



Те, кто регулярно работает в операционной системы Windows, могли обращать внимание, на тот факт, что основную массу файлов операционной системы занимают файлы в формате * .dll (Dynamic Link Library).

Эти файлы могут быть расположены в каждой папке приложения, и используются для хранения фрагментов логики приложения, кроме того эти библиотеки могут быть доступны из разных приложений.

Как правило нет никакого способа непосредственного запуска файлов DLL. Для этого в операционной системы Windows используется rundll32.exe приложение, которое выполняется запуск функций, хранящейся в общих DLL-файлах. Этот исполняемый файл является неотъемлемой частью Windows, и, как правило, не должен быть угрозой.

Примечание: исполняемый файл обычно находится в каталоге:

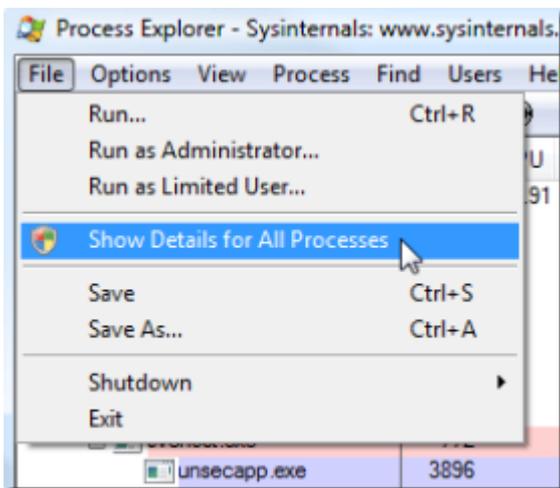
`C:\Windows\System32\rundll32.exe`

Но иногда шпионское программное обеспечение использует такое же имя файла (rundll32.exe) и/или запускается из другой директории для того, чтобы замаскировать себя. Если есть подозрение, что выполняются неизвестные программы, то необходимо выполнить детальную проверку запускаемых процессов, чтобы убедиться в правомерности запускаемого программного обеспечения.

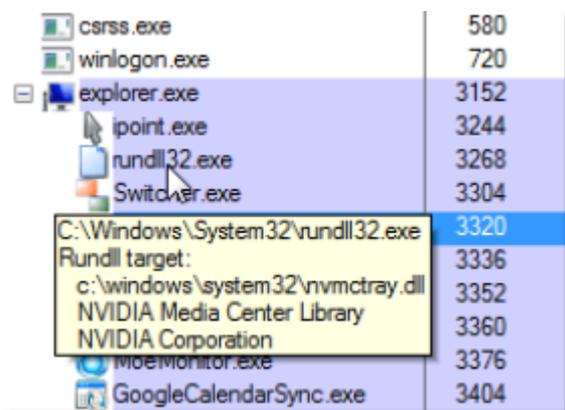
Здесь стоит обратить внимание на тот факт, что зачастую используется системный файл rundll32.exe, но при этом запускаемые им библиотеки, могут быть неизвестного происхождения, что бывает не так очевидно при первом взгляде на процессы в диспетчере задач Windows.

Вместо того чтобы использовать Task Manager (стандартный диспетчер задач), мы скачаем бесплатную утилиту **Process Explorer**, разработанную Марком Руссиновичем и опубликованную на сайте Microsoft (<https://technet.microsoft.com/ru-ru/sysinternals/processexplorer.aspx>), чтобы выяснить, что происходит. Утилита имеет ряд преимуществ по сравнению со стандартной версией и является лучшим выбором для любой работы по устранению неполадок.

Просто запустите программу **Process Explorer**, далее в главном меню необходимо выбрать пункт File -> Show Details for All Processes, для отображения детальной информации о процессах. Скриншот ниже.

