

Пошаговые Руководства

Сам Себе Админ

системное администрирование

Microsoft Windows



Как сбросить пароль в Windows ?



Сегодняшний наш урок написан в соавторстве с Павлом Гришенковым (фото - слева), который любезно согласился поделиться интересной и полезной информацией с читателями нашего сайта.



Ситуация с потерей пароля к Windows, в общем, типичная. Поэтому неплохо бы подготовиться к ней заранее и знать, как быстро сбросить или сменить пароль. Приложение «Offline NT Password & Registry Editor» – это бесплатная утилита на базе Linux. Записав образ ISO на CD-диск, вы в любой момент сможете воспользоваться ей для смены паролей учетных записей в ОС Windows NT, 2000, XP и Vista. Утилита обнаруживает учетные записи пользователей и дает возможность поменять существующий пароль на любую другую комбинацию. Приложение работает даже с заблокированными и отключенными учетными записями.

Загрузите компьютер с созданного вами диска (не забудьте настроить BIOS на загрузку с CD) и вы увидите следующее диалоговое окно:

```
*****
*
*      Windows Reset Password / Registry Editor / Boot CD
*
*      (c) 1998-2011 Petter Nordahl-Hagen. Distributed under GNU GPL v2
*
*      DISCLAIMER: THIS SOFTWARE COMES WITH ABSOLUTELY NO WARRANTIES!
*                  THE AUTHOR CAN NOT BE HELD RESPONSIBLE FOR ANY DAMAGE
*                  CAUSED BY THE (MIS)USE OF THIS SOFTWARE
*
*      More info at: http://pogostick.net/~pnh/ntpasswd/
*      Email      : pnh@pogostick.net
*
*      CD build date: Wed May 11 20:16:09 CEST 2011
*
*****

Press enter to boot, or give linux kernel boot options first if needed.
Some that I have to use once in a while:
boot nousb      - to turn off USB if not used and it causes problems
boot irqpoll    - if some drivers hang with irq problem messages
boot vga=ask    - if you have problems with the videomode
boot nodrivers  - skip automatic disk driver loading

boot:
```

Нажимаем клавишу «Enter».

Далее программа спросит, на каком разделе у вас находится Windows. При этом пункт [1] уже выбран, так что просто нажимаем «Enter».

```

* (c) 1997 - 2010 Petter N Hagen - pnoordahl@eunet.no
* GNU GPL v2 license, see files on CD
*
* This utility will enable you to change or blank the password of
* any user (incl. administrator) on an Windows NT/2k/XP/Vista
* WITHOUT knowing the old password.
* Unlocking locked/disabled accounts also supported.
*
* It also has a registry editor, and there is now support for
* adding and deleting keys and values.
*
* Tested on: NT3 51 & NT4: Workstation, Server, PDC.
* Win2k Prof & Server to SP4. Cannot change AD.
* XP Home & Prof: up to SP3
* Win 2003 Server (cannot change AD passwords)
* Vista & Win7 32 and 64 bit, Server 2008 32+64 bit
*
* HINT: If things scroll by too fast, press SHIFT-PGUP/PGDOWN ...
*****
=====
There are several steps to go through:
- Disk select with optional loading of disk drivers
- PATH select, where are the Windows systems files stored
- File select, what parts of registry we need
- Then finally the password change or registry edit itself
- If changes were made, write them back to disk
DON'T PANIC! Usually the defaults are OK, just press enter
all the way through the questions
=====
Step ONE: Select disk where the Windows installation is
=====
Disks:
Disk /dev/sda: 61.4 GB, 61492838400 bytes
Candidate Windows partitions found:
1 : /dev/sda1 29329MB (LBA) ROOT
2 : /dev/sda5 29313MB
Please select partition by number or
q = quit
d = automatically start disk drivers
m = manually select disk drivers to load
f = fetch additional drivers from floppy / usb
a = show all partitions found
l = show propable Windows (NTFS) partitions only
Select: [1]

```

Если под операционную систему отведен другой физический (логический) диск делаем соответствующие правки.

Затем утилита попросит указать путь до папки, где находятся файлы SAM (фактически SAM это - куст реестра). По умолчанию путь к нему: Windows\System32\config, его же и предлагает программа. Нажимаем «Enter».

```

=====
There are several steps to go through:
- Disk select with optional loading of disk drivers
- PATH select, where are the Windows systems files stored
- File select, what parts of registry we need
- Then finally the password change or registry edit itself
- If changes were made, write them back to disk
DON'T PANIC! Usually the defaults are OK, just press enter
all the way through the questions
=====
Step ONE: Select disk where the Windows installation is
=====
Disks:
Disk /dev/sda: 61.4 GB, 61492838400 bytes
Candidate Windows partitions found:
1 : /dev/sda1 29329MB (LBA) ROOT
2 : /dev/sda5 29313MB
Please select partition by number or
q = quit
d = automatically start disk drivers
m = manually select disk drivers to load
f = fetch additional drivers from floppy / usb
a = show all partitions found
l = show propable Windows (NTFS) partitions only
Select: [1] 1
Selected 1
Mounting from /dev/sda1, with assumed filesystem type FAT/UFAT/FAT32 and similar
Trying to mount FAT / UFAT / FAT32 etc
Success
=====
Step TWO: Select PATH and registry files
=====
DEBUG path: windows found as WINDOWS
DEBUG path: system32 found as system32
DEBUG path: config found as config
DEBUG path: found correct case to be: WINDOWS/system32/config
What is the path to the registry directory? (relative to windows disk)
[WINDOWS/system32/config] :

```

Далее, мы можем выбрать сброс пароля или работу в консоли восстановления. Опять же, просто нажимаем коавишу «Enter» для выбора опции сброса пароля (она у нас под цифрой «1»).

```

2 : /dev/sda5 29313MB
Please select partition by number or
q = quit
d = automatically start disk drivers
r = manually select disk drivers to load
n = fetch additional drivers from floppy / usb
a = show all partitions found
l = show probable Windows (NTFS) partitions only
Select: [1] 1
Selected 1
Mounting from /dev/sda1, with assumed filesystem type FAT/UFAT/FAT32 and similar
Trying to mount FAT / UFAT / FAT32 etc
Success
=====
Step TWO: Select PATH and registry files
=====
DEBUG path: windows found as WINDOWS
DEBUG path: system32 found as system32
DEBUG path: config found as config
DEBUG path: found correct case to be: WINDOWS/system32/config
What is the path to the registry directory? (relative to windows disk)
DEBUG path: WINDOWS found as WINDOWS
DEBUG path: system32 found as system32
DEBUG path: config found as config
DEBUG path: found correct case to be: WINDOWS/system32/config
-rwxr-xr-x 1 0 0 524288 Jul 24 13:25 DEFAULT
-rwxr-xr-x 2 0 0 16384 May 28 2012 RCCBackup
-rwxr-xr-x 1 0 0 262144 Jul 24 13:25 SAM
-rwxr-xr-x 1 0 0 262144 Jul 24 13:25 SECURITY
-rwxr-xr-x 1 0 0 1739360 Jul 24 13:25 SOFTWARE
-rwxr-xr-x 1 0 0 3932160 Jul 24 15:54 SYSTEM
-rwxr-xr-x 14 0 0 16384 May 1 2012 systemprofile
-rwxr-xr-x 1 0 0 262144 May 1 2012 userdiff
Select which part of registry to load, use predefined choices
or list the files with space as delimiter
1 - Password reset [sam system security]
2 - RecoveryConsole parameters [software]
q - quit - return to previous
[1] : 1

```

На следующий вопрос, о том, что мы хотим сделать: отредактировать пользовательские данные и пароли или реестр, – нажимаем «Enter».

```

-rwxr-xr-x 1 0 0 3932160 Jul 24 15:54 SYSTEM
-rwxr-xr-x 14 0 0 16384 May 1 2012 systemprofile
-rwxr-xr-x 1 0 0 262144 May 1 2012 userdiff
Select which part of registry to load, use predefined choices
or list the files with space as delimiter
1 - Password reset [sam system security]
2 - RecoveryConsole parameters [software]
q - quit - return to previous
[1] : 1
Selected files: sam system security
Copying sam system security to /tmp
=====
Step THREE: Password or registry edit
=====
chntpw version 0.99.6 119511 : (c) Petter N Hagen
Hive <SAM> name (from header): (c:\SystemRoot\System32\Config\SAM)
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 262144 [40000] bytes, containing 6 pages (+ 1 headerpage)
Used for data: 230/18304 blocks/bytes, unused: 9/6080 blocks/bytes.
Hive <SYSTEM> name (from header): <SYSTEM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 3932160 [3c0000] bytes, containing 851 pages (+ 1 headerpage)
Used for data: 64800/3635984 blocks/bytes, unused: 1594/14992 blocks/bytes.
Hive <SECURITY> name (from header): (c:\SystemRoot\System32\Config\SECURITY)
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 262144 [40000] bytes, containing 11 pages (+ 1 headerpage)
Used for data: 871/40392 blocks/bytes, unused: 6/4312 blocks/bytes.
* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length : 0
Password history count : 0
<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <SAM> <SYSTEM> <SECURITY>
1 - Edit user data and passwords
9 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)
What to do? [1] ->

```

Вписываем имя пользователя или его идентификатор в формате 0xabcd, где abcd это - RID, указанный в первом столбце. Идентификатор RID пригодится, если имя пользователя некорректно отображается или его не получается ввести. Например, при использовании кириллицы. Нажимаем «Enter».

```

=====
Step THREE: Password or registry edit
=====
chntpw version 0.99.6 110511 : (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 262144 [40000] bytes, containing 6 pages (+ 1 headerpage)
Used for data: 230/18304 blocks/bytes, unused: 9/6080 blocks/bytes.

Hive <SYSTEM> name (from header): <SYSTEM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 3932160 [3c0000] bytes, containing 852 pages (+ 1 headerpage)
Used for data: 64800/3635984 blocks/bytes, unused: 1602/19056 blocks/bytes.

Hive <SECURITY> name (from header): <emRoot\System32\Config\SECURITY>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 262144 [40000] bytes, containing 11 pages (+ 1 headerpage)
Used for data: 871/40392 blocks/bytes, unused: 6/4312 blocks/bytes.

* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length          : 0
Password history count           : 0

<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <SAM> <SYSTEM> <SECURITY>

 1 - Edit user data and passwords
 9 - Registry editor, now with full write support!
 q - Quit (you will be asked if there is something to save)

What to do? [1] ->
==== chntpw Edit User Info & Passwords ====
RID  - Username ----- Admin?  - Lock?  --
03e8  HelpAssistant          dis/lock
03ea  SUPPORT 388945a0         dis/lock
01f4  4<8=8AB@0B>e             ADMIN   *BLANK*
01f5  >ABL                     ADMIN   dis/lock
03eb  >025;

Select: ↑ - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [ ] 0x01f5

