Три способа сбросить пароль в Windows 7: простой, сложный и неправильн

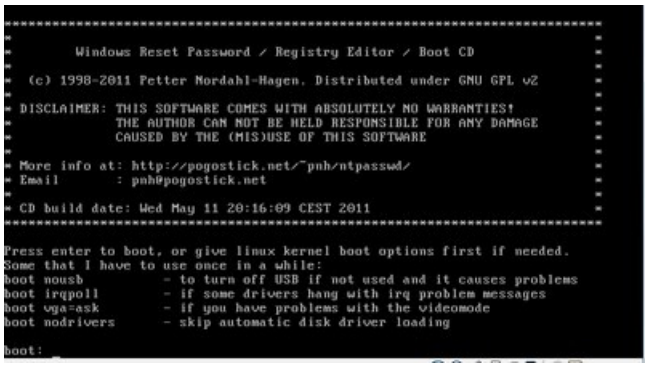
Автор: Игорь Осколков
Дата: 26.01.2012

Пароли, а особенно безопасные (читай сложные) имеют неприятное свойство — они легко забываются. Ну или чаще всего просто теряется бумажка с этим самым паролем. Ситуация, в общем, типичная. Поэтому неплохо бы подготовиться к ней заранее и знать, как быстро сбросить или сменить пароль

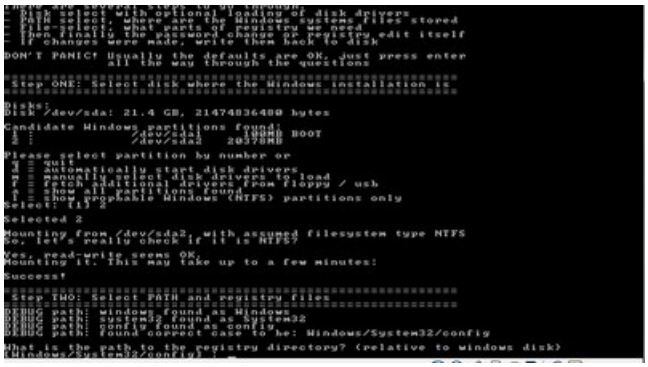
Напоминаем, что попытки повторить действия автора могут привести к потере гарантии на оборудование и даже к выходу его строя. Материал приведен исключительно в ознакомительных целях. Если же вы собираетесь воспроизводить действи описанные ниже, настоятельно советуем внимательно прочитать статью до конца хотя бы один раз. Редакция 3DNews не нес никакой ответственности за любые возможные последствия.

В Windows уже давно для хранения паролей всех пользователей и управления ими используется система SAM. Вся информация ней хорошо защищена, поэтому для того чтобы узнать пароль, придётся затратить кучу времени и ресурсов, особенно если достаточно сложный. Чаще всего, однако, вовсе не требуется именно узнать пароль — достаточно сбросить его или поменят Для этого разработано несколько утилит, одной из которых мы воспользуемся. Ещё один важный момент — очевидно, что, ког ОС запущена, она не позволит просто так влезать в хранилище паролей. Поэтому надо убедиться, что компьютер поддержива загрузку с CD/DVD- или USB-носителя, чтобы запустить нужные утилиты.

