





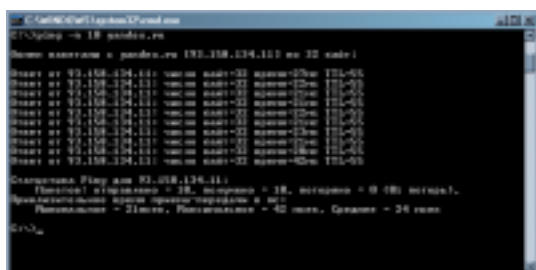
имени в IP.

Попробуем разобраться, почему это происходит. Ни для кого не секрет, что при попытке расшифровки имени, **DNS-client** компьютера обращается изначально к кешу **DNS**, в котором информация о предыдущих преобразованиях хранится некоторое время. Это время задается либо в записи **SOA** для всего доменного имени, либо отдельно для каждой зоны (для **MX-записи** может быть одно, для **A-записи** - другое...). Запись в файле **hosts** это время делает бесконечно большим, т.е. эта запись хранится постоянно и не изменяется.

## Отображение и очистка кеша DNS

Попробуем более подробно разобраться, что такое кеш **DNS**. Это информация, о соответствии **IP-адрес<-> имя**, которая хранится в памяти устройства. Для чего это нужно? Рассмотрим на простом примере... Воспользуемся утилитой **ping**, которая посылает **ICMP-пакеты** "поверх" **IP-протокола**, и получает их обратно (при этом используются различные метки).

Однако, когда даем команду "**ping yandex.ru**", компьютер должен сначала выполнить преобразование **DNS-имени yandex.ru** в **IP-адрес 93.158.134.11**. Кеш **DNS** нужен для того, чтобы каждый раз не делать запросов на разрешение доменного имени в **IP-адрес** заново.



[3]

Если выполнить команду **ping**, как в примере, то если бы не было кеша DNS, процедуру преобразование **DNS-имени yandex.ru** в **IP-адрес** необходимо было бы выполнить 10 раз. Также стоит иметь ввиду, что **DNS-сервера** провайдера тоже кешируют информацию на период времени, указанный в **SOA-записи** домена.

Для просмотра локального **DNS-кеша** на компьютере под управлением **OS Windows** воспользуемся командой **ipconfig** с ключем **displaydns**:

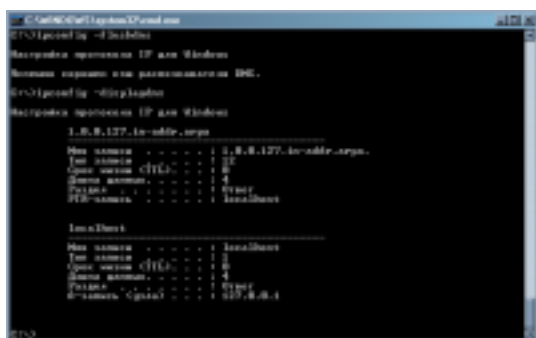


[4]

Этот список и есть локальный DNS-кеш, где параметр "**Срок жизни**" - это время в секундах, которое запись еще будет храниться.



Чтобы сбросить кеш, необходимо использовать ключ **flushdns**. После выполнения "**ipconfig -flushdns**" будет сброшен весь кеш DNS, исключая записи, указанные в файле **hosts**.



```
С:\Windows\System32\cmd.exe
C:\>ipconfig /flushdns

Настройка протокола IP для Windows
Выполнение операции или разблокировка DNS.
C:\>ipconfig /flushdns

Настройка протокола IP для Windows
1. E. B. 127. 0. 0. 1 -> 127. 0. 0. 1
Местная ссылка -> -> -> 1 127. 0. 0. 1
Гипер-ссылка -> -> -> 2 0
Данные протокола -> -> -> 4
Ссылка -> -> -> 1 127. 0. 0. 1
Имя хоста -> -> -> 1 localhost

Таблица 1
Местная ссылка -> -> -> 1 localhost
Гипер-ссылка -> -> -> 2 0
Данные протокола -> -> -> 4
Ссылка -> -> -> 1 127. 0. 0. 1
Имя хоста -> -> -> 1 127. 0. 0. 1
```

[5]

### Что это нам дает?

Озникотившись с информацией, необходимо взять ее "на вооружение". В основном возможность использования файла **hosts** пригодится веб-мастерам и системным администраторам. Довольно удобно использовать файл **hosts** при переносе хостинга или других операциях, где необходимо эмулировать запросы к **DNS-имени**.

Также стоит иметь ввиду, что в файл **hosts** довольно часто добавляют информацию вредоносные программы, блокируя доступ к сайтам обновлений антивирусных программ. Так что, если антивирус не обновляется - проверьте первым делом файл **hosts**.

### Источник (получено 2026-04-07 05:28):

<http://muff.kiev.ua/content/hosts-nemnogo-informatsii-o-faile-hosts>

### Ссылки:

- [1] <http://ru.wikipedia.org/wiki/DNS>
- [2] <http://muff.kiev.ua/files/imagepicker/1/hosts00.png>
- [3] <http://muff.kiev.ua/files/imagepicker/1/hosts01.png>
- [4] <http://muff.kiev.ua/files/imagepicker/1/hosts02.png>
- [5] <http://muff.kiev.ua/files/imagepicker/1/hosts03.png>