```

Выбираем вариант – очистить пароль, так что просто еще раз нажмите нашу любимую клавишу «Enter» ☺ При этом, вернувшись позже в Windows, сможете изменить свой пароль на любой понравившийся.

```

 1 - Edit user data and passwords
 9 - Registry editor, now with full write support!
 q - Quit (you will be asked if there is something to save)

What to do? [1] ->
==== chntpw Edit User Info & Passwords ====
RID  - Username ----- Admin?  - Lock?  --
03e8  HelpAssistant          dis/lock
03ea  SUPPORT 388945a0         dis/lock
01f4  4<8=8AB@0B>e             ADMIN   *BLANK*
01f5  >ABL                     ADMIN   dis/lock
03eb  >025;

Select: ↑ - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [ ] 0x01f5
RID      : 0501 [01f5]
Username : >ABL
fullname :
comment  : AB@5==00 CG5B=00 7@?8AL 4;0 4>ABC?0 3>AB59 : :>?LNB5@C/4><5=C
homedir  :

User is member of 1 groups:
00000222 =>AB8 (which has 1 members)

Account bits: 0x0215 =
[X] Disabled          [ ] Homedir req.      [X] Psswd not req.
[ ] Temp, duplicate  [X] Normal account  [ ] NMS account
[ ] Domain trust ac  [ ] Wks trust act.  [ ] Sev trust act
[X] Pwd don't expir   [ ] auto lockout   [ ] (unknown 0x08)
[ ] (unknown 0x10)   [ ] (unknown 0x20)  [ ] (unknown 0x40)

Failed login count: 0, while max tries is: 0
Total login count: 0
** No NT MD4 hash found. This user probably has a BLANK password!
** No LANMAN hash found either. Sorry, cannot change. Try login with no password
↑

- - - User Edit Menu:
1 - Clear (blank) user password
2 - Edit (blank) user password (careful with this on XP or Vista)
3 - Promote user (make user an administrator)
4 - Unlock and enable user account [probably locked now]
q - Quit editing user, back to user select
Select: [q] >

```

Теперь необходимо выйти из режима редактирования. Для этого, как и предлагает программа, вводим восклицательный знак (!), далее - «Enter».

```
q - Quit (you will be asked if there is something to save)

What to do? [1] ->

==== chntpw Edit User Info & Passwords ====

RID      Username      Admin?      Lock?
03e8     HelpAssistant  dis/lock
03ea     SUPPORT_388945a0 dis/lock
01f4     4<8=8AB00B>@   ADMIN      *BLANK*
01f5     >ABL           ADMIN      dis/lock
03eb

Select: ? - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [ ] 0x01f5

RID      : 0501 [01f5]
Username : >ABL
Fullname :
Comment  : AB0>5==00 CG5B=00 70?8AL 4;0 4>ABC?0 3>AB59 : :><?LNB50C/4><5=C
Homedir  :

User is member of 1 groups:
00000222 = >AB8 (which has 1 members)

Account bits: 0x0215 =
[X] Disabled           [ ] Homedir req.      [X] Passwd not req.
[ ] Temp. duplicate    [X] Normal account   [ ] NMS account
[ ] Domain trust ac   [ ] Wks trust act.   [ ] Srv trust act
[X] Pwd don't expir   [ ] Auto lockout     [ ] (unknown 0x08)
[ ] (unknown 0x10)    [ ] (unknown 0x20)   [ ] (unknown 0x40)

Failed login count: 0, while max tries is: 0
Total login count: 0
** No NT MD4 hash found. This user probably has a BLANK password!
** No LANMAN hash found either. Sorry, cannot change. Try login with no password

- - - User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP or Vista)
3 - Promote user (make user an administrator)
4 - Unlock and enable user account [probably locked now]
q - Quit editing user, back to user select
Select: [q] > 1
Password cleared!

Select: ? - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [ ] ?
```

Нажимаем клавишу «q» (quit) чтобы выйти.

```
Select: ? - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [ ] 0x01f5

RID      : 0501 [01f5]
Username : >ABL
Fullname :
Comment  : AB0>5==00 CG5B=00 70?8AL 4;0 4>ABC?0 3>AB59 : :><?LNB50C/4><5=C
Homedir  :

User is member of 1 groups:
00000222 = >AB8 (which has 1 members)

Account bits: 0x0215 =
[X] Disabled           [ ] Homedir req.      [X] Passwd not req.
[ ] Temp. duplicate    [X] Normal account   [ ] NMS account
[ ] Domain trust ac   [ ] Wks trust act.   [ ] Srv trust act
[X] Pwd don't expir   [ ] Auto lockout     [ ] (unknown 0x08)
[ ] (unknown 0x10)    [ ] (unknown 0x20)   [ ] (unknown 0x40)

Failed login count: 0, while max tries is: 0
Total login count: 0
** No NT MD4 hash found. This user probably has a BLANK password!
** No LANMAN hash found either. Sorry, cannot change. Try login with no password

- - - User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP or Vista)
3 - Promote user (make user an administrator)
4 - Unlock and enable user account [probably locked now]
q - Quit editing user, back to user select
Select: [q] > 1
Password cleared!

Select: ? - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [ ] ?

<>=====<> chntpw Main Interactive Menu <>=====<>

Loaded hives: <SAM> <SYSTEM> <SECURITY>

1 - Edit user data and passwords
q - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)

What to do? [1] -> q
```

Затем вводим «y» (yes - подтверждение) для сохранения и - «Enter».

```

User is member of 1 groups:
00000222 =>AB8 (which has 1 members)
Account bits: 0x0215 =
[X] Disabled [ ] Homedir req. [X] Passwd not req.
[ ] Temp. duplicate [X] Normal account [ ] NMS account
[ ] Domain trust ac [ ] Wks trust act. [ ] Srv trust act
[X] Pwd don't expir [ ] Auto lockout [ ] (unknown 0x08)
[ ] (unknown 0x10) [ ] (unknown 0x20) [ ] (unknown 0x40)
Failed login count: 0, while max tries is: 0
Total login count: 0
** No NT MD4 hash found. This user probably has a BLANK password!
** No LANMAN hash found either. Sorry, cannot change. Try login with no password
- - - User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP or Vista)
3 - Promote user (make user an administrator)
4 - Unlock and enable user account [probably locked now]
q - Quit editing user, back to user select
Select: [q] > q
Password cleared!
Select: ? - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [ ] !
<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <SAM> <SYSTEM> <SECURITY>
1 - Edit user data and passwords
9 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)
What to do? [1] -> q
Hives that have changed:
# Name
0 <SAM> - OK
=====
Step FOUR: Writing back changes
=====
About to write file(s) back! Do it? [n] : y

```

Отказаться от дальнейшей работы в Offline NT Password and Registry editor – клавиша «n» (no).

```

[ ] Domain trust ac [ ] Wks trust act. [ ] Srv trust act
[X] Pwd don't expir [ ] Auto lockout [ ] (unknown 0x08)
[ ] (unknown 0x10) [ ] (unknown 0x20) [ ] (unknown 0x40)
Failed login count: 0, while max tries is: 0
Total login count: 0
** No NT MD4 hash found. This user probably has a BLANK password!
** No LANMAN hash found either. Sorry, cannot change. Try login with no password
- - - User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP or Vista)
3 - Promote user (make user an administrator)
4 - Unlock and enable user account [probably locked now]
q - Quit editing user, back to user select
Select: [q] > q
Password cleared!
Select: ? - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [ ] !
<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <SAM> <SYSTEM> <SECURITY>
1 - Edit user data and passwords
9 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)
What to do? [1] -> q
Hives that have changed:
# Name
0 <SAM> - OK
=====
Step FOUR: Writing back changes
=====
About to write file(s) back! Do it? [n] : y
Writing SAM
***** EDIT COMPLETE *****
You can try again if it somehow failed, or you selected wrong
New run? [n] : n

```

Увидим сообщение о том, что редактирование файла SAM завершено (EDIT COMPLETE):

```

- - - User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP or Vista)
3 - Promote user (make user an administrator)
4 - Unlock and enable user account [probably locked now]
q - Quit editing user, back to user select
Select: [q] > 1
Password cleared!

Select: ? - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [l] ?

<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <SAM> <SYSTEM> <SECURITY>

1 - Edit user data and passwords
9 - Registry editor, now with full write support!
q - Quit (you will be asked if there is something to save)

What to do? [1] -> q
Hives that have changed:
# Name
0 <SAM> - OK

=====  

Step FOUR: Writing back changes  

=====  

About to write file(s) back? Do it? [n] : y
Writing SAM

***** EDIT COMPLETE *****

You can try again if it somehow failed, or you selected wrong
New run? [n] : n
=====  

* end of scripts., returning to the shell..
* Press CTRL-ALT-DEL to reboot now (remove floppy first)
* or do whatever you want from the shell..
* However, if you mount something, remember to umount before reboot
* You may also restart the script procedure with 'sh /scripts/main.sh'
#

```

Извлекаем наш загрузочный CD/DVD диск и нажимаем комбинацию Alt+Ctrl+Del для перезагрузки. Готово: пароль Windows - сброшен!

Теперь – важно: ссылка на скачивание небольшого образа рассматриваемой нами в статье программы «Offline NT Password & Registry Editor». https://sebeadmin.thelogos.in.ua/soft/password_recovery.zip Просто запишите данный файл на «болванку» (в режиме iso, естественно) и можете сразу же его использовать, согласно данной инструкции.

Примечание: для записи рекомендую использовать замечательную и маленькую по размеру программу «ImgBurn». https://sebeadmin.thelogos.in.ua/soft/img_burn.zip

Есть и другие решения для данной задачи. И с одним из них мы бы хотели Вас, уважаемые читатели, познакомить.