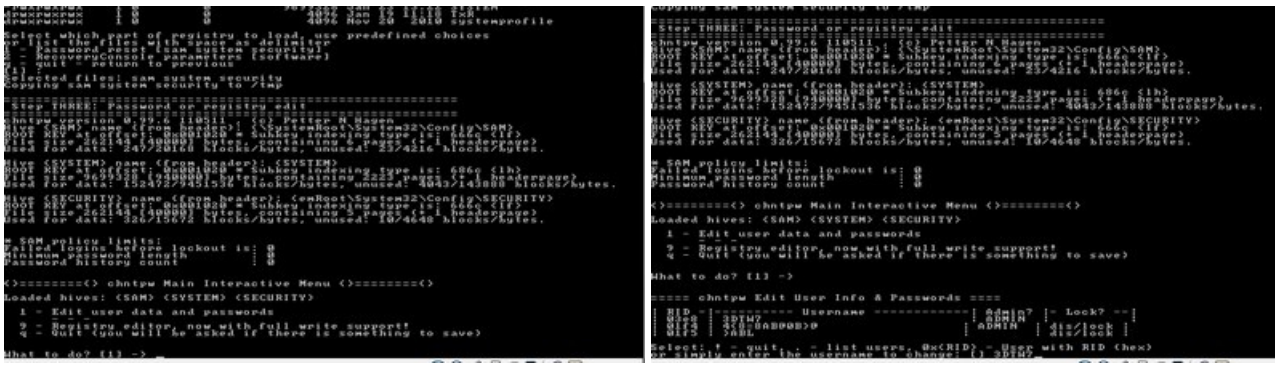
Самая известная из них — это Offline NT Password and Registry editor, которая умеет работать с паролями и реестром Windo XP/Vista/7. Скачайте USB- или CD-версию утилиты, запишите загруженный образ на диск или воспользуйтесь нашими советам по созданию мультизагрузочной флешки. Утилита не имеет графического интерфейса, но пугаться этого не стоит — всё в н довольно просто и понятно. К тому же часто нужная опция предлагается по умолчанию, так что от вас потребуется толь нажать клавишу Enter.



Загрузитесь со съёмного носителя Offline NT Password and Registry editor. Вам вряд ли понадобятся дополнительные опц загрузки, но в некоторых случаях придётся опытным путём подобрать те, которые помогут утилите запуститься. На следующ этапе надо выбрать номер раздела, на котором установлена Windows. Ориентироваться придётся в первую очередь по е размеру. В принципе, до самого последнего момента программа не вносит никаких изменений в Windows, поэтому в случ ошибки можно просто начать процедуру сброса пароля заново.




Затем утилита попросит указать путь до папки, где находятся файлы SAM (фактически это куст реестра). По умолчанию э *X:/Windows/System32/config*, его же и предлагает вначале программа. Потом надо выбрать первый пункт (Password reset), т как мы собрались сбросить пароль.



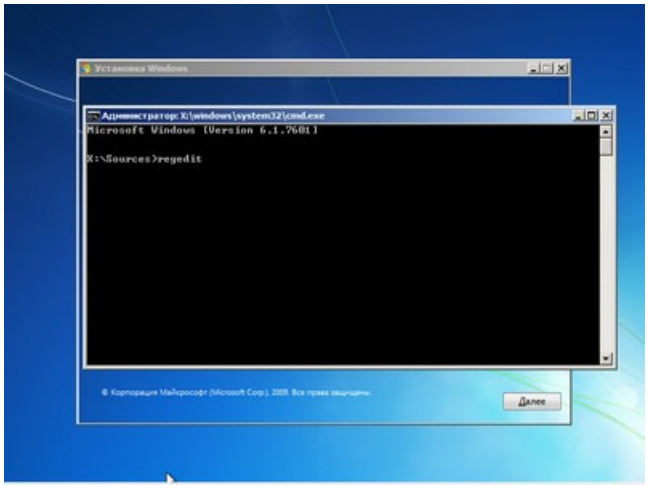
Дальше всё просто. Выбираем первый пункт (Edit user data and password) и вписываем имя пользователя или его идентификат в формате *0xabcd*, где *abcd* — это RID, указанный в первом столбце. RID пригодится, если имя пользователя некоррект отображается или его не получается ввести. Например, при использовании кириллицы.

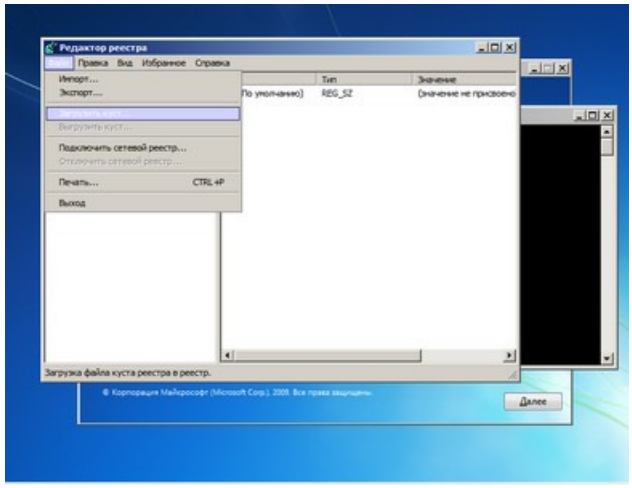
Осталось указать пункт 1 (сброс пароля) или 2 (смена пароля) для выбранного пользователя. Выходим из режи редактирования пароля, введя восклицательный знак и нажав Enter.

