

# Лекция 7

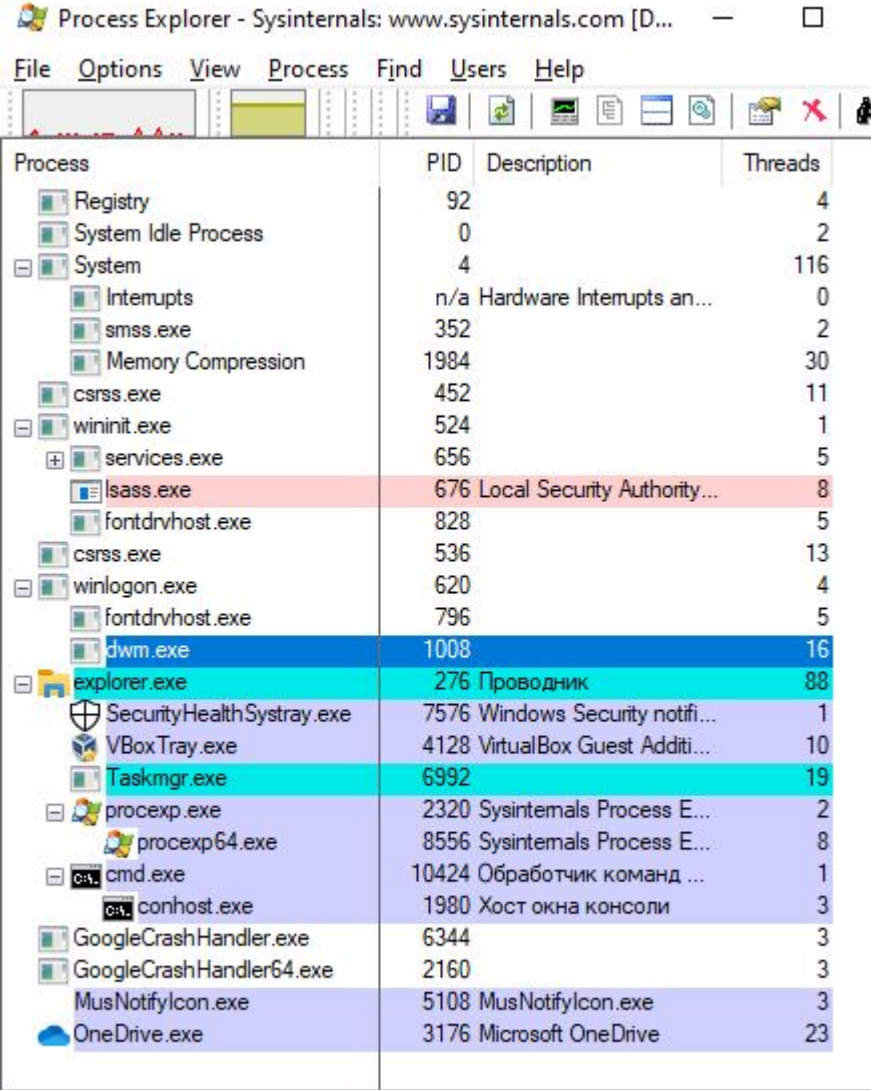
Системные процессы Windows

# 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 files 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**)



The screenshot shows the Process Explorer window from Sysinternals. The main pane displays a list of processes with columns for Process, PID, Description, and Threads. The processes are organized into a tree view. The status bar at the bottom shows CPU Usage: 7.87%, Commit Charge: 71.47%, and Processes: 144.

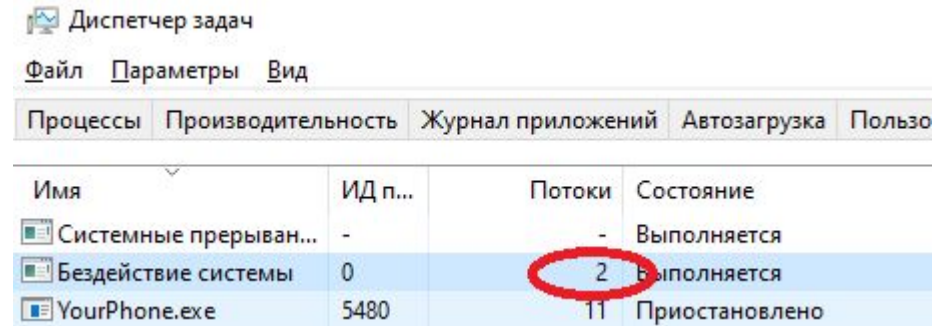
Process	PID	Description	Threads
Registry	92		4
System Idle Process	0		2
System	4		116
Interrupts	n/a	Hardware Interrupts an...	0
smss.exe	352		2
Memory Compression	1984		30
csrss.exe	452		11
wininit.exe	524		1
services.exe	656		5
lsass.exe	676	Local Security Authority...	8
fontdrvhost.exe	828		5
csrss.exe	536		13
winlogon.exe	620		4
fontdrvhost.exe	796		5
dwm.exe	1008		16
explorer.exe	276	Проводник	88
SecurityHealthSystray.exe	7576	Windows Security notifi...	1
VBoxTray.exe	4128	VirtualBox Guest Additi...	10
Taskmgr.exe	6992		19
procexp.exe	2320	Sysinternals Process E...	2
procexp64.exe	8556	Sysinternals Process E...	8
cmd.exe	10424	Обработчик команд ...	1
conhost.exe	1980	Хост окна консоли	3
GoogleCrashHandler.exe	6344		3
GoogleCrashHandler64.exe	2160		3
MusNotifylcon.exe	5108	MusNotifylcon.exe	3
OneDrive.exe	3176	Microsoft OneDrive	23