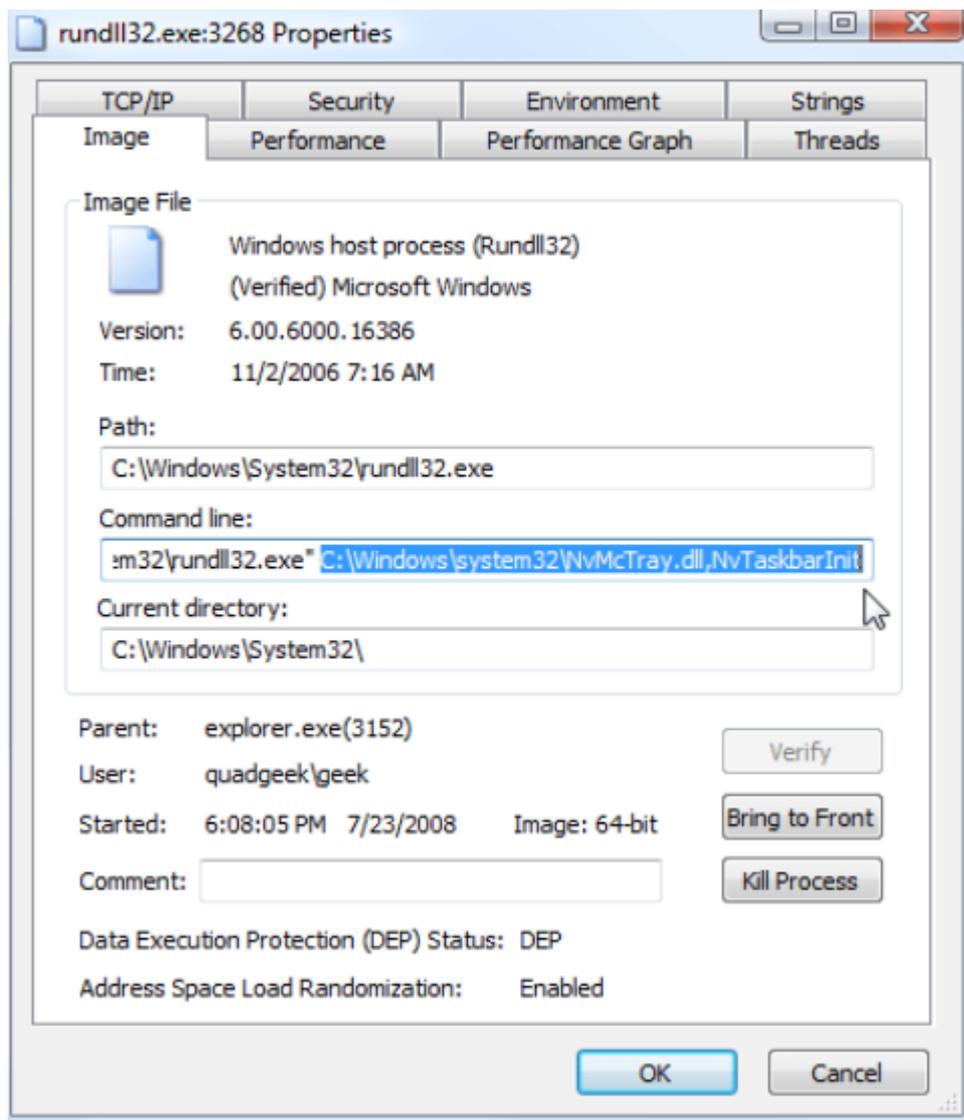


Теперь, когда вы наведете курсор мыши на rundll32.exe в списке процессов, вы увидите всплывающую подсказку с подробностями о том, что это на самом деле:



Или же вы можете щелкнуть правой кнопкой мыши, выберите **Properties** (Свойства), а затем посмотрите на вкладке **Image**, чтобы увидеть полный путь к файлу, который в