Всё, почти готово. Вводим *q*, нажимаем Enter, а затем соглашаемся с внесением изменений, введя *y* и ещё раз нажав Ente Отказываемся от дальнейшей работы в Offline NT Password and Registry editor (*n*), извлекаем флешку или CD-диск и нажима заветную комбинацию Alt+Ctrl+Del для перезагрузки. Готово — пароль сброшен!

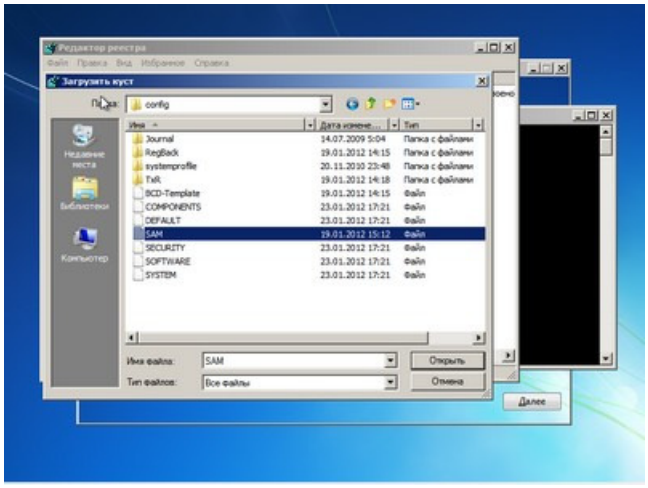
Это был простой способ сброса пароля Windows 7. Сложностей с ним быть не должно. Надо всего лишь быть внимательным аккуратным. Проблемы могут возникнуть только при отсутствии необходимых драйверов для работы с жёстким диском. Тог придётся закинуть их на дискету (если вы, конечно, найдёте живого представителя этого почти вымершего вида и рабоч привод для него) или на USB-флешку и на первом этапе выбрать пункт fetch additional drivers.

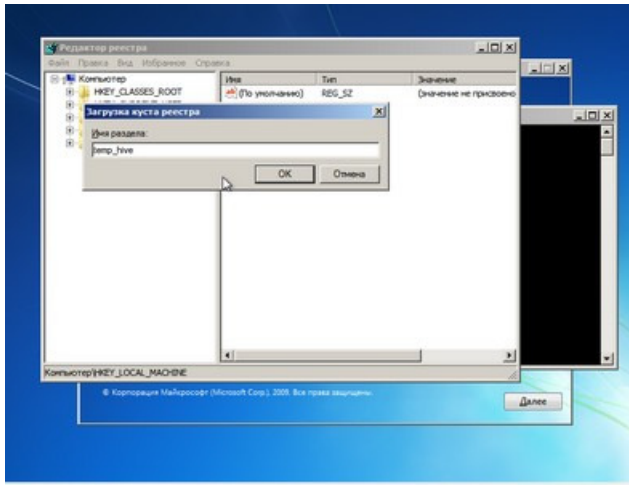
Для второго и третьего способов понадобится только установочный диск Windows 7 и больше ничего. Более сложный вариа подразумевает включение изначально скрытой учётной записи «Администратор» путём правки реестра из установочной сред Windows 7. В дальнейшем можно будет войти в систему под этой учёткой и отредактировать любой другой аккаунт в ОС. I умолчанию «Администратор» не имеет пароля, что только играет нам на руку.