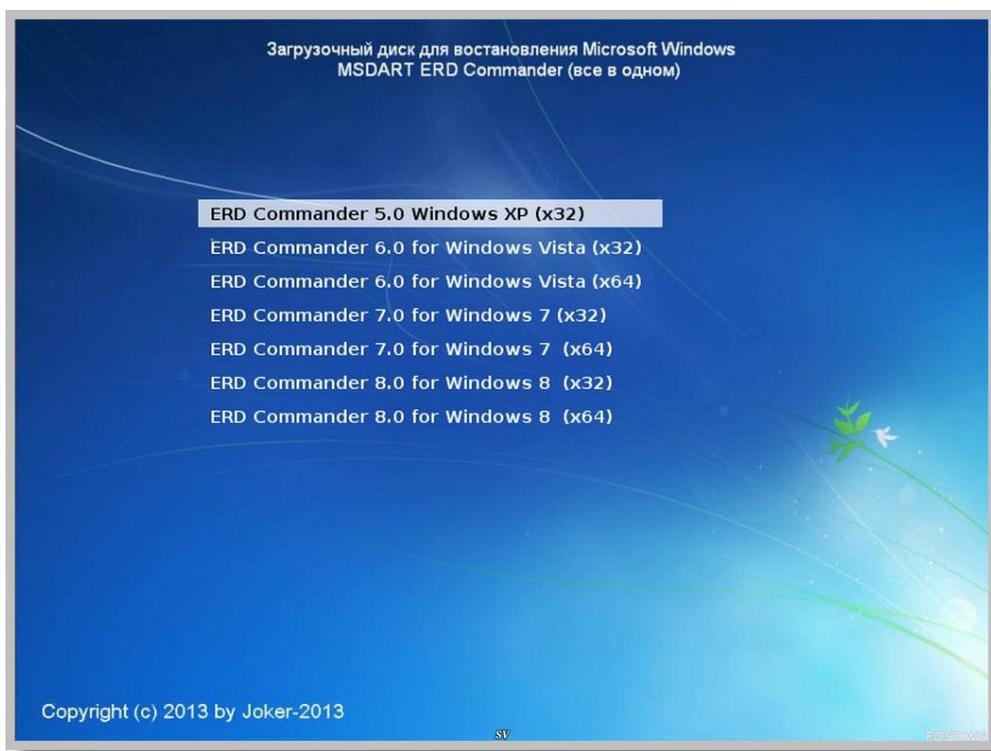
Одним из специализированных пакетов, которые являются целой средой для восстановления работоспособности системы есть «ERD Commander». Первоначально разработанный компанией Wininternals и представлявший собой ядро пакета «Wininternals Administrator's Pak». Сейчас ERD Commander - один из компонентов **DaRT** (Diagnostics and Recovery Toolset - набор для диагностики и восстановления), который входит в состав «Microsoft Desktop Optimization Pack».

Видите, как все запутано? ☺ Но что сейчас нам с Вами из всего этого надо усвоить? А то, что плохую вещь корпорация Microsoft вряд ли купила бы, а именно это произошло с ERD Commander-ом. Поэтому этот инструмент смело можете брать на

«вооружение»: вряд ли его разработка в скором времени будет прекращена, а один раз научившись им пользоваться, Вы всегда будете иметь под рукой мощное средство для восстановления и обслуживания операционных систем Microsoft Windows.

Другое дело, что свободно скачивать MDOP (Microsoft Desktop Optimization Pack) могут только обладатели платных подписок TechNet. Но, как Вы понимаете, мир – не без добрых людей и достаточно набрать в любом поисковике фразу: «скачать ERD Commander» и мы получим набор ссылок, из которых можем выбрать понравившийся нам дистрибутив ☺

Рекомендую обратить внимание на сборки, которые включают в себя все, доступные на данный момент, версии пакета. Они «везят» больше гигабайта, но это – того стоит! При загрузке с такого диска мы увидим вот такое удобное меню:



Каждая из версий подходит для восстановления определенного типа операционных систем семейства Windows.

- ERD Commander 5.0 годится для восстановления Windows XP и Windows Server 2003
- Шестая версия – для Windows Vista и Windows Server 2008 (32 бита)
- Седьмая – для Windows 7 и Windows Server 2008 R2 и т.д.
- То же касается и 64-х разрядных систем (для них – используются 64-х битные версии пакета)

ERD Commander это - набор программ, работающих в среде Windows PE (Preinstallation Environment - о ней мы говорили в одном из наших предыдущих уроков). Windows PE позволяет выполнить загрузку системы со съемного носителя, что дает возможность запустить компьютер даже в случае серьезного повреждения файлов существующей на диске ОС, необходимых для ее старта.

Являясь «почти настоящей» 32-битной Windows, среда PE обеспечивает полный доступ к NTFS-томам, системному реестру, параметрам настройки драйверам и службам «ремонтируемой» системы. Стандартный оконный интерфейс ERD Commander-a, позволяет легко и эффективно использовать входящие в него инструменты.

Все программы, входящие в состав ERD Commander, разделены на три категории:

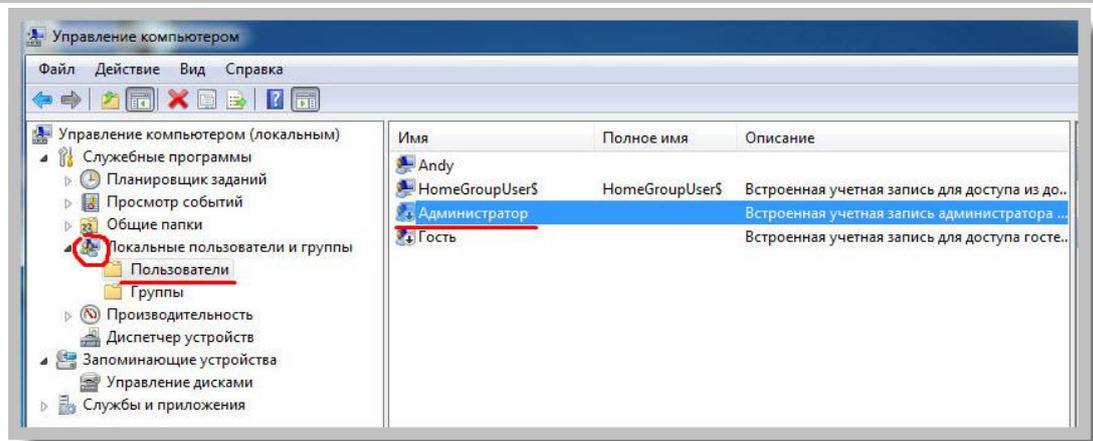
- административные средства
- инструменты для работы с сетью
- системные утилиты.

Кроме того, присутствуют довольно стандартные программы: интерпретатор командной строки (cmd), файловый менеджер (проводник Windows), поиск, блокнот и т.д. Также в состав ERD входит Solution Wizard - небольшой мастер, с помощью диалоговых окон "подсказывающий", применение какого инструмента будет уместным в той или иной ситуации.

Так, с теорией разобрались, переходим к практике! Поскольку у нас статья, главным образом, посвящена сбросу (удалению) пароля администратора в ОС Windows, то и начнем мы именно с этой задачи.

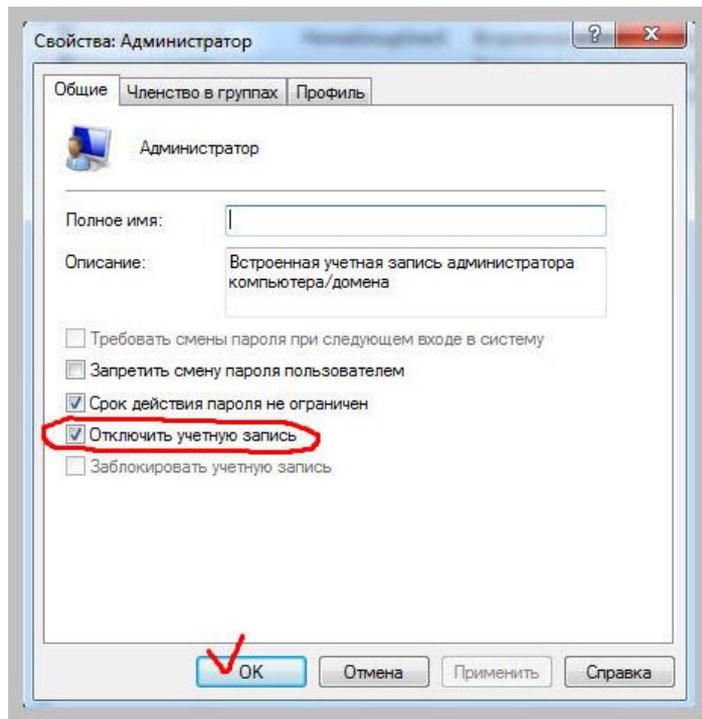
Чтобы удалить пароль, его нужно сначала установить. Давайте так и сделаем!

Нажимаем правой кнопкой мыши на значке «Мой компьютер» на рабочем столе и из открывшегося меню выбираем пункт «Управление». В открывшейся оснастке раскрываем список «Локальные пользователи и группы», выделяем пункт «Пользователи». В правой части окна мы увидим список всех учетных записей, зарегистрированных на компьютере:

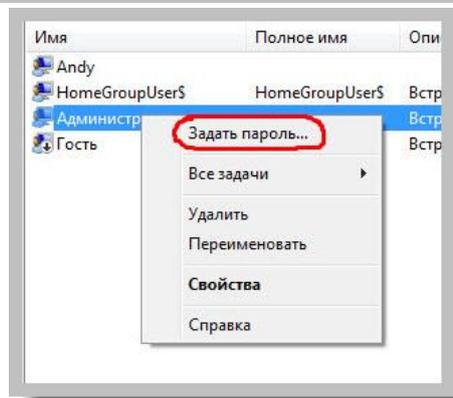


Примечание: сбросить пароль можно для любой учетной записи, мы будем рассматривать этот процесс на примере записи «Администратор».

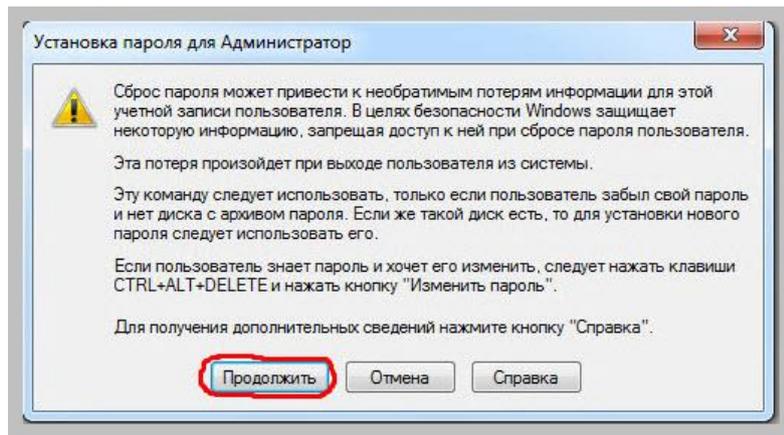
Нажимаем на ней правой кнопкой мыши и из открывшегося списка выбираем пункт «Свойства». В Windows 7 (в отличие от Windows XP) учетная запись «Администратор» по умолчанию отключена. Давайте исправим эту ситуацию!



