

Пошаговые Руководства

Сам Себе Админ

системное администрирование

Microsoft Windows



Играем в «игры» с загрузчиком Windows 7

В сегодняшнем нашем уроке я хочу (у Вас на глазах) добиться полной неработоспособности операционной системы Windows 7, а после этого – восстановить ее загрузку! Проще говоря, поломать, а потом – исправить! Убежден, что это – лучший способ чему-то научиться на практике (особенно, если «ломает» кто-то другой а наблюдающий – смотрит и «на ус мотает») ☺

Если помните, в одной из статей на нашем сайте (https://sebeadmin.thelogos.in.ua/ntldr_is_missing_kak_ispravit.html) мы подробно рассматривали принцип загрузки операционной системы Windows XP и решали проблему с ее загрузчиком **NTLDR**.

В статье мы упомянули о том, что с Windows 7 – история другая и за ее загрузку отвечает файл **winload.exe**. Это – так, но... не совсем ☺ Читайте дальше и я постараюсь максимально этот вопрос прояснить.

Но перед этим, позвольте рассказать Вам очередную небольшую байку из жизни нашего IT отдела. Как Вы знаете, территория нашего предприятия – достаточно большая, а компьютерная сеть насчитывает около 400 машин.

Бывает так, что нужно оперативно решить какой-то рабочий вопрос (например: провести инвентаризацию или плановую профилактику конкретного ПК), а для этого нужен компьютер пользователя. Притом, что рабочее место этого пользователя находится черт знает где на территории предприятия. Чтобы самому не идти туда и не нести системный блок оттуда, мы придумали такую штуку: по сети заходим на нужный нам компьютер и удаляем на нем файл загрузчика ntldr (предварительно скопировав его себе). После следующей перезагрузки пользователь видит на мониторе надпись NTLDR is missing (загрузчик поврежден) и сам звонит нам, а мы уже – благодушно разрешаем ему принести компьютер к нам на ремонт. Естественно, подобная процедура происходит только если «клиент» это – «мужчина в самом расцвете сил»!) ☺

Думаю, понятно, что «ремонт», в данном случае, ограничивается простым возвращением файла на его законное место! Мы получили нужный нам компьютер, а пользователь через час-два - своего «отремонтированного» железного друга, заходит к нам и с благодарностью уносит его к себе на рабочее место, все – довольны!

К чему я это рассказываю? А к тому, что в случае с Windows 7 у нас такой фокус проделать не получится. Дело в том, что существовавший еще со времен Windows NT, загрузчик операционной системы NTLDR, начиная с Windows Vista, заменен новым диспетчером загрузки **BOOTMGR**. Официальная версия звучит примерно так: старый добрый **NTLDR** уже не годился для выполнения загрузки системы на компьютерах, использующих спецификацию **EFI** (Extensible Firmware Interface – расширенный интерфейс микропрограмм). Это «чудо» (EFI) призвано заменить уже привычную базовую систему ввода-вывода - **BIOS** (basic input-output system - базовая система ввода-вывода) ☺

Модель EFI является новым поколением реализации интерфейса между оборудованием компьютера и операционными системами, и в недалеком будущем (как по мне, – к сожалению) полностью заменит просуществовавшую несколько десятилетий модель BIOS.

Давайте, для лучшего понимания описываемых ниже действий, немного порассуждаем теоретически.

Для начала, вкратце рассмотрим процесс загрузки операционных систем семейства Windows. Загрузка любой операционной системы начинается всегда одинаково: после проверки оборудования, управление получает BIOS, который считывает с устройства загрузки первый сектор, являющийся главной загрузочной записью MBR (Master Boot Record). Стандартно **MBR** располагается в первом секторе загрузочного диска и занимает 512 байт. Это, к слову, - не обязательное условие и MBR может занимать более одного сектора, что зависит от конкретной разновидности загрузчика.