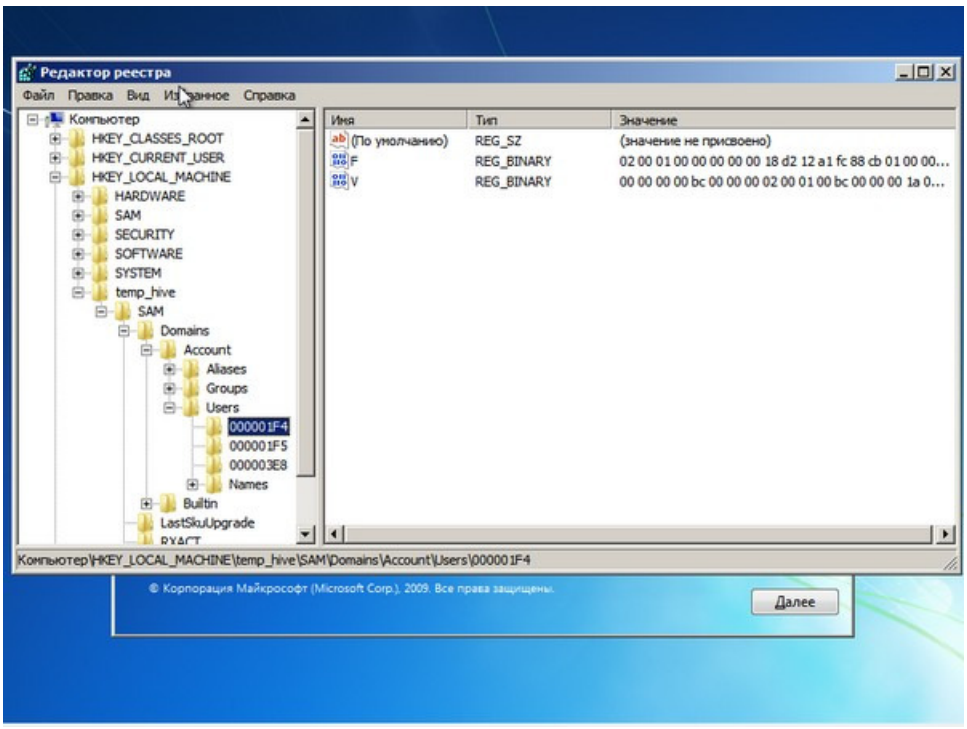


Итак, загружаемся с установочного диска и нажимаем Shift+F10 для вызова командной строки, где вбиваем *regedit* и жмём Ent для запуска редактора реестра.