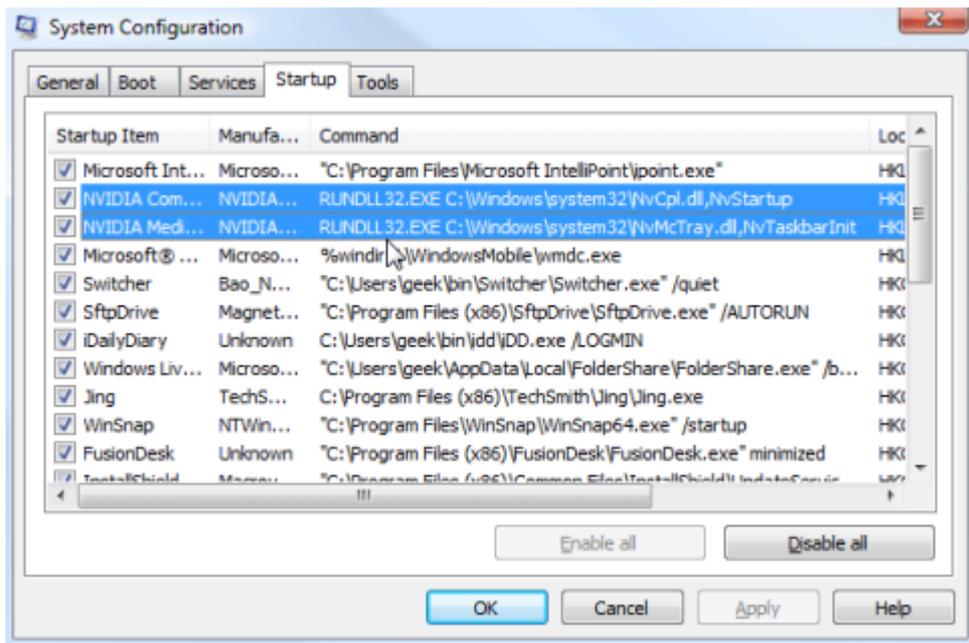
настоящее время запущен, и вы даже можете увидеть процесс Родитель, который в данном случае является оболочкой для Windows (explorer.exe), что свидетельствует о том, что он, вероятно, запускается с ярлыка или из раздела автозапуска.



В конце этой статьи можно посмотреть сведения о файле так же, как мы это делали в разделе менеджера задач выше. В моем случае файл - это часть панели управления NVIDIA, и поэтому я не собираюсь ничего с ним делать.

Как отключить процесс Rundll32 (Windows 7)

Для отключения процесса в операционной системе Windows 7, достаточно запустить из командной строки утилиту msconfig.exe.



Далее необходимо перейти к вкладке Startup (Автозагрузка) и далее найти нужный процесс в колонке Command, которая должна быть такой же, как поле "Командная строка" в окне Process Explorer.

Просто снимите флажок, чтобы предотвратить его автоматический запуск при следующей загрузке системы.

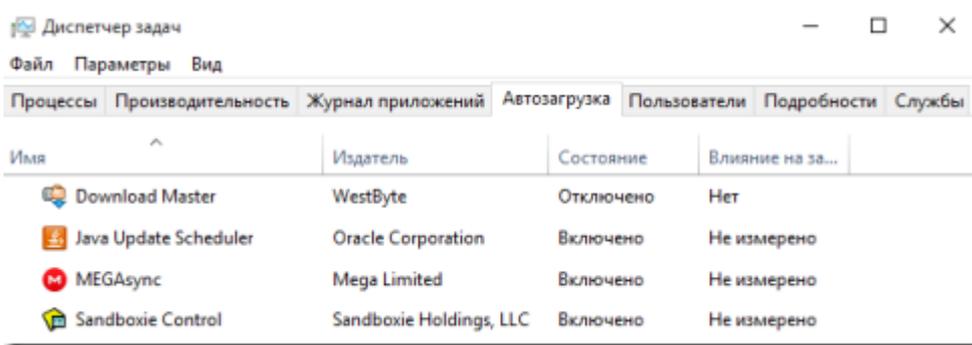
Иногда процесс фактически не имеет элемента в автозагрузки, в этом случае придется выполнить поиск запускаемого файла например в реестре.

Об использовании сторонней утилиты, для поиска проблемных файлов автозапуска, я напишу в завершении этой статьи.