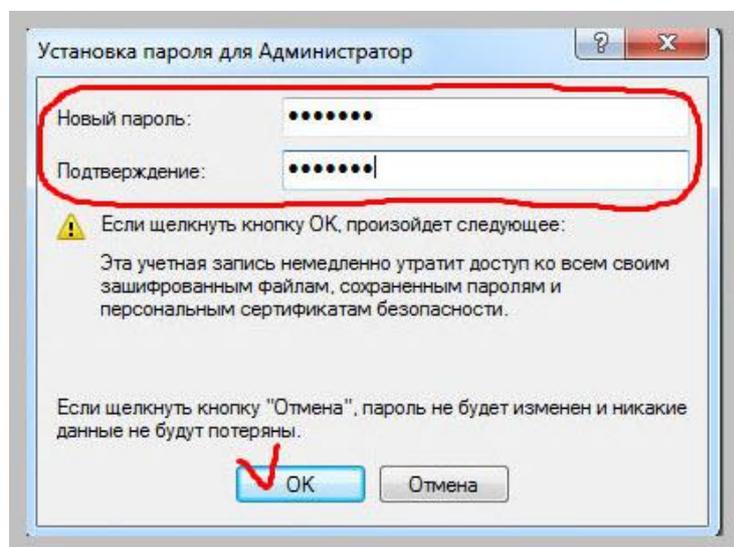
На вкладке «Общие» убираем галочку рядом с пунктом «Отключить учетную запись» и нажимаем кнопку «ОК». Затем, снова нажимаем правой кнопкой и из меню выбираем пункт «Задать пароль».



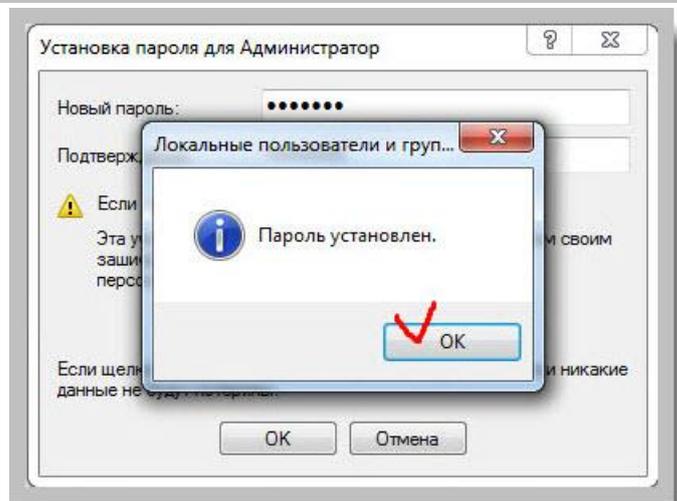
Появится вот такое окно с предупреждением:



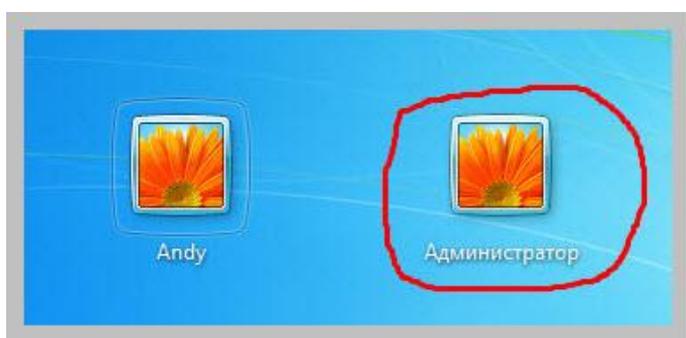
Поскольку мы знаем что делаем, то нажимаем кнопку «Продолжить». Появится окно, в котором мы можем установить пароль для учетной записи «Администратор».



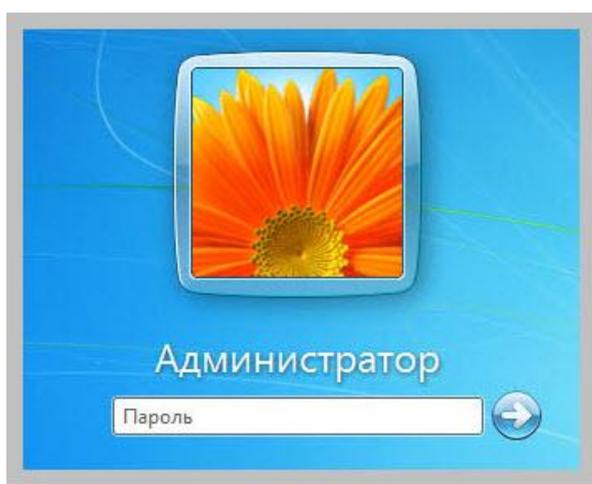
Вводим его дважды и нажимаем кнопку «OK». Увидим сообщение об успешной установке (смене) пароля.



Если мы сейчас перезагрузим систему, то увидим, что у нас при входе в Windows появились две учетные записи.



Причем, если мы попробуем войти в «Администратор», то увидим запрос на ввод пароля.



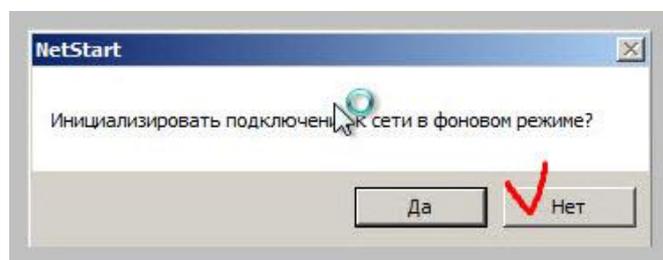
Так! Пароль у нас есть! Теперь, давайте представим, что мы его забыли (или компьютер принес нам на ремонт клиент, который также его не помнит) и нам, как мастеру, нужно этот пароль убрать ☺

Для этого нам нужен загрузочный диск с записанным на нем ERD Commander-ом (я пользуюсь сборкой, скриншот из которой я показывал выше), выставить в биос загрузку с CD/DVD и перезагрузиться.

Если мы все сделали правильно, начнется загрузка с компакт-диска:

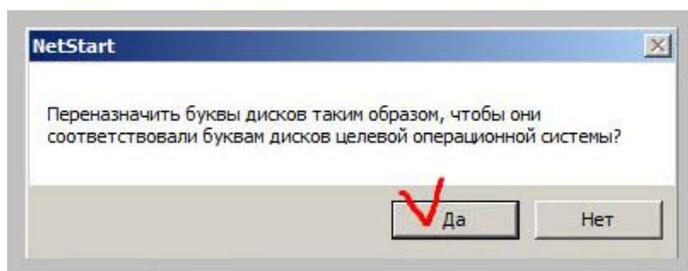


По прошествии некоторого времени (пока среда восстановления загружается в память компьютера) мы увидим вот такое окно, с которого начнется ее минимальная настройка:

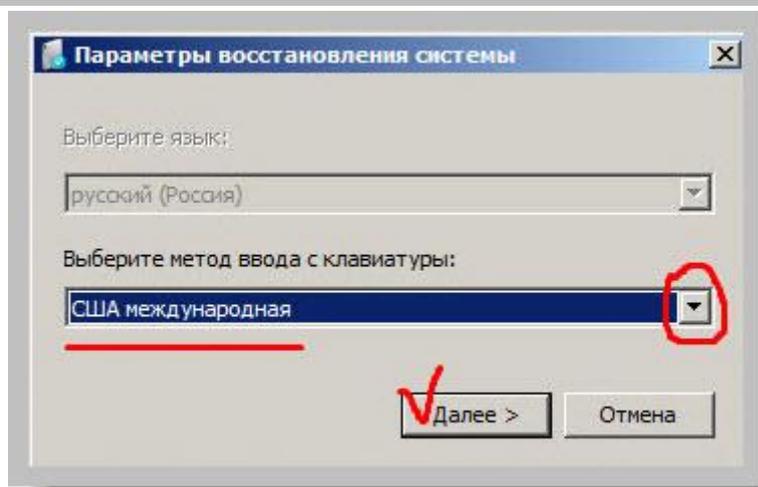


Уже на данном этапе, мы можем настроить подключение к локальной сети прямо из среды ERD. Но можно этого и не делать (непосредственно для нашей задачи это – не принципиально).

Следующее окно также не очень важно (я нажал «Да», но можете поступить и по другому).

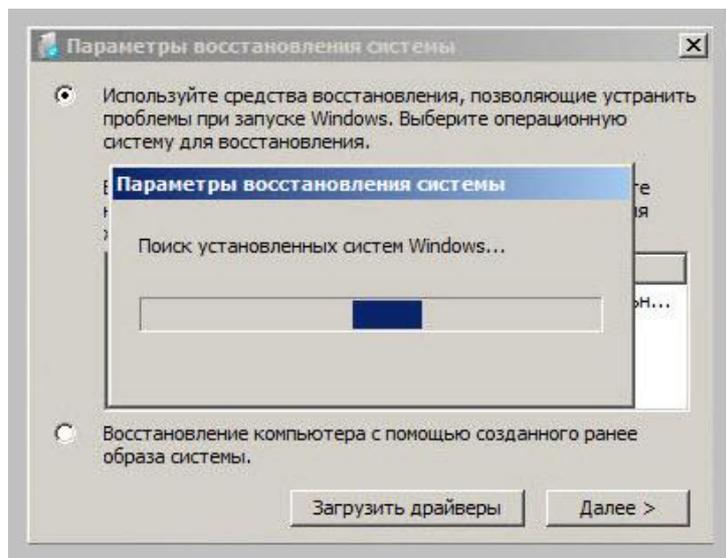


Вот в следующем окне я бы рекомендовал выбрать из списка международную английскую раскладку клавиатуры (просто для удобства в дальнейшем).