CPU Usage: 7.87%    Commit Charge: 71.47%    Processes: 144

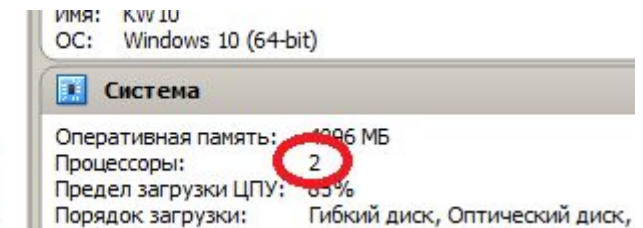
# Процесс простоя

## 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**



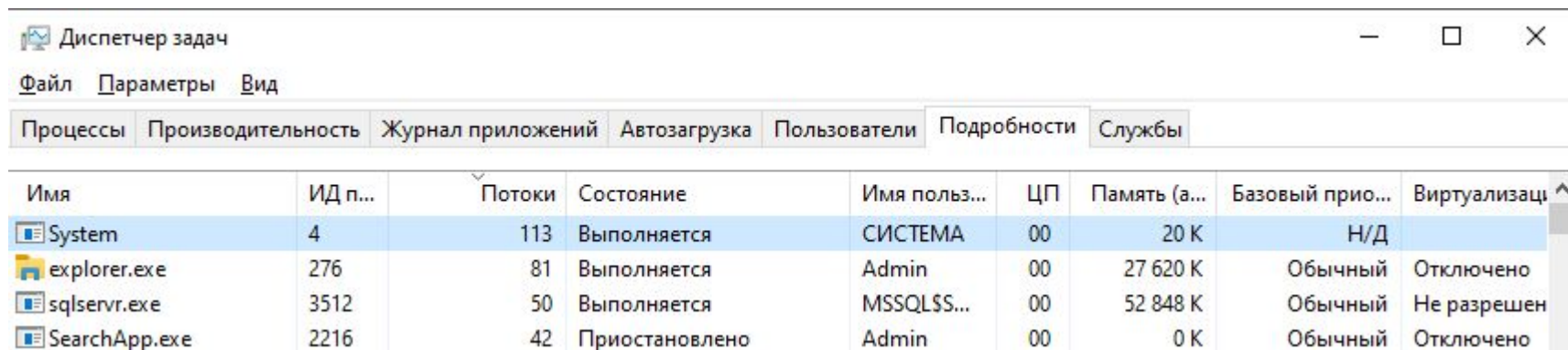
Имя	ИД п...	Потоки	Состояние
Системные прерыван...	-	-	Выполняется
Бездействие системы	0	2	Выполняется
YourPhone.exe	5480	11	Приостановлено



# 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 необходимая им динамическая память выделяется из куч памяти операционной системы, например из **пула подкачиваемых или неподкачиваемых страниц**