После считывания в оперативную память компьютера, программный код начального загрузчика получает управление и выполняет поиск активного раздела (Active Partition), - раздела, с которого может выполняться загрузка конкретной операционной системы. Такой раздел имеет свою загрузочную запись, называемую загрузочной записью раздела **PBR** (Partition Boot Record). Конкретное содержимое загрузочной записи активного раздела зависит от загружаемой операционной системы.

В случае с загрузкой Windows 7 (а также Windows Vista, Server 2008 и т.д., программный код загрузчика раздела выполняет подготовку и запуск следующего этапа загрузки системы. А именно - считывания в оперативную память и передачу управления специальной программе - диспетчеру загрузки **BOOTMGR**.

Диспетчер загрузки представляет собой файл небольшого размера, расположенный в корневом каталоге активного раздела. Основное его предназначение - обеспечение дальнейшей процедуры загрузки в соответствии с существующей конфигурацией, хранящейся в специальном хранилище. Это - хранилище данных конфигурации - BCD (Boot Configuration Data). Оно представляет собой файл с именем BCD, находящийся в каталоге BOOT активного раздела. По своей структуре, файл BCD является кустом реестра и отображается в редакторе реестра, как раздел HKEY_LOCAL_MACHINE\BCD0000000х. Следующий этап загрузки операционной системы обеспечивается уже диспетчером bootmgr в соответствии с существующей конфигурацией.

При стандартной установке операционной системы Windows 7 на новый жесткий диск, в качестве активного раздела используется автоматически создаваемый при инсталляции раздел небольшого размера (100Мб). Это - скрытый системный раздел, на котором хранятся некоторые системные файлы и загрузчик **bootmgr**. Данному разделу не присваивается буква, и в проводнике он не отображается. Это сделано с целью защиты загрузчика от «кривых» рук пользователя и, видимо, чтобы мы, как администраторы, не могли удалить его по сети ☺

Скрытый раздел также используется для **WRE** (Windows Recovery Environment – среды восстановления Windows). О ней мы уже говорили в одной из статей нашего сайта (https://sebeadmin.thelogos.in.ua/ne_udaetsya_zapustit_windows_iz_z_ntoskrnl.html).

Windows RE построена на основе Windows PE (Windows Preinstallation Environment). Среда Windows PE) это - минимальная версия операционной системы Win32 с ограниченными возможностями и минимальным набором служб.

Среда PE эффективно заменяет собой, уже набивший всем оскомину MSDOS, если надо подготовить диск к установке операционной системы («format» и другие дисковые операции). Она также позволяет автоматизировать установку Windows, предоставляет доступ к NTFS дискам, файлам и системному реестру для резервного копирования и восстановления работоспособности системы. Поддерживает работу по сети.

Если говорить коротко, то одним из основных назначений «Windows Recovery Environment» является автоматизация диагностики и устранения неполадок загрузки операционной системы.