Как отключить процесс Rundll32 (Windows 8 или 10)

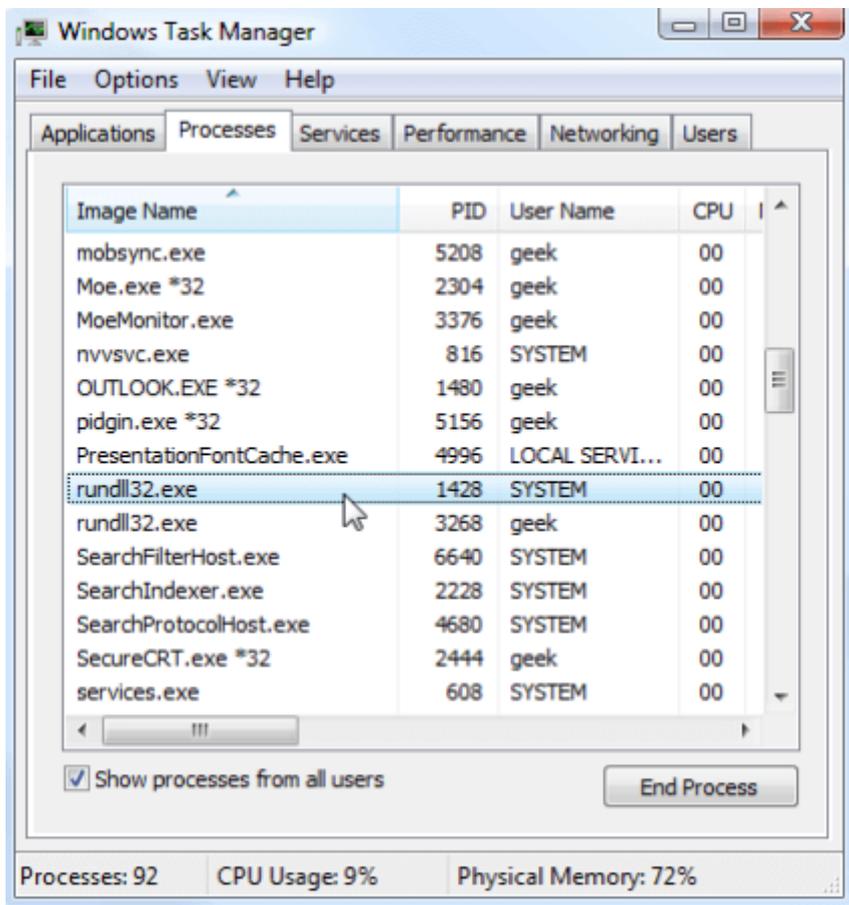
Если вы используете Windows 8 или 10, вы можете использовать раздел Автозагрузка

диспетчера задач, для проверки состояния и отключения приложений, выполняющих запуск при загрузке операционной системы.



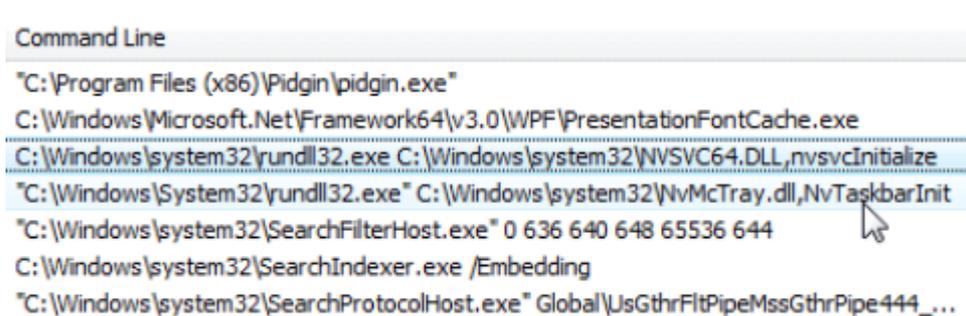
Использование диспетчера задач (Windows 7)

Одной из главных особенностей диспетчера задач (Task Manager) в Windows 7 или Vista, является возможность видеть полную командную строку для любого запущенного приложения. Например, вы увидите, что у меня есть два процесса rundll32.exe в моем списке задач на скриншоте ниже:



Если мы перейдем в ВидВыбор столбцов (ViewSelect columns), то в списке колонок увидим опцию "Командная строка" (Command Line), который хотим увидеть в диспетчере задач, ставим соответствующую галочку.