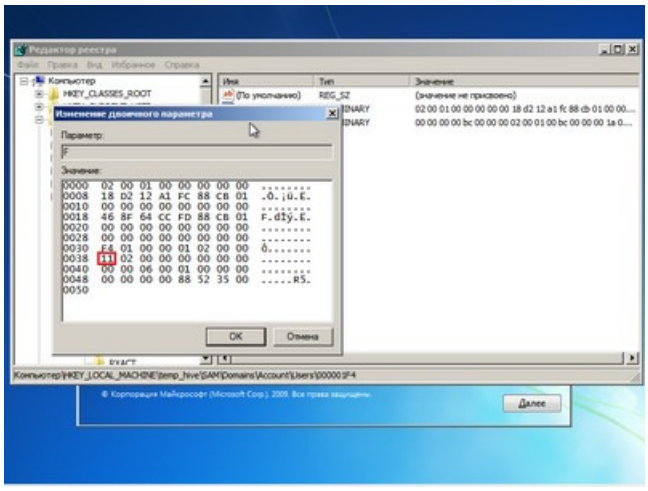


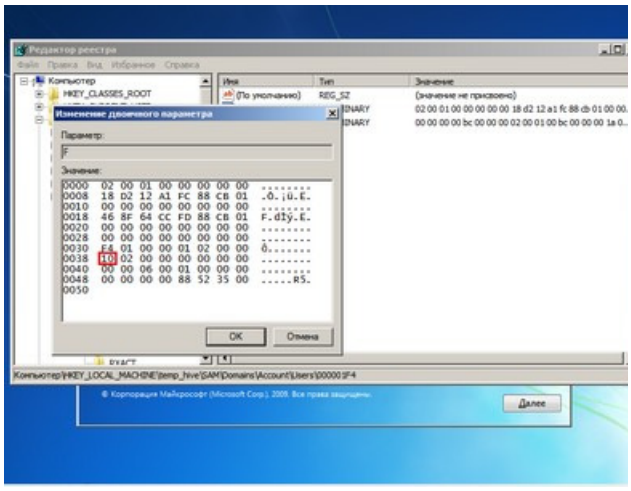


Выделяем раздел *HKEY_LOCAL_MACHINE*, а в меню выбираем «Файл» → «Загрузить куст…» (File → Load hive…). Нам на открыть файл SAM, который находится в папке *|Windows|System32|config* на том разделе, где установлена Windows 7. П открытии будет предложено ввести имя загружаемого куста — вбивайте любое.

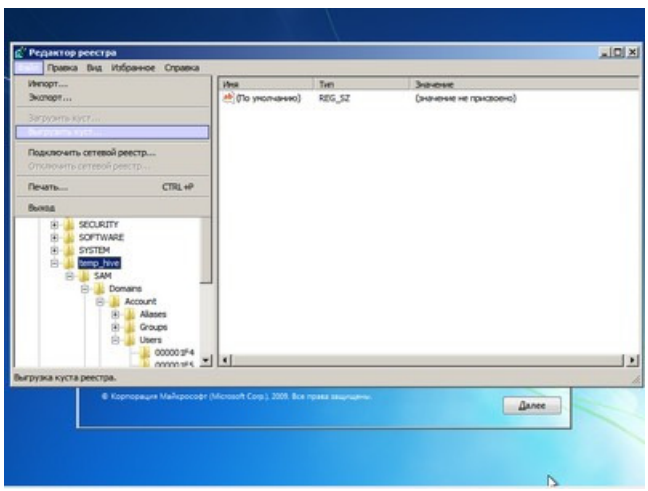


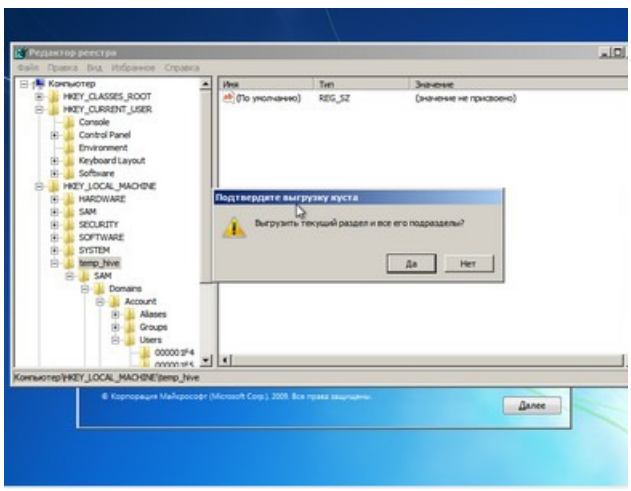
Теперь надо выбрать раздел *HKEY_LOCAL_MACHINE|имя_куста|SAM|Domains|Account|Users0001F4* и дважды кликнуть по клю *F*. Откроется редактор, в котором надо перейти к первому числу в строке 038 — это 11. Его надо изменить на 10. Будь аккуратны и не ошибитесь — поменять надо только его, не добавляя и не удаляя другие числа!