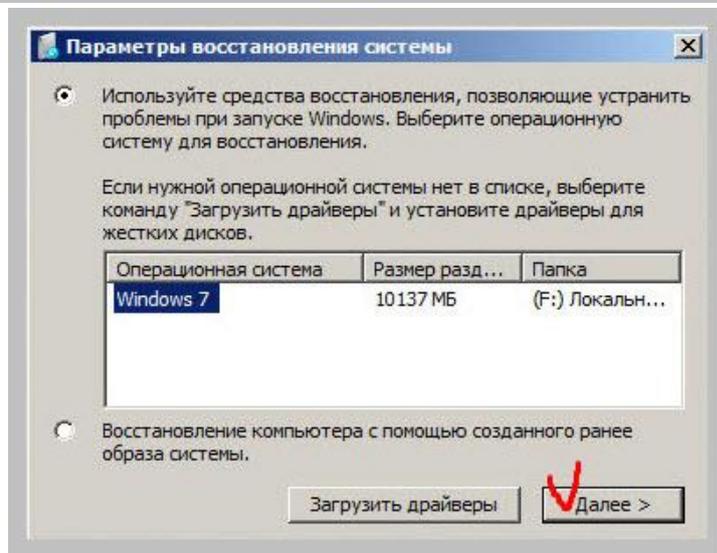


Нажимаем кнопку «Далее».

Запустится, знакомое нам уже по предыдущим статьям, окно среды восстановления WRE (Windows Recovery Environment), которое выполнит поиск потенциальных проблем загрузки Windows.

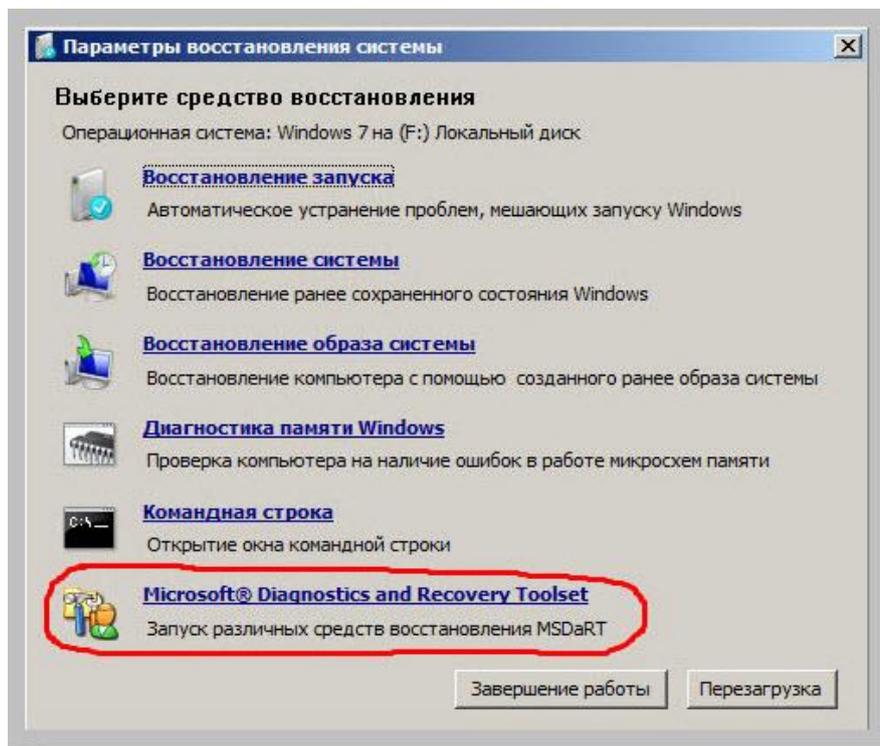


Также в автоматическом режиме будет произведен поиск установленных на компьютере операционных систем:



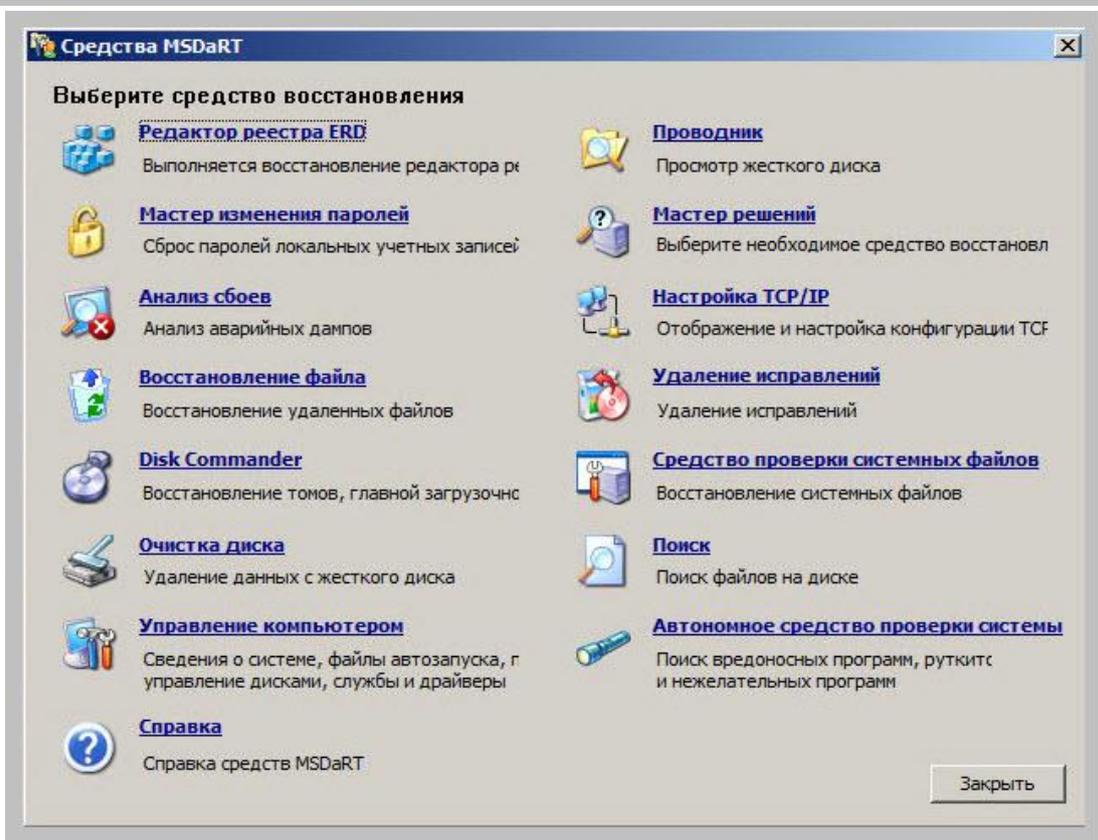
Никаких драйверов мы загружать не будем. Нажимаем кнопку «Далее».

Появится также уже знакомое нам ранее по урокам окно, но – с одним очень важным дополнительным пунктом в самом его низу:



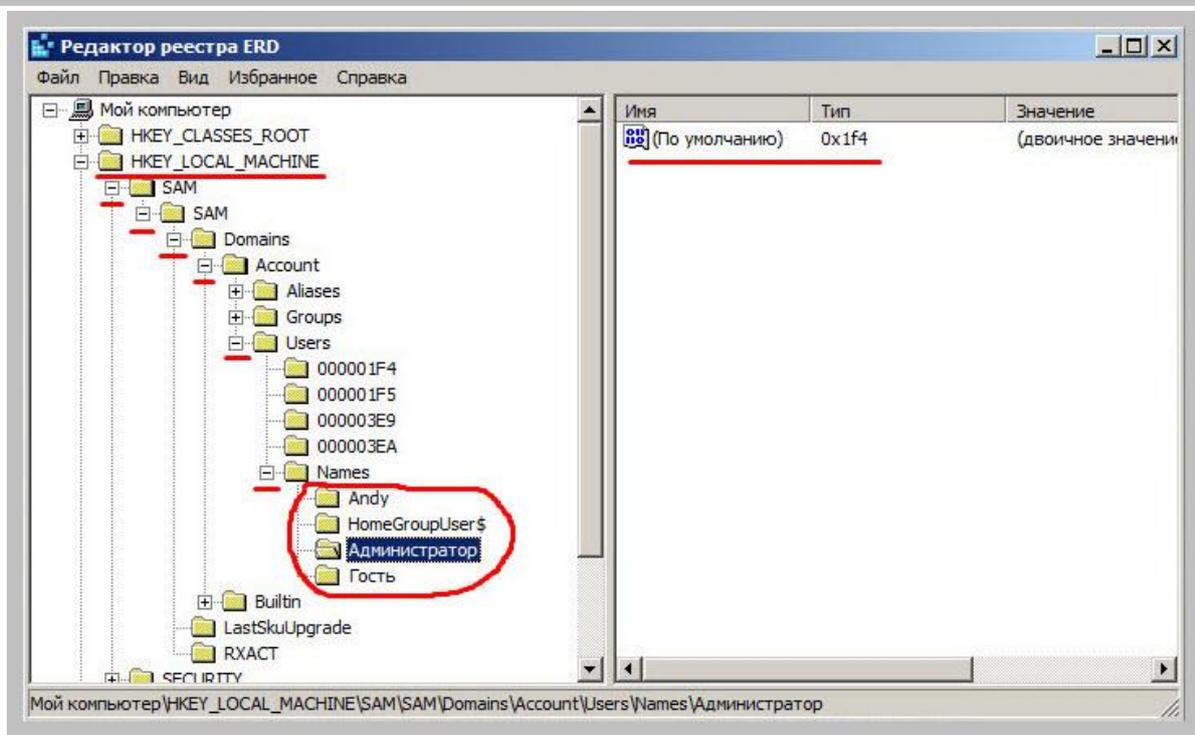
Вот это и есть MSaRT, о котором мы говорили в начале данной статьи.

Нажимаем на одноименную ссылку и видим вот такое окно:



Каждая ссылка здесь – отдельный инструмент восстановления или настройки тех или иных параметров системы, которая уже установлена на нашем компьютере. Среда MSDaRT только максимально удобным образом предоставляет нам доступ к различным ее параметрам и настройкам.

Первым пунктом идет «Редактор реестра ERD». Нажмем на него левой кнопкой мыши. Запустится почти привычное нам окно редактора системного реестра Windows. Только реестр этот – *с реально установленной на компьютере системы* (напоминаю об этом еще раз).



На скриншоте выше я открыл одну из главных его ветвей: HKEY_LOCAL_MACHINE, чтобы показать Вам, что в реестре в разделе SAM действительно хранятся сведения об учетных записях пользователей и их паролях (просто «раскрывайте» обозначенные на фото разделы и все сами увидите). Помните наших пользователей, которых мы наблюдали некоторое время назад с помощью оснастки Windows (Andy, Администратор)?