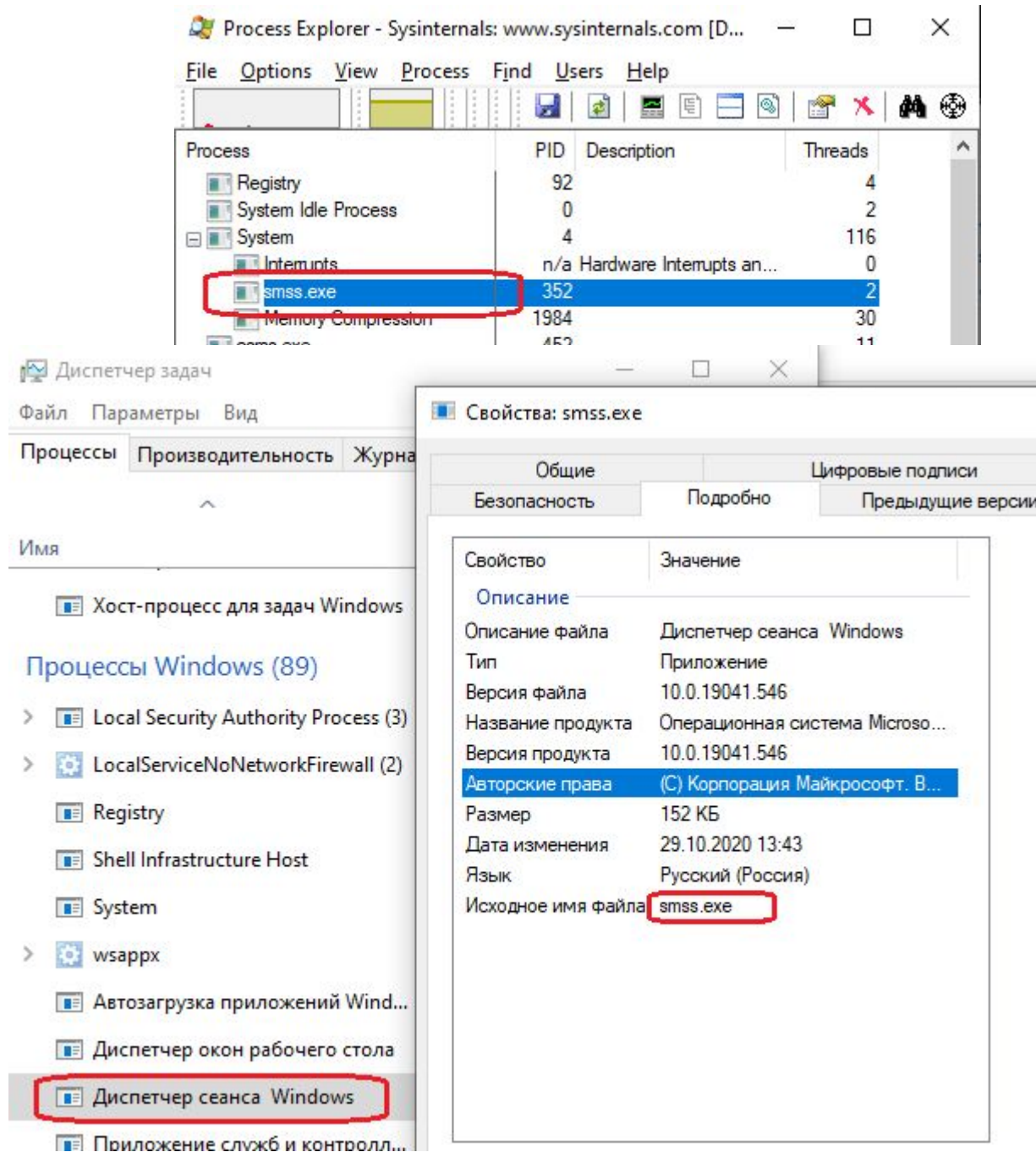


Имя	ИД п...	Потоки	Состояние	Имя польз...	ЦП	Память (а...	Базовый прио...	Виртуализац
System	4	113	Выполняется	СИСТЕМА	00	20 К	Н/Д	
explorer.exe	276	81	Выполняется	Admin	00	27 620 К	Обычный	Отключено
sqlservr.exe	3512	50	Выполняется	MSSQLSS...	00	52 848 К	Обычный	Не разрешен
SearchApp.exe	2216	42	Приостановлено	Admin	00	0 К	Обычный	Отключено