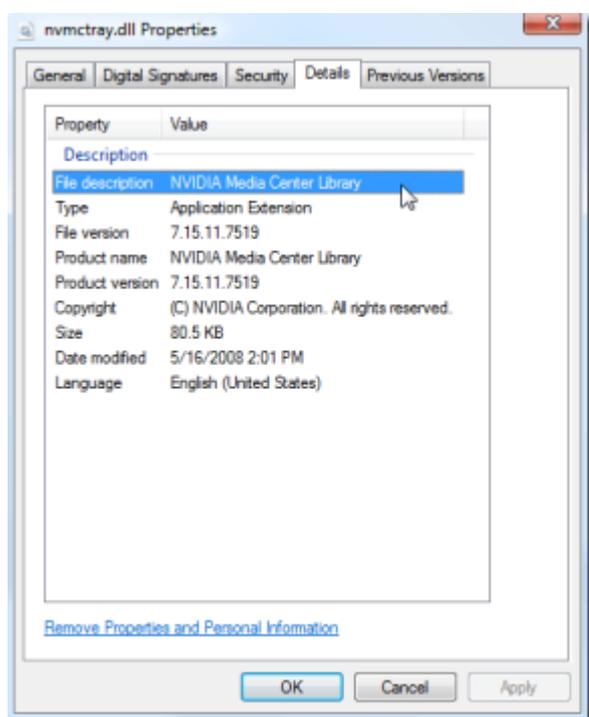
Теперь в диспетчере задач можно увидеть полный путь к файлу в отдельной колонке. Это правильный путь для rundll32.exe в каталоге System32, а его аргумент путь к другой DLL, которая на самом деле работает в настоящий момент.



Если навести курсор мыши, то отобразится полный путь к файлу. Можно пойти по этому пути и убедиться, в том что библиотека *.dll запущенная с помощью rundll32.exe действительно принадлежит программе которую мы устанавливали ранее в системе.

Можно открыть Свойства библиотеки и посмотреть на детали

В противном случае, вы можете открыть Свойства и посмотреть на вкладке Подробно (Details) информацию о разработчике этого файла. Скриншот ниже.



Выяснив эти детали можно понять, стоит исключать данную библиотеку из автозагрузки или нет. Если вы не в курсе что это за библиотека, то в этом вам поможет Google.

Использование диспетчера задач (Windows 10)

Тем же функционалом, который присутствует в диспетчере задач в Windows 7 можно воспользоваться и в диспетчере задач в Windows 10.

Имя	ИД п...	Состояние	Имя польз...	ЦП	Память (ч...	Командная строка
SnippingTool.exe	3904	Выполняется	Wolf	01	2 580 K	"C:\Windows\system32\SnippingTool.exe"
spoolsv.exe	1420	Выполняется	СИСТЕМА	00	5 080 K	C:\Windows\System32\spoolsv.exe
sqlwriter.exe	1836	Выполняется	СИСТЕМА	00	1 068 K	"C:\Program Files\Microsoft SQL Server\90\Shared\sqlwriter.exe"
svchost.exe	4312	Выполняется	СИСТЕМА	00	972 K	C:\Windows\System32\svchost.exe -k swprv
svchost.exe	728	Выполняется	СИСТЕМА	00	4 308 K	C:\Windows\system32\svchost.exe -k DcomLaunch
svchost.exe	784	Выполняется	NETWORK...	00	3 700 K	C:\Windows\system32\svchost.exe -k RPCSS
svchost.exe	932	Выполняется	СИСТЕМА	00	13 932 K	C:\Windows\system32\svchost.exe -k netsvcs
svchost.exe	288	Выполняется	СИСТЕМА	00	8 276 K	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted
svchost.exe	324	Выполняется	LOCAL SE...	00	2 232 K	C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation
svchost.exe	456	Выполняется	LOCAL SE...	00	10 012 K	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted
svchost.exe	768	Выполняется	LOCAL SE...	00	5 160 K	C:\Windows\system32\svchost.exe -k LocalService
svchost.exe	1260	Выполняется	NETWORK...	00	8 412 K	C:\Windows\system32\svchost.exe -k NetworkService
svchost.exe	1484	Выполняется	LOCAL SE...	00	11 024 K	C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
svchost.exe	1828	Выполняется	LOCAL SE...	00	1 352 K	C:\Windows\system32\svchost.exe -k imgsvc
svchost.exe	1856	Выполняется	СИСТЕМА	00	3 296 K	C:\Windows\system32\svchost.exe -k appmodel
svchost.exe	2312	Выполняется	NETWORK...	00	948 K	C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted
svchost.exe	5068	Выполняется	Wolf	00	1 468 K	C:\Windows\system32\svchost.exe -k UnistackSvcGroup
System	4	Выполняется	СИСТЕМА	00	28 K	
taskhostv.exe	1788	Выполняется	Wolf	00	2 032 K	taskhostv.exe (222A245B-E637-4AE9-AB3F-A59CA119A75E)
Taskmgr.exe	3640	Выполняется	Wolf	05	8 352 K	"C:\Windows\system32\taskmgr.exe" /4
VSSVC.exe	1088	Выполняется	СИСТЕМА	00	1 208 K	C:\Windows\system32\vssvc.exe
WindowsLiveWriter.exe	1896	Выполняется	Wolf	00	45 136 K	"C:\Program Files (x86)\Windows Live\Writer\WindowsLiveWriter.exe"
wininit.exe	512	Выполняется	СИСТЕМА	00	800 K	