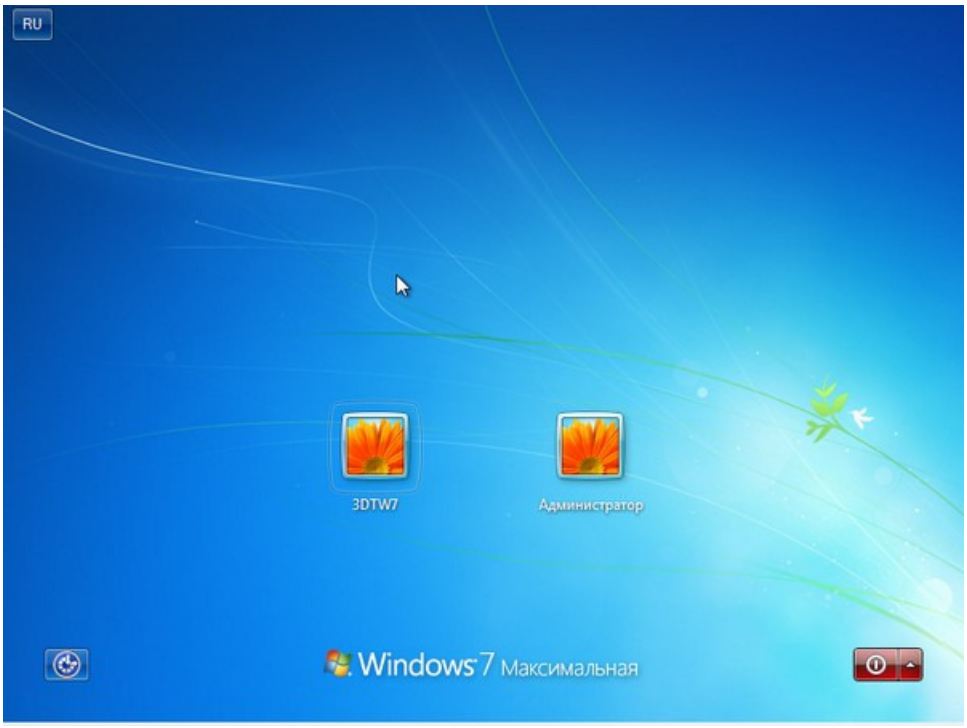


Теперь надо выделить наш куст *HKEY_LOCAL_MACHINE|имя_куста|* и в меню выбрать «Файл» → «Выгрузить куст...» (File Unload hive...), а затем подтвердить выгрузку куста.

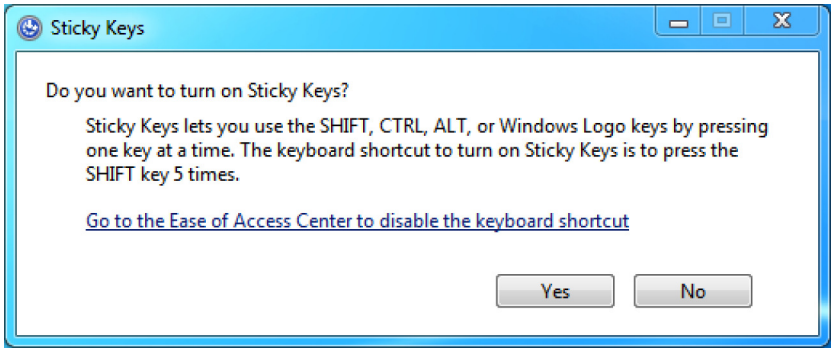




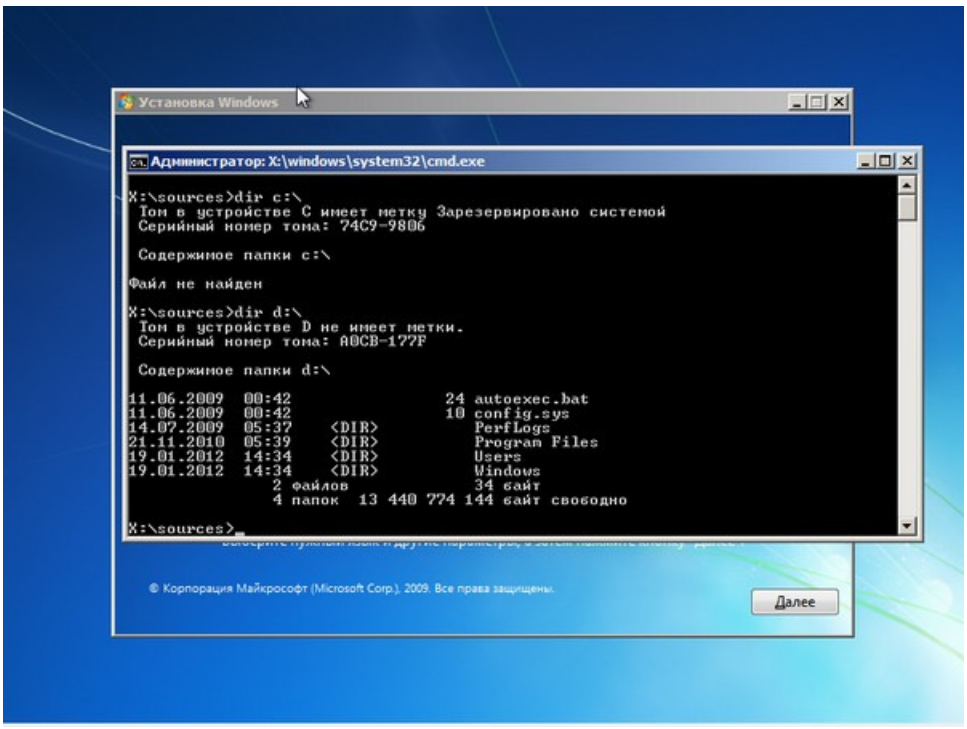
Всё, можно перезагрузиться, вытащив предварительно установочный диск, и войти в систему под администраторским аккаунто
В панели управления Windows в разделе управления пользователями можно изменить настройки другой учётной записи. В то
числе поменять пароль.