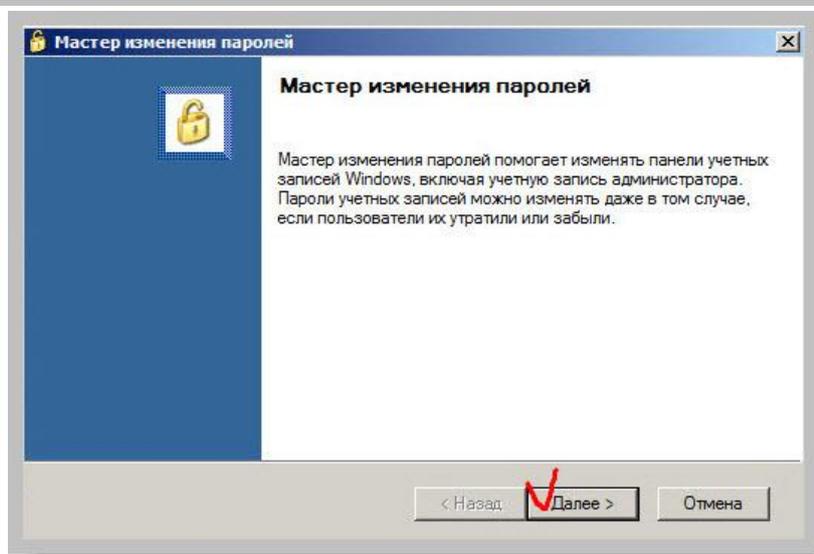
Давайте немного отвлечемся и усвоим необходимый минимум общей теории: Ветка реестра «HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Local Settings\Software\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\Names» формируется из файла, который находится по адресу: «Windows\System32\config\SAM» (можете зайти по этому адресу на своем компьютере).

Что такое этот SAM, и зачем он нужен?

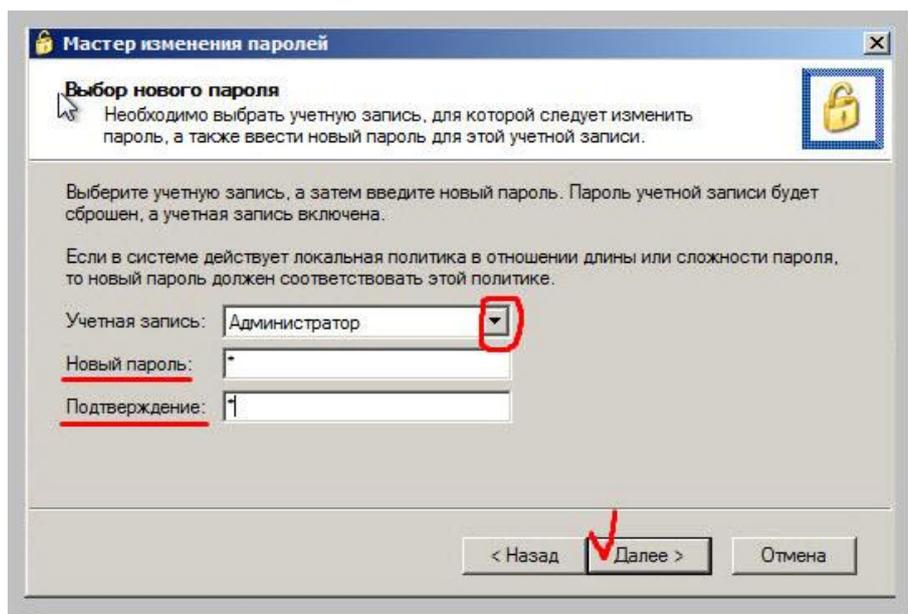
Это - файл реестра (SAM - Security Account Manager), который реально представляет собой «куст» "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Local Settings\Software\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\Names". В данном файле содержатся имена локальных пользователей данного компьютера и их зашифрованные пароли (хэши паролей). Поскольку пароли хранятся в зашифрованном виде, то, естественно, что просто так через реестр мы их не увидим ☺

Для этого нам нужен инструмент «Мастер изменения паролей» (он доступен из общего окна установок MSDaRT).

Запускаем его и видим первое окно «мастера» сброса и изменения пароля Windows:



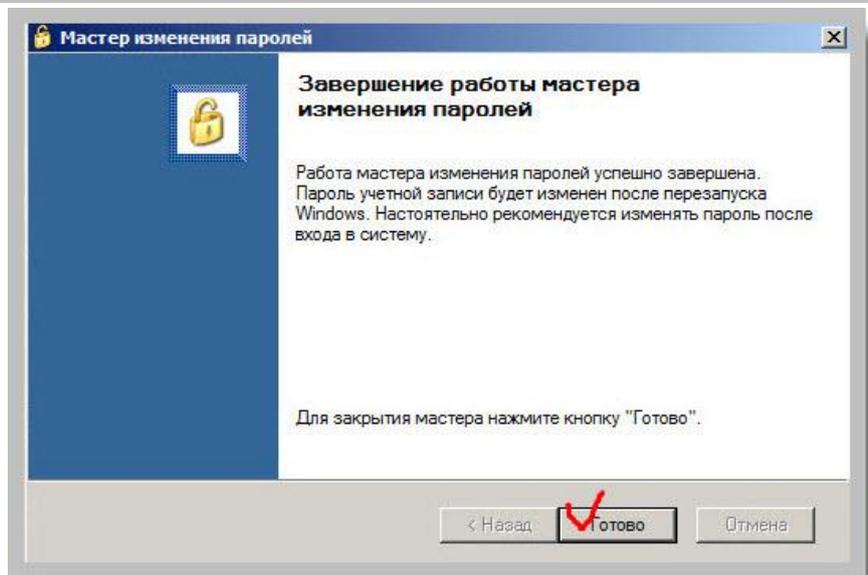
Просто нажимаем кнопку «Далее» и переходим к следующему шагу: из раскрывающегося списка выбираем ту учетную запись, для которой мы будем сбрасывать пароль (в нашем случае это – «Администратор») и в полях «Новый пароль» и «Подтверждение» указываем свои значения.



Я просто поставил цифру «1» (потом поменяем или совсем уберем уже из Windows).

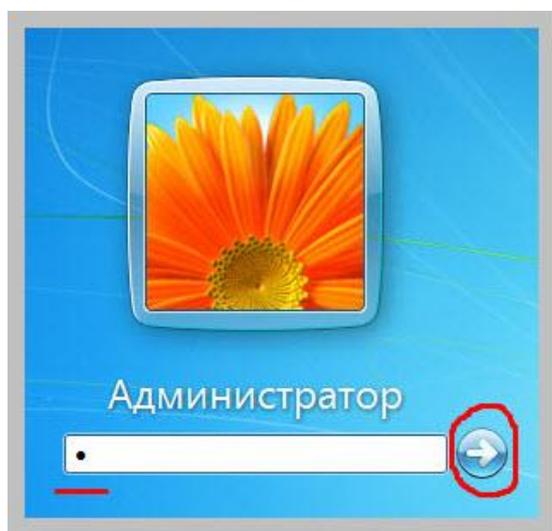
Нажимаем кнопку «Далее».

На этом, собственно, работа «мастера» заканчивается и нам напишут, что пароль будет изменен (сброшен) при следующей перезагрузке компьютера.



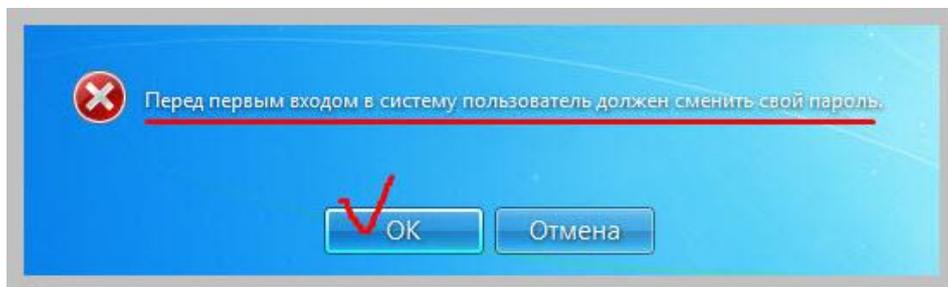
Нажимаем кнопку «Готово» и перезагружаемся!

При входе в учетную запись «Администратор» увидим окно ввода пароля.

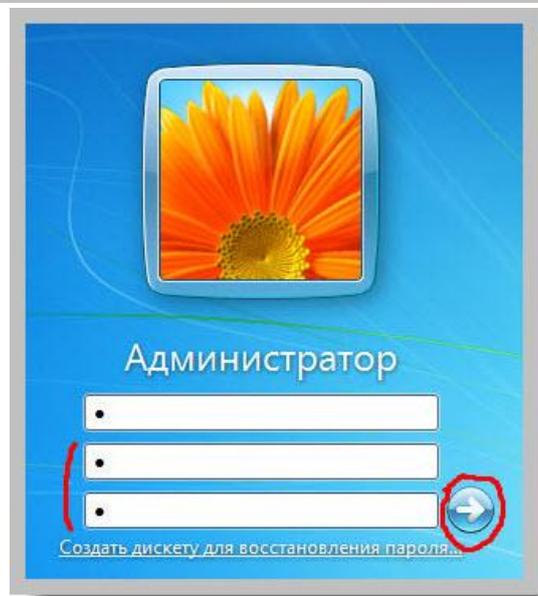


Вводим в него только что установленное нами значение (1).

Мы увидим вот такую надпись:

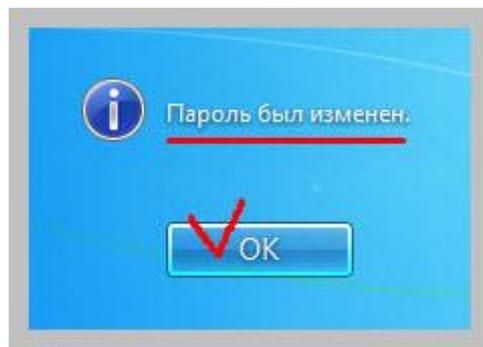


Нажимаем кнопку «ОК». Появится специальное окно изменения пароля. Здесь уже можем ввести тот пароль, который будет использоваться для входа в Windows (я просто ввел ту же единицу).

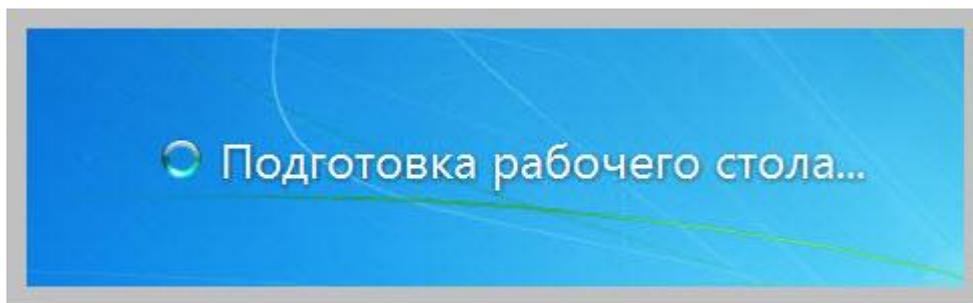


Нажимаем на кнопку со стрелкой.