# 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

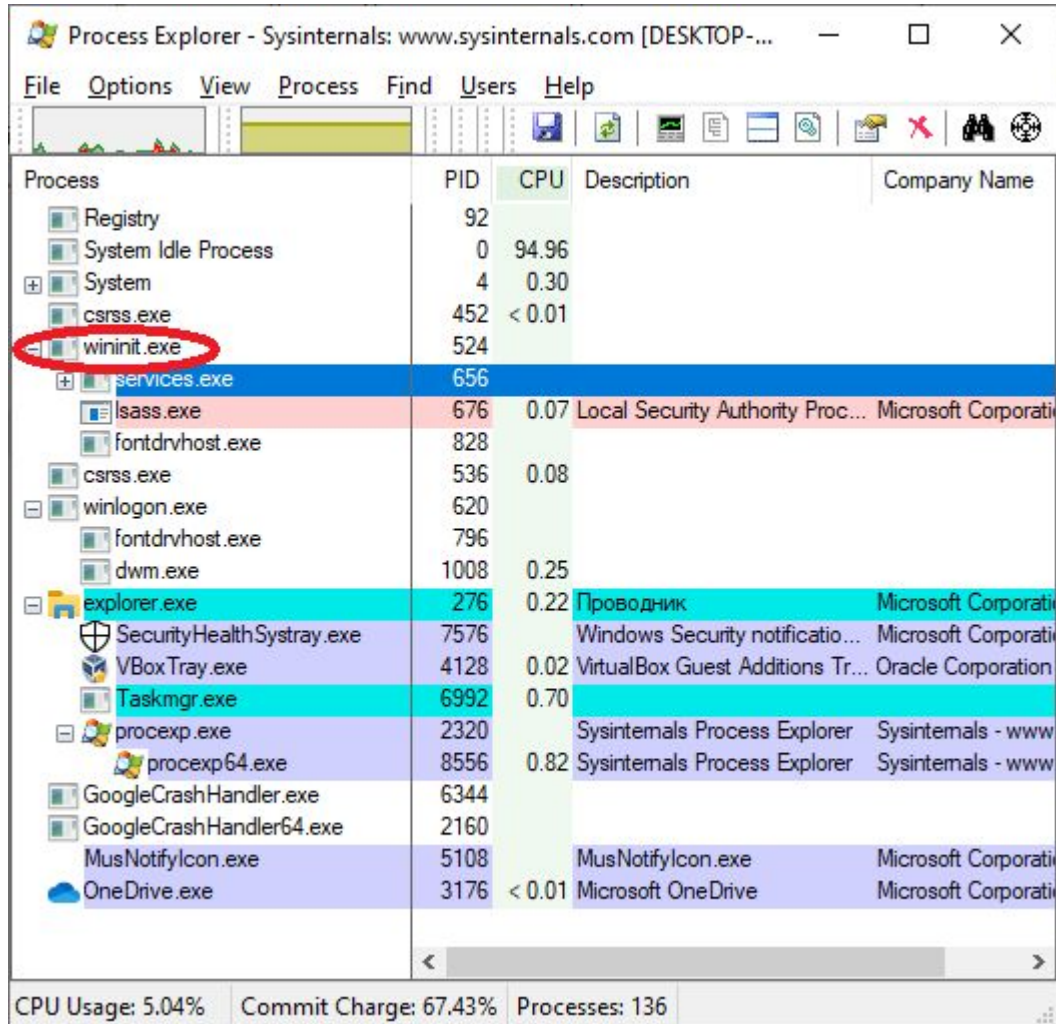


The image shows two screenshots from a Windows system. The top screenshot is a window titled "Process Explorer - Sysinternals: www.sysinternals.com [D...". It displays a list of processes with columns for Process, PID, Description, and Threads. The process "smss.exe" is highlighted in blue and circled in red. The bottom screenshot is a window titled "Свойства: smss.exe" (Properties: smss.exe). It shows the "Общие" (General) tab with a list of file properties. The "Авторские права" (Copyright) property is highlighted in blue, and the "Исходное имя файла" (Original filename) property is circled in red.

Process	PID	Description	Threads
Registry	92		4
System Idle Process	0		2
System	4		116
Interrupts	n/a	Hardware Interrupts an...	0
<b>smss.exe</b>	<b>352</b>		<b>2</b>
Memory Compression	1984		30
csrss.exe	452		11

Свойство	Значение
<b>Описание</b>	
Описание файла	Диспетчер сеанса Windows
Тип	Приложение
Версия файла	10.0.19041.546
Название продукта	Операционная система Microso...
Версия продукта	10.0.19041.546
<b>Авторские права</b>	<b>(C) Корпорация Майкрософт. В...</b>
Размер	152 КБ
Дата изменения	29.10.2020 13:43
Язык	Русский (Россия)
Исходное имя файла	<b>smss.exe</b>

# Процесс инициализации Wininit



The screenshot shows the Process Explorer window with the following data:

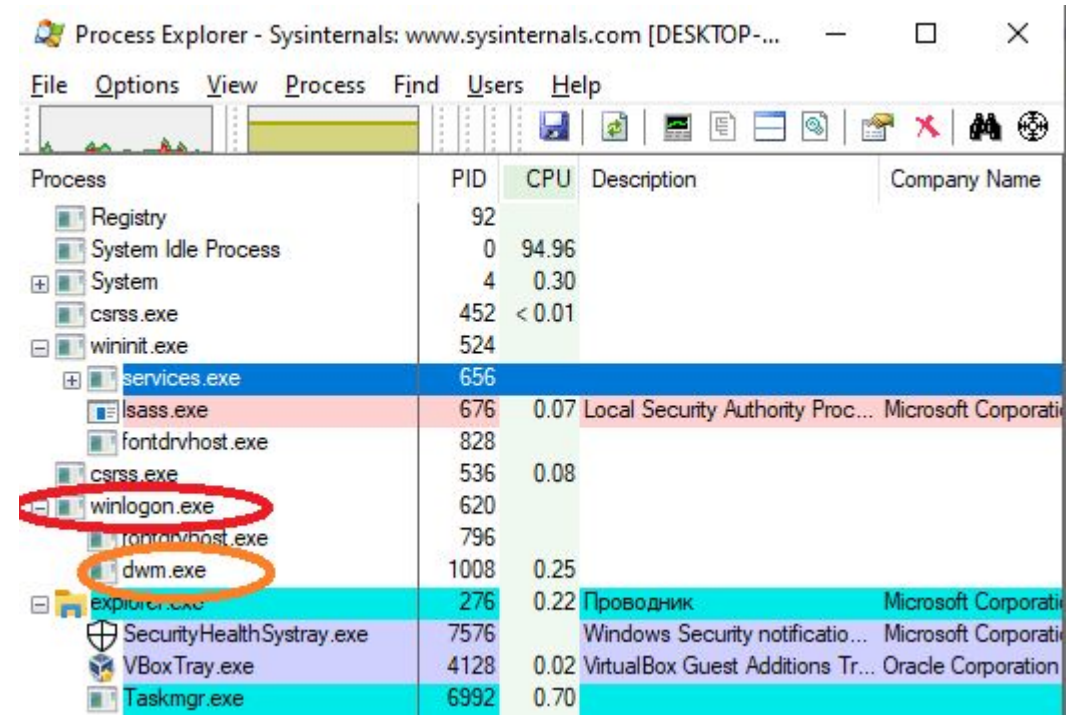
Process	PID	CPU	Description	Company Name
Registry	92			
System Idle Process	0	94.96		
System	4	0.30		
csrss.exe	452	< 0.01		
<b>wininit.exe</b>	524			
services.exe	656			
lsass.exe	676	0.07	Local Security Authority Proc...	Microsoft Corporati
fontdrvhost.exe	828			
csrss.exe	536	0.08		
winlogon.exe	620			
fontdrvhost.exe	796			
dwm.exe	1008	0.25		
explorer.exe	276	0.22	Проводник	Microsoft Corporati
SecurityHealthSystray.exe	7576		Windows Security notificatio...	Microsoft Corporati
VBoxTray.exe	4128	0.02	VirtualBox Guest Additions Tr...	Oracle Corporation
Taskmgr.exe	6992	0.70		
procexp.exe	2320		Sysinternals Process Explorer	Sysinternals - www
procexp64.exe	8556	0.82	Sysinternals Process Explorer	Sysinternals - www
GoogleCrashHandler.exe	6344			
GoogleCrashHandler64.exe	2160			
MusNotifylcon.exe	5108		MusNotifylcon.exe	Microsoft Corporati
OneDrive.exe	3176	< 0.01	Microsoft OneDrive	Microsoft Corporati

At the bottom of the window, the status bar shows: CPU Usage: 5.04%, Commit Charge: 67.43%, Processes: 136.

- 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.



Process	PID	CPU	Description	Company Name
Registry	92			
System Idle Process	0	94.96		
System	4	0.30		
csrss.exe	452	< 0.01		
wininit.exe	524			
services.exe	656			
lsass.exe	676	0.07	Local Security Authority Proc...	Microsoft Corporati
fontdrvhost.exe	828			
csrss.exe	536	0.08		
winlogon.exe	620			
fontdrvhost.exe	796			
dwm.exe	1008	0.25		
explorer.exe	276	0.22	Проводник	Microsoft Corporati
SecurityHealthSystray.exe	7576		Windows Security notificatio...	Microsoft Corporati
VBoxTray.exe	4128	0.02	VirtualBox Guest Additions Tr...	Oracle Corporation
Taskmgr.exe	6992	0.70		