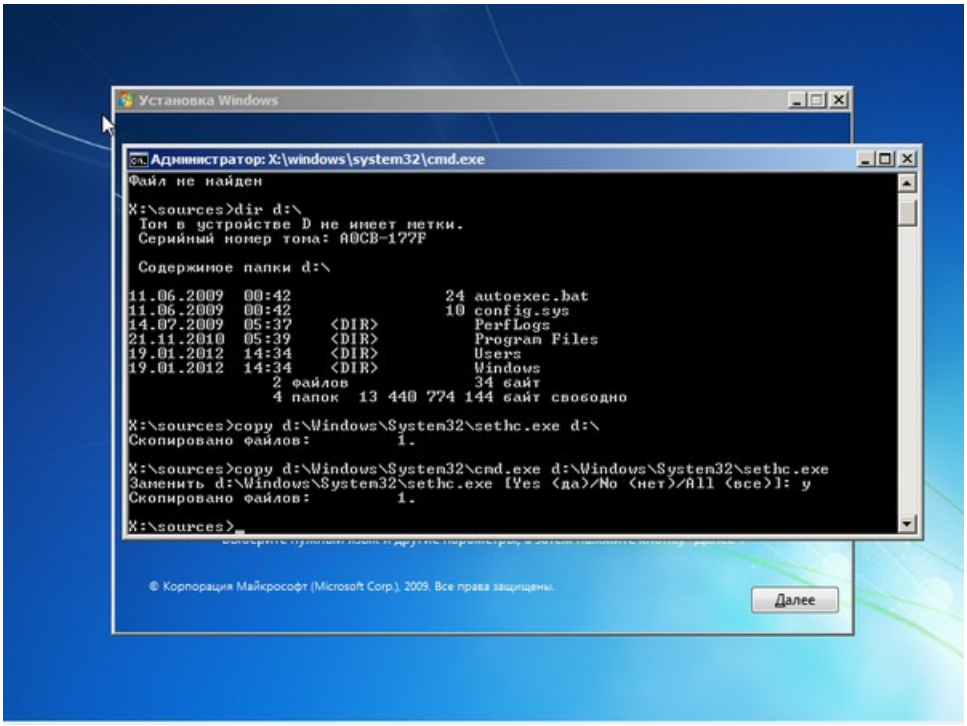
Остался последний способ, неправильный. Почему неправильный? Потому что мы займёмся подменой системных файлов, а э
дело неблагородное. В чём заключается основная идея? Всё просто — в ОС по умолчанию включена функция детектирован
залипающих клавиш. Вы с ней наверняка сталкивались хотя бы раз, а если нет — то просто быстро нажмите Shift не менее 5 ра
и вы увидите вот такое замечательное окошко:



Окошко это принадлежит маленькой вспомогательной программке *sethc.exe*, которая лежит в системной директории Window
Более того, она запускается даже на экране приветствия, когда вам предлагают выбрать пользователя и ввести пароль. Но ве
её можно заменить чем-нибудь полезным. К примеру, *cmd.exe*. Естественно, не прямо в запущенной ОС, а загрузившись
установочного диска Windows 7 и нажав Shift+F10.



Начать надо с определения буквы диска, на котором установлена Windows. Самое легкое — просто просмотреть содержим корня раздела командой *dir*. C:, скорее всего, будет виден как D:, но необязательно.

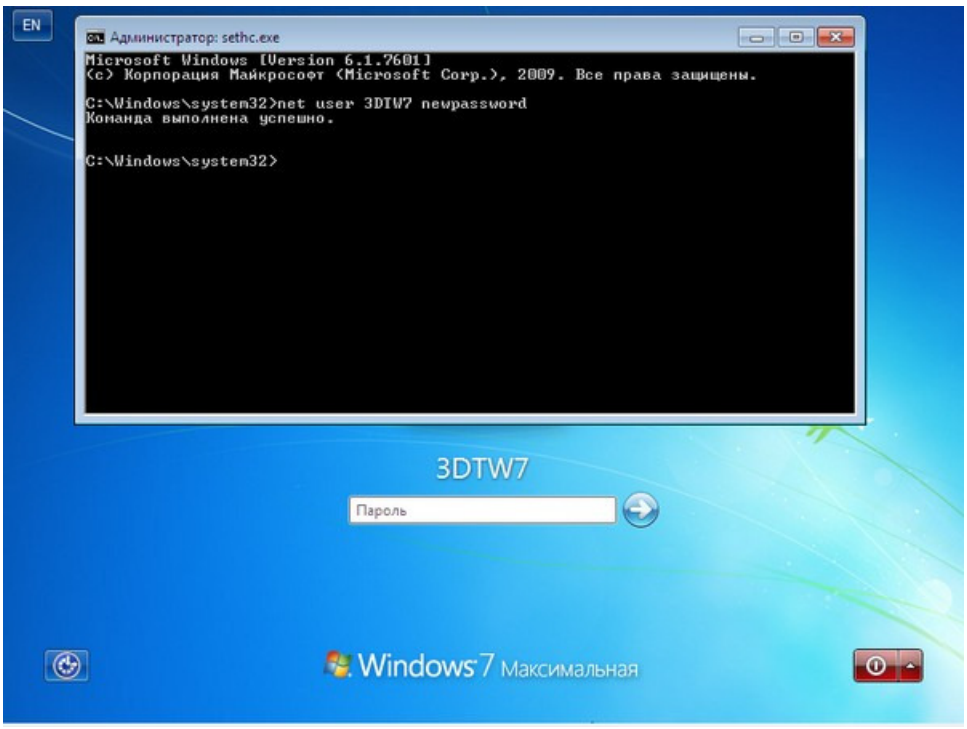


Определившись с буквой тома, выполняем две простые команды — одной копируем на всякий случай оригинальный фа *sethc.exe* в корень диска или куда душе угодно, а второй меняем его на *cmd.exe*.

```
copy d:\windows\system32\sethc.exe d:\
copy d:\windows\system32\cmd.exe
d:\windows\system32\sethc.exe
```

Перезагружаемся, быстро нажимаем несколько раз клавишу Shift (или Ctrl, или Alt) и наблюдаем окно с командной строкой. нём надо ввести ещё одну команду, подставив соответственно имя нужного пользователя и новый пароль. С други параметрами этой команды можно ознакомиться в официальной справке.

```
net user имя_пользователя
новый_пароль
```



Если вы захотите вернуть всё на круги своя, то надо снова загрузиться с установочного диска, открыть консоль и выполни команду:

```
copy d:\sethc.exe
d:\windows\system32\sethc.exe
```

Впрочем, можно ничего не восстанавливать, а оставить такой маленький трюк в системе на всякий случай. Помим перечисленных выше способов, есть множество других методик сброса или восстановления пароля в Windows, но сейчас мы рассматривать не будем. Ещё раз призываем наших читателей быть внимательными и аккуратными при работе с внутренностя ОС, а ещё лучше не доводить ситуацию до «хирургического» вмешательства в SAM. Удачного вам восстановления доступа учётным