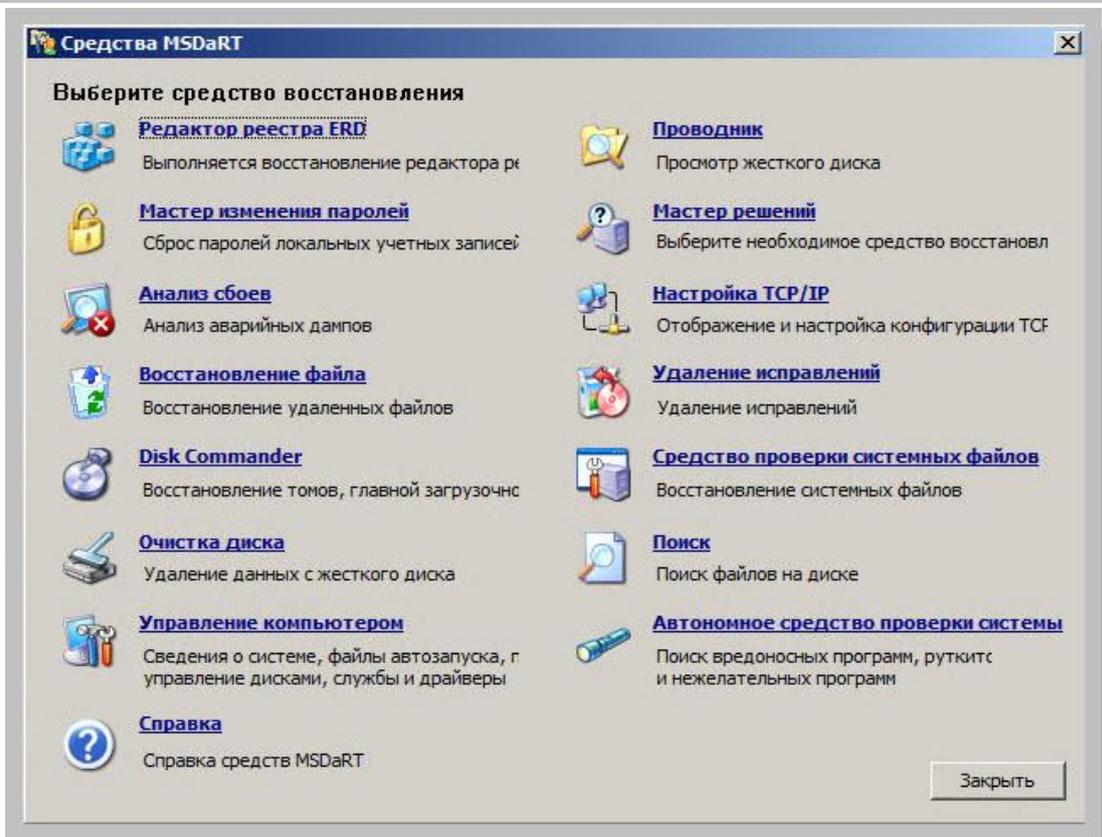
Вот теперь – все нормально!



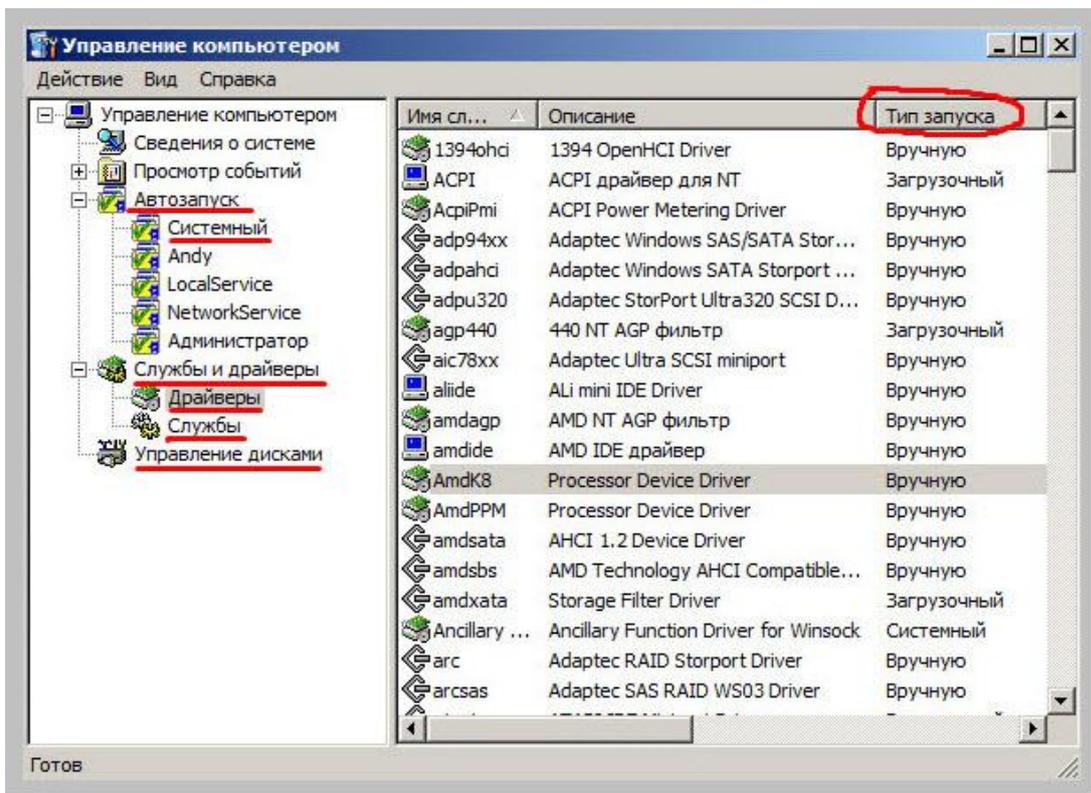
Пароль – изменен и началась загрузка рабочего стола Windows.



Давайте рассмотрим еще несколько интересных и весьма полезных при восстановлении системы инструментов из главного окна MSDaRT. Продублируем его здесь:



Первый инструмент на очереди – оснастка «Управление компьютером»:

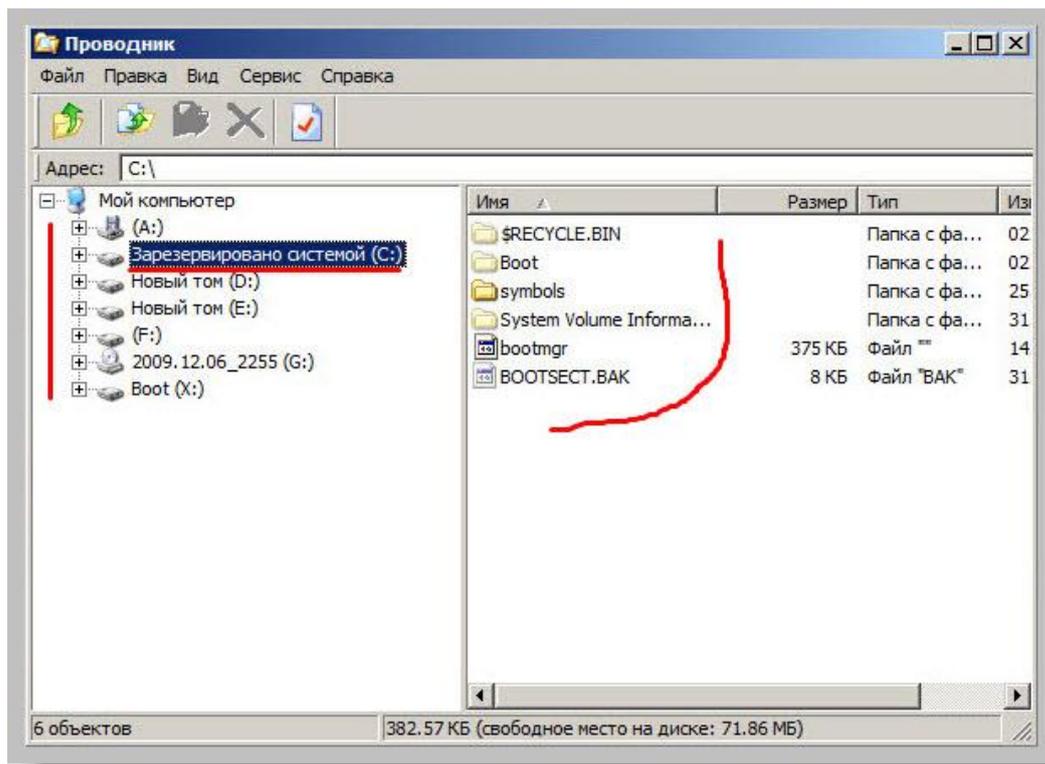


Незаменимая вещь в тех случаях, когда после установки какого-либо драйвера или системной службы, операционная система не загружается. Здесь мы можем, дважды кликнув на нужный нам драйвер (службу), в появившемся окне задать режим ее запуска (или вовсе отключить, тем самым восстановив загрузку ОС).

В разделе «Автозапуск» мы можем наглядно увидеть, какие приложения и сервисы запускаются вместе с Windows и внести, при необходимости, свои коррективы.

Раздел «Управление дисками» аналогичен одноименной оснастке самой Windows и позволяет производить простые манипуляции с разделами жесткого диска.

Следующий раздел, который поможет по быстрому «вытащить» нужные файлы с неработающего компьютера это – «Проводник». Здесь в удобном графическом интерфейсе мы получаем полный доступ к файловой системе и можем скопировать нужные нам файлы с компьютера, скажем, на флешку.



Совет: подключайте флеш-накопитель к компьютеру *перед его загрузкой*, и до *старта ERD Commander-а*. Тогда флешка будет корректно подмонтирована в систему.

Обратите внимание на скриншот выше: из среды ERD мы, по умолчанию, имеем полный доступ к скрытым файлам и папкам, а также – скрытому разделу восстановления Windows 7 (мы разбирали работу с ним в предыдущих уроках). На фото выше мы совершенно спокойно зашли на него и получили прямой доступ к загрузчику Windows (файл bootmgr) и другим системным файлам.

