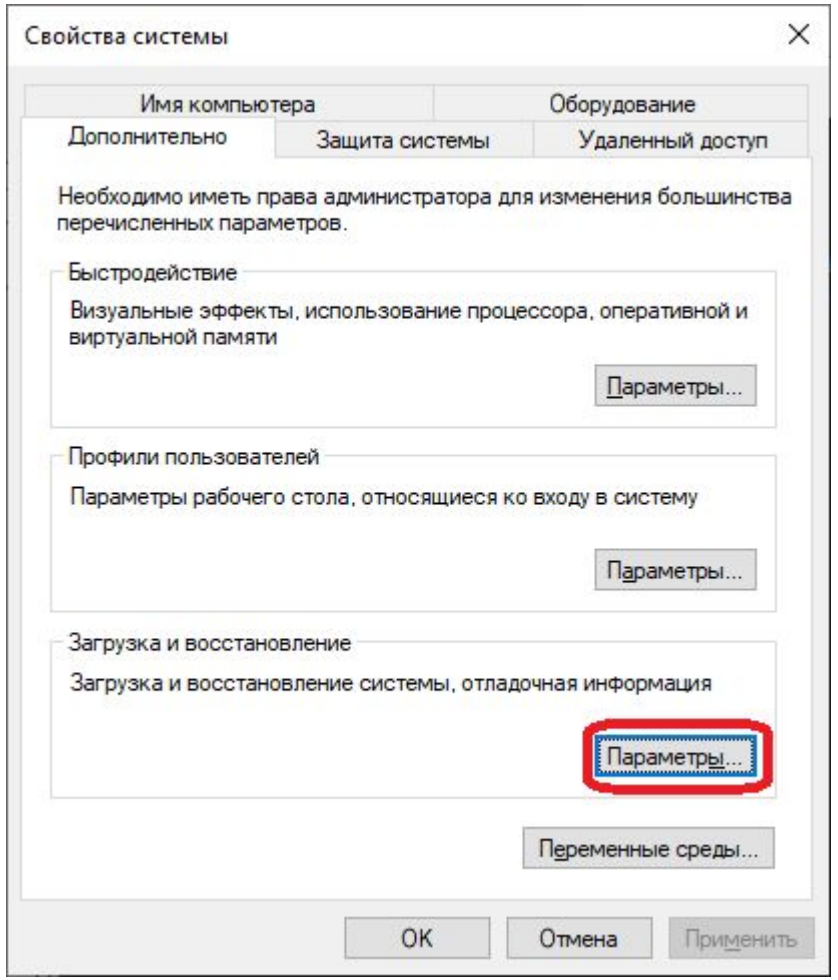
- LogonUI — дочерний процесс с вызовом пользовательского интерфейса входа в систему
- LogonUI отсылает информацию LSASS, который вызывает пакет аутентификации — AD или SAM
- Запускает исходный процесс пользовательского сеанса
- HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon, по умолчанию Userinit.exe, но могут быть и другие
- Userinit инициализирует пользовательскую среду, запускает сценарий входа и применяет групповую политику, затем запускает оболочку из параметра Shell и завершается
- Поэтому у процесса Explorer.exe родительский процесс не показывается

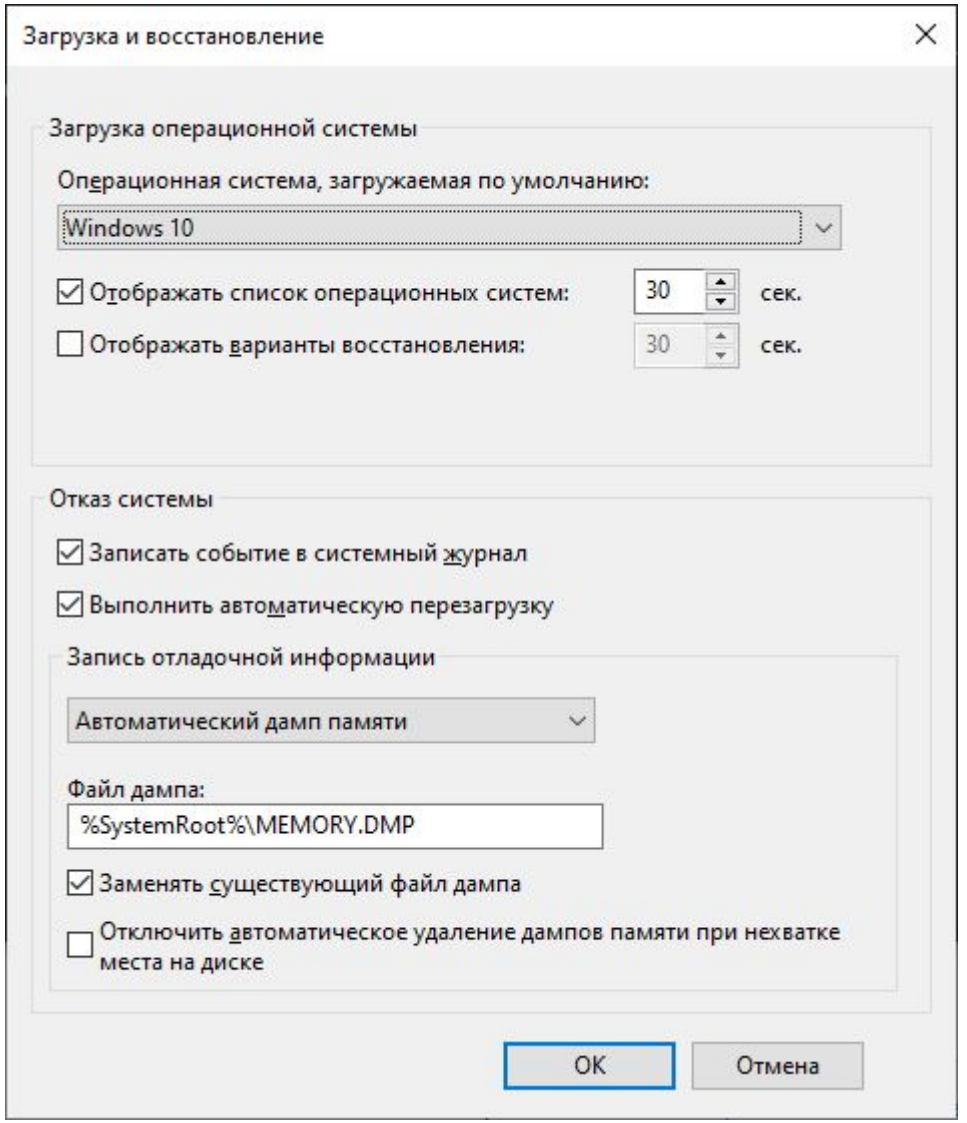
Диспетчер управления службами



- %SystemRoot%\System32\Services.exe - специальный системный процесс , отвечающий за запуск и остановку служб и за взаимодействие с ними
- HKLM\SYSTEM\CurrentControlSet\Services
- Три имени:
  - имя процесса, запущенного в системе
  - внутреннее имя в реестре
  - имя в консоли mmc Services.msc
- Примеры системных служб: Диспетчер печати, Журнал событий, Планировщик заданий и т д

Параметры загрузки и восстановления





Переменные среды