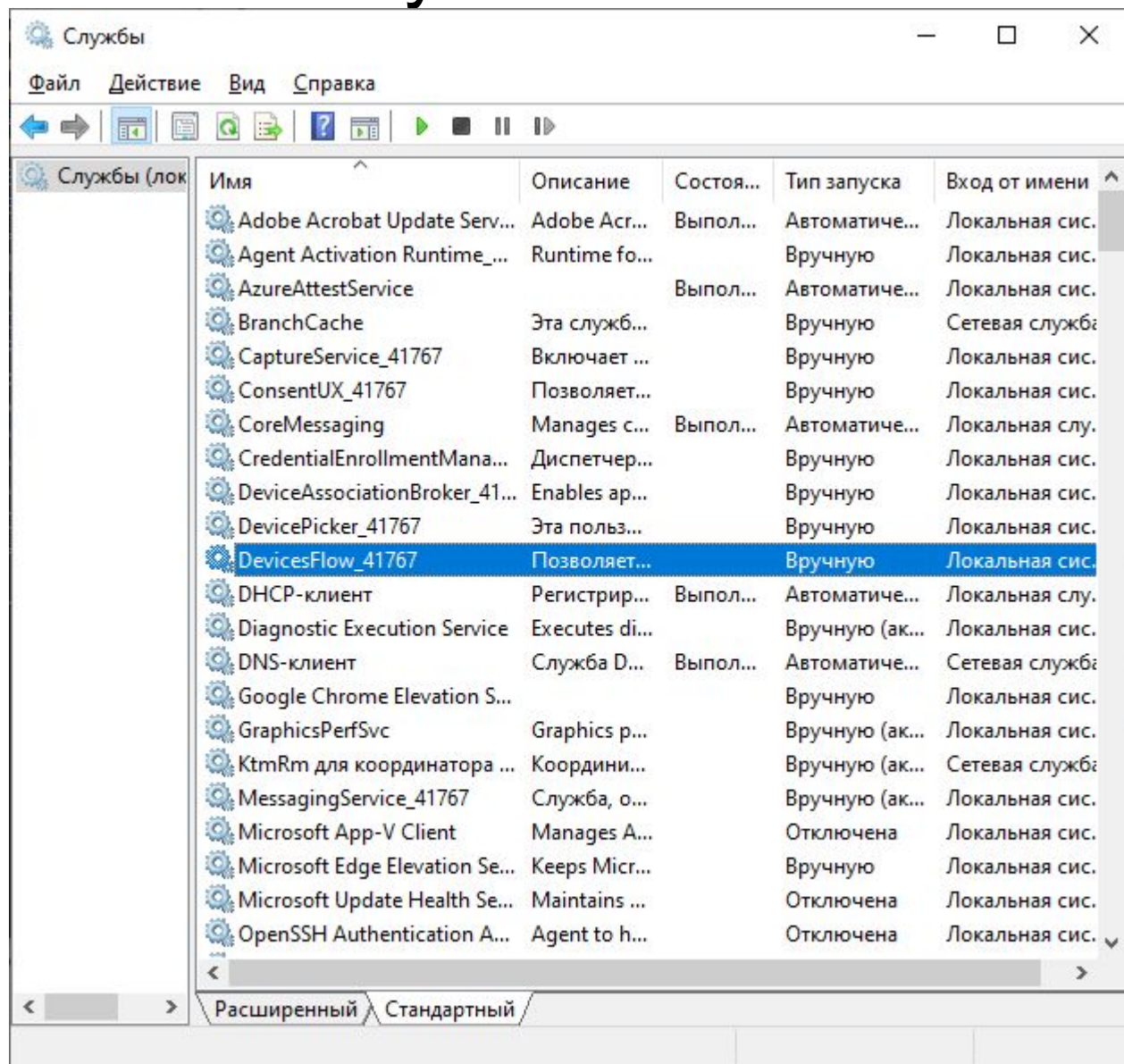




# Winlogon, LSASS и Userinit

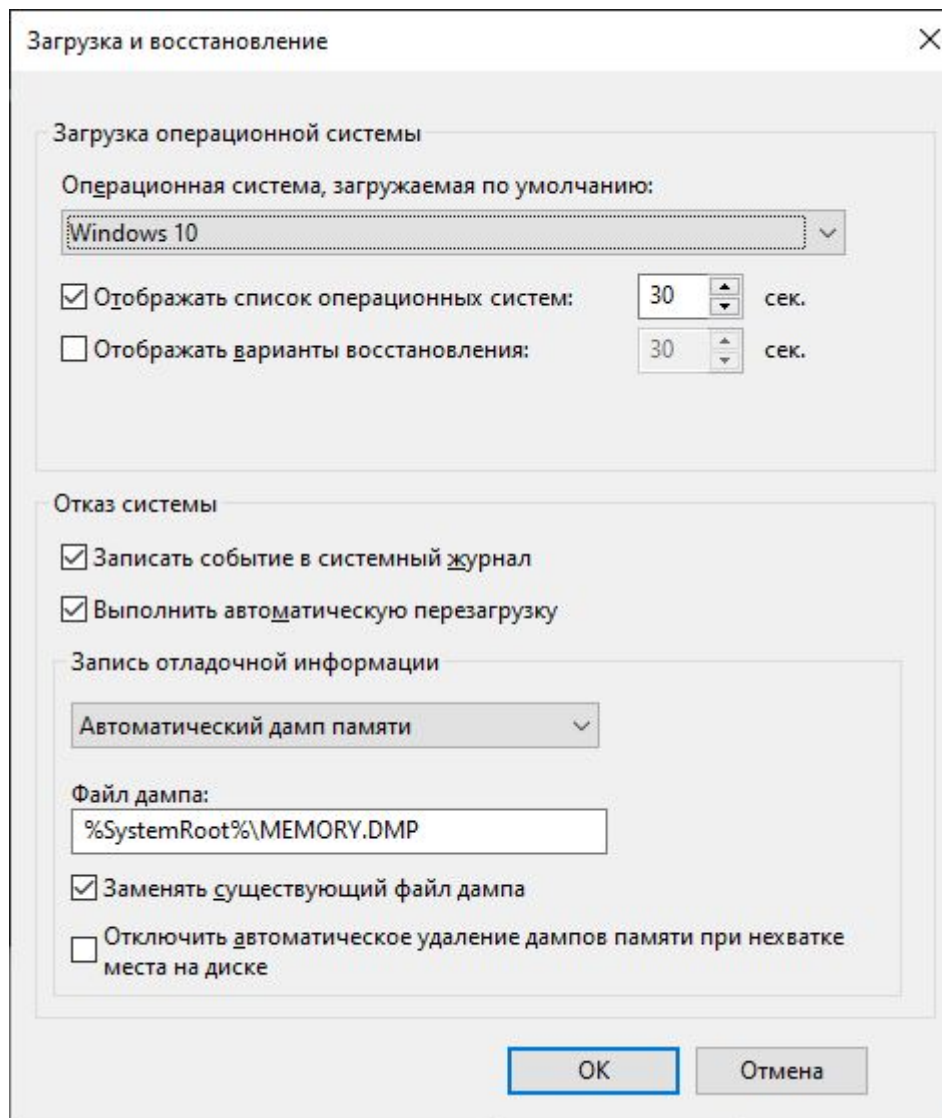
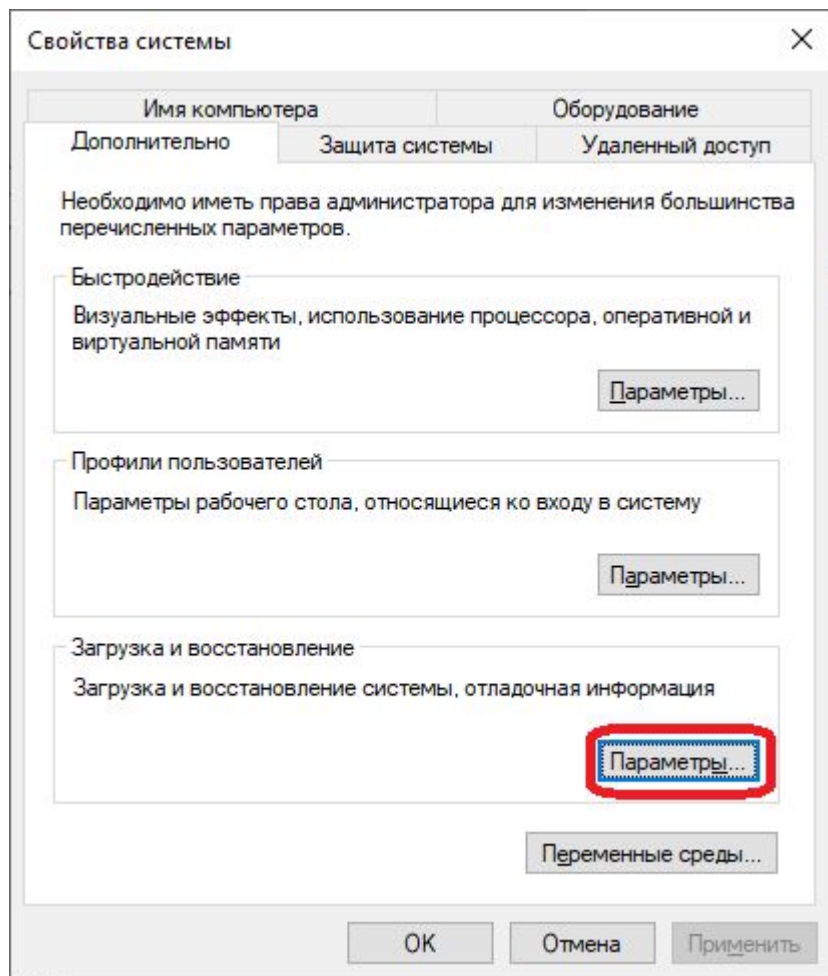
- LogonUI — дочерний процесс с вызовом пользовательского интерфейса входа в систему
- LogonUI отсылает информацию LSASS, который вызывает пакет аутентификации — AD или SAM
- Запускает исходный процесс пользовательского сеанса
- HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon, по умолчанию Userinit.exe, 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

## Переменные среды

### Переменные среды пользователя для Admin

Переменная	Значение
OneDrive	C:\Users\Admin\OneDrive
Path	C:\Users\Admin\AppData\Local\Microsoft\WindowsApps;C:\Users\Admin\AppData\Local\Microsoft\WindowsApps
QT_DEVICE_PIXEL_RATIO	auto
TEMP	C:\Users\Admin\AppData\Local\Temp
TMP	C:\Users\Admin\AppData\Local\Temp

Создать... Изменить... Удалить

### Системные переменные

Переменная	Значение
ComSpec	C:\Windows\system32\cmd.exe
DriverData	C:\Windows\System32\Drivers\DriverData
NUMBER_OF_PROCESSORS	2
OS	Windows_NT
Path	C:\Program Files (x86)\Embarcadero\Studio\20.0\bin;C:\Users\Admin\AppData\Local\Microsoft\WindowsApps;C:\Users\Admin\AppData\Local\Microsoft\WindowsApps
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE	AMD64

Создать... Изменить... Удалить

OK Отмена

```
Выбрать C:\Windows\system32\cmd.exe
(c) Корпорация Майкрософт (Microsoft Corporation), 2020. Все права защищены.

C:\Users\Admin>set
ALLUSERSPROFILE=C:\ProgramData
APPDATA=C:\Users\Admin\AppData\Roaming
CommonProgramFiles=C:\Program Files\Common Files
CommonProgramFiles(x86)=C:\Program Files (x86)\Common Files
CommonProgramW6432=C:\Program Files\Common Files
COMPUTERNAME=DESKTOP-90L788C
ComSpec=C:\Windows\system32\cmd.exe
DriverData=C:\Windows\System32\Drivers\DriverData
HOMEDRIVE=C:
HOMEPATH=\Users\Admin
LOCALAPPDATA=C:\Users\Admin\AppData\Local
LOGONSERVER=\\DESKTOP-90L788C
NUMBER_OF_PROCESSORS=2
OneDrive=C:\Users\Admin\OneDrive
OneDriveConsumer=C:\Users\Admin\OneDrive
OS=Windows_NT
Path=C:\Program Files (x86)\Embarcadero\Studio\20.0\bin;C:\Users\Public\Documents\Embarcadero\Studio\20.0\Bpl;C:\Program Files (x86)\Embarcadero\Studio\20.0\bin64;C:\Users\Public\Documents\Embarcadero\Studio\20.0\Bpl\Win64;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\System32\OpenSSH\;C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\170\Tools\Binn\;C:\Program Files (x86)\Microsoft SQL Server\150\Tools\Binn\;C:\Program Files\Microsoft SQL Server\150\Tools\Binn\;C:\Program Files\Microsoft SQL Server\150\DTS\Binn\;C:\Program Files\Microsoft SQL Server\150\DTS\Binn\;C:\Program Files\dotnet\;C:\Program Files\Microsoft SQL Server\130\Tools\Binn\;C:\Users\Admin\AppData\Local\Microsoft\WindowsApps;C:\Users\Admin\dotnet\tools
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
PROCESSOR_ARCHITECTURE=AMD64
PROCESSOR_IDENTIFIER=Intel64 Family 6 Model 60 Stepping 3, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=3c03
ProgramData=C:\ProgramData
ProgramFiles=C:\Program Files
ProgramFiles(x86)=C:\Program Files (x86)
ProgramW6432=C:\Program Files
PROMPT=$P$G
PSModulePath=C:\Program Files\WindowsPowerShell\Modules;C:\Windows\system32\WindowsPowerShell\v1.0\Modules;C:\Program Files (x86)\Microsoft SQL Server\150\Tools\PowerShell\Modules
PT7HOME=C:\Program Files\Cisco Packet Tracer 7.3.1
PUBLIC=C:\Users\Public
QT_DEVICE_PIXEL_RATIO=auto
SESSIONNAME=Console
SystemDrive=C:
SystemRoot=C:\Windows
TEMP=C:\Users\Admin\AppData\Local\Temp
TMP=C:\Users\Admin\AppData\Local\Temp
USERDOMAIN=DESKTOP-90L788C
USERDOMAIN_ROAMINGPROFILE=DESKTOP-90L788C
USERNAME=Admin
USERPROFILE=C:\Users\Admin
windir=C:\Windows
```