Пункт «Восстановление файлов» главного окна MSaRT позволяет восстанавливать случайно удаленные пользовательские файлы (сам не использовал, так как для этого есть много других специализированных утилит). Но, при случае, можете попробовать.

«Disk Commander» позволяет восстанавливать тома файловой системы в случае сбоя, а также – главную загрузочную запись (MBR – Master Boot Records).

«Мастер решений» - попытается помочь с общим определением проблемы и выбором между тем или иным из средств восстановления. Не пользовался (попробуйте - отпишетесь) ☺

«Настройка TCP/IP» призвана помочь нам настроить сеть прямо из среды ERD. Мы можем предоставить папки локального компьютера для общего использования и скопировать с него файлы по сети. Или же – выполнить обратную процедуру: подключить папки общего доступа удаленного компьютера, как сетевые диски к нашему ПК. Естественно, на удаленном компьютере, для папок должны быть выставлены соответствующие разрешения и права доступа.

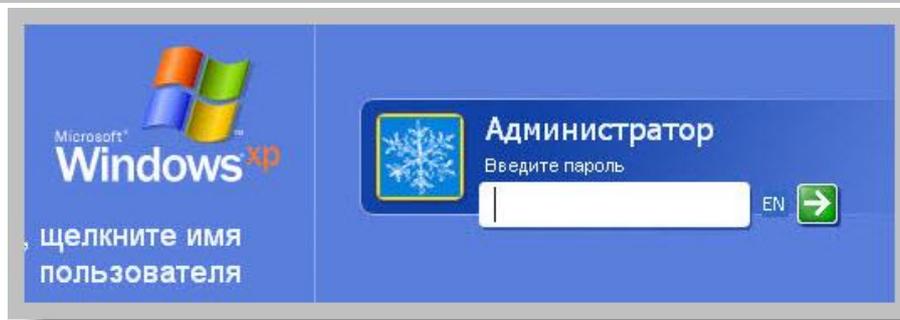
Пункт «Удаление исправлений» может быть эффективно использован в том случае, если нужно корректно удалить официальные исправления или сервиспаки операционной системы Microsoft Windows, если мы подозреваем, что проблема именно в них. Работает только в том случае, если для каждого конкретного исправления предусмотрен свой деинсталлятор!

«Автономное средство проверки системы» поможет выявить притаившихся на компьютере троянов и прочую «нечисть». Хотя, антивирусные сигнатуры, скорее всего, - будет иметь устаревшие, так что полностью полагаться на него не стоит.

Итак, основные возможности среды MSDaRT (она же – ERD) мы разобрали. При случае – еще раз Вам ее настоятельно рекомендую! Самой процедуре сброса пароля уделили достаточно внимания. Что еще можно сказать напоследок? Разве что, - кратко о том, как выглядят все те же действия применимо к ОС Windows XP (несмотря на свой почтенный возраст, она еще достаточно распространена среди пользователей).

Для того чтобы начать работать с Windows XP, нам нужно загрузить ERD Commander версии 5.0. Давайте кратко рассмотрим работу с ним на примере процедуры сброса пароля, рассмотренной нами выше для Windows 7.

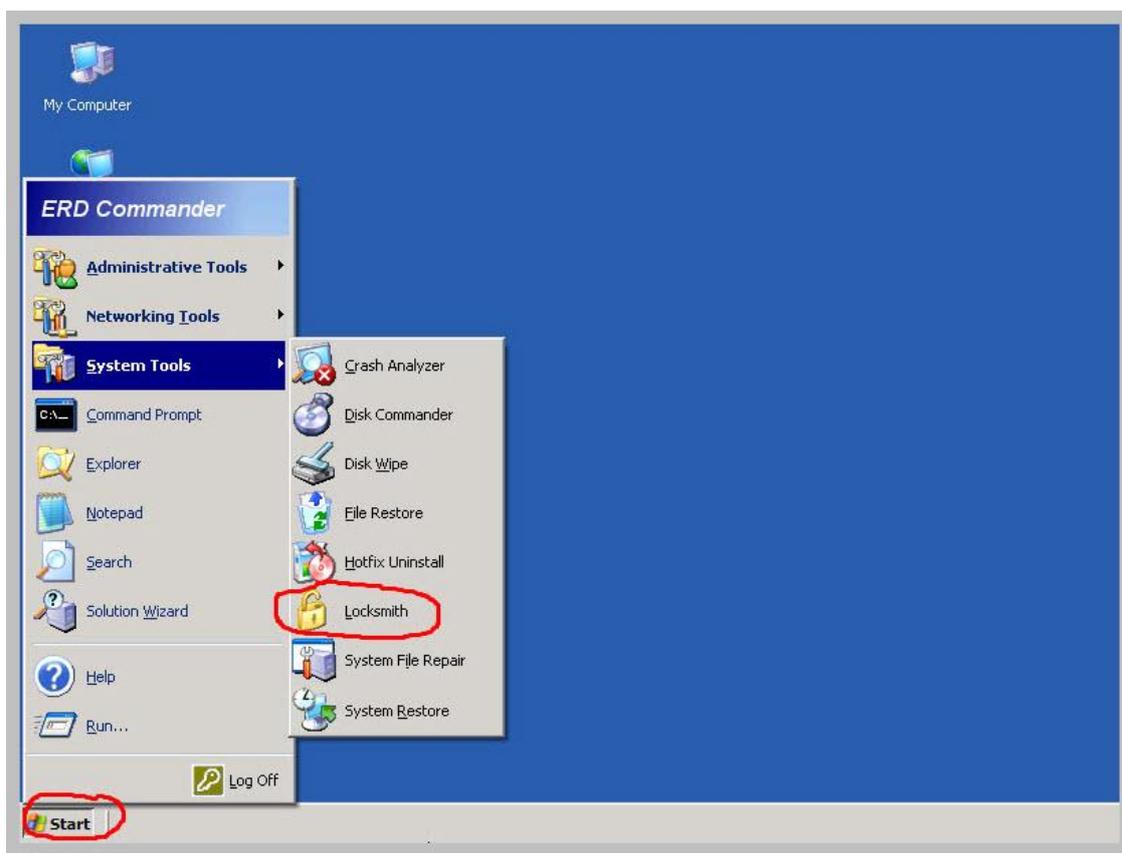
Вот - наш «неизвестный» пароль ☺



Загружаем ERD Commander 5.0



После завершения процесса загрузки, мы можем видеть почти полноценный рабочий стол Windows PE с кнопкой «Start», под которой собраны основные средства восстановления и управления системой.

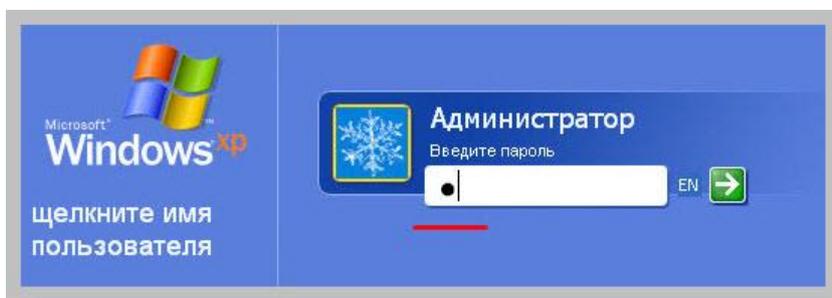


Все они, в основном, схожи с теми, что мы разбирали выше. Пункт, «Locksmith» (отмычка), отмеченный на фото выше, и есть инструментом сброса пароля для Windows XP.

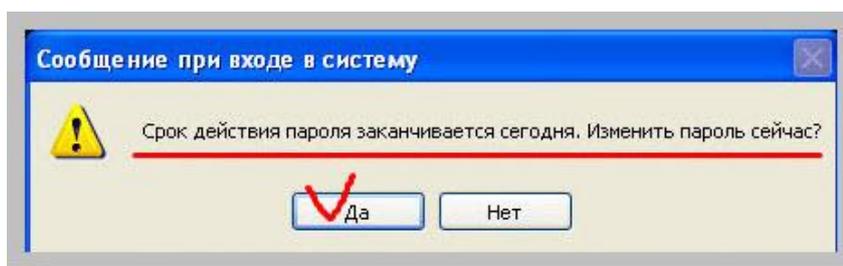
Работа с ним практически ничем не отличается от уже описанной нами процедуры:



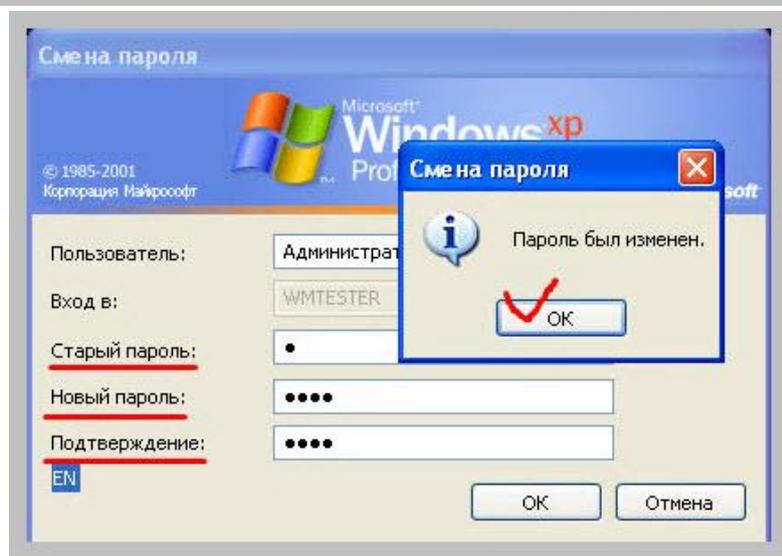
После установки нового пароля и перезагрузки вводим наш новый пароль в окно старта системы и нажимаем кнопку со стрелочкой.



Появится окно, которое визуально немного отличается от аналогичного в Windows 7, но по смыслу – совершенно идентичное:



После нажатия на кнопку «Да», нам будет предоставлена возможность ввести новый пароль:



Меняем пароль на свой и нажимаем кнопку «ОК». Теперь мы можем спокойно войти в систему!

Вот теперь – действительно ВСЕ! Думаю, что о сбросе пароля в Windows авторы данного руководства рассказали достаточно, а заодно – познакомили Вас с такой полезной, хотя и неудобопроизносимой вещью, как MSDaRT ☺

Урок взят с сайта: <https://sebeadmin.thelogos.in.ua>

До встречи в следующих уроках !