Для подробного отображения сведений о текущих запущенных процессах, необходимо в диспетчере задач перейти во вкладку **"Подробности"**.

Для того, чтобы отображался столбец **"Командная строка"**, необходимо щелкнуть правой кнопкой мыши по соседнему столбцу и в контекстном меню пункт **"Выбрать столбцы"**, далее в списке необходимо выбрать пункт **"Командная строка"**, поставить галочку и нажать Ок. Результат представлен на скриншоте выше.

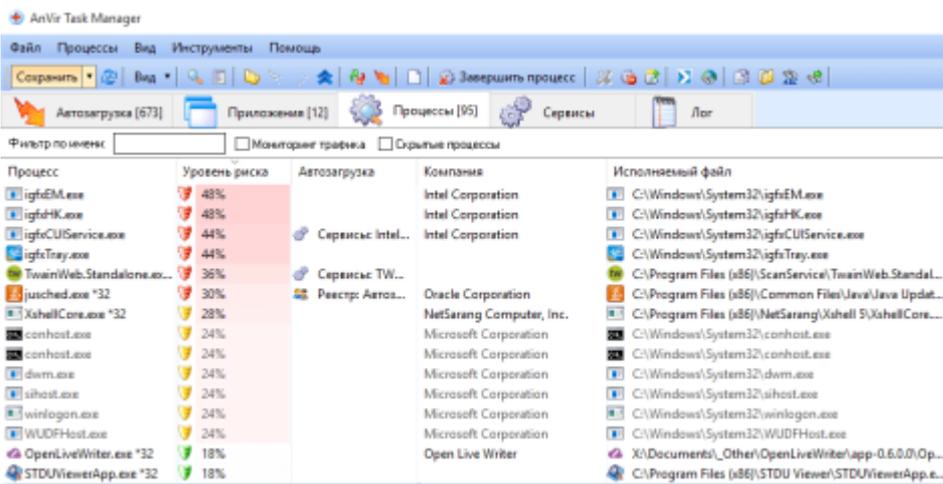
AnVir Task Manager

В завершении рассмотрения программ, обеспечивающих поиск неуставного программного обеспечения, нельзя не обратить внимание на еще один бесплатный, но полезный продукт AnVir Task Manager, который обладает следующими функциями:

- Управление автозагрузкой, запущенными процессами, сервисами и драйверами,
- Обнаружение и удаление вирусов и шпионов, блокирование попыток заразить систему,
- Может заменять стандартный Диспетчера Задач.

Данная программа доступна для загрузки с сайта <http://www.anvir.net>. Одной из особенностей AnVir является поиск всего автоматически запускаемого программного обеспечения в операционной системе Windows. В главном окне программы показаны названия процессов, степень их риска, где определен механизм автозапуска (например в реестре или в качестве системного сервиса), указана информация о

разработчике, и путь к файлу.



Как правило из всего программного обеспечения указанного выше, в части управления процессами, AnVir можно считать лидером. AnVir обладает не только удобным в т.ч. русскоязычным интерфейсом, но позволяем достаточно гибко управлять процессами запуска различного ПО. Поэтому при исследовании запущенных процессов, я бы рекомендовал начинать с **AnVir**, и потом в дополнение использовать **Process Explorer**.