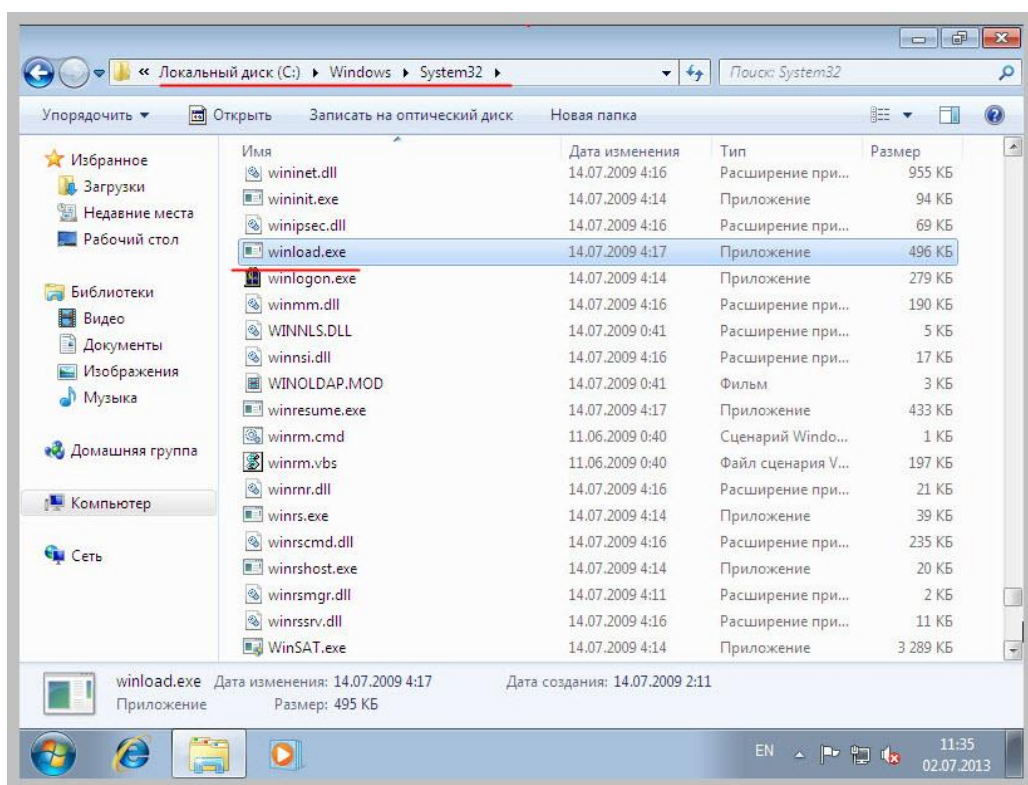
Уф, что-то многовато теории получилось (не люблю) ☺ Ну, ничего! Дальше пойдет только практика!

Начнем с простого. Попробуем удалить один из компонентов загрузчика: Winload.exe

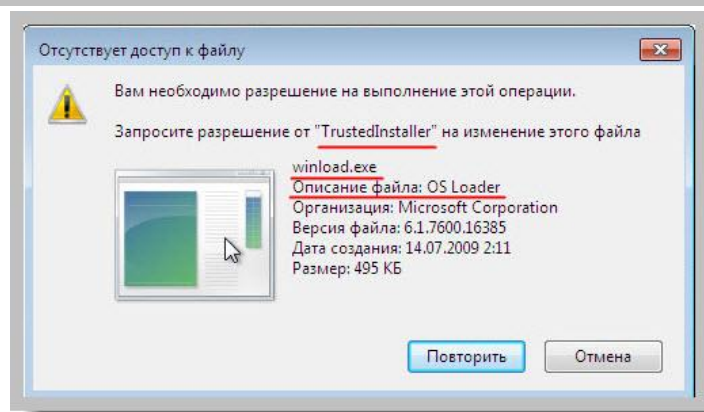
Примечание: на одном из этапов менеджер загрузки (bootmgr) передает дальнейшее управление загрузкой файлу Winload.exe, который выполняет следующие важные операции:

1. Загружает ядро операционной системы Ntoskrnl.exe и уровень аппаратных абстракций HAL.dll (<https://sebeadmin.thelogos.in.ua/hal-dll-otsytstvyet-or-povrejden.html>).
2. Подготавливает файлы национальных языковых систем
3. Считывает раздел реестра \Windows\System32\Config\System для определения драйверов устройств необходимых для старта операционной системы
4. Загружает системные драйверы из загрузочного раздела. В это время для пользователя отображается текст «Запуск Windows» с символикой операционной системы

На скриншоте ниже мы видим список файлов директории System32 на Windows 7 и присутствующий там файл winload.exe.



Попробуем удалить его кавалерийским наскоком: нажимаем на нем правой кнопкой мыши и выбираем одноименный пункт. Не тут-то было! ☺ Мы увидим вот такую картину.



Запросите разрешение от «TrustedInstaller» на изменение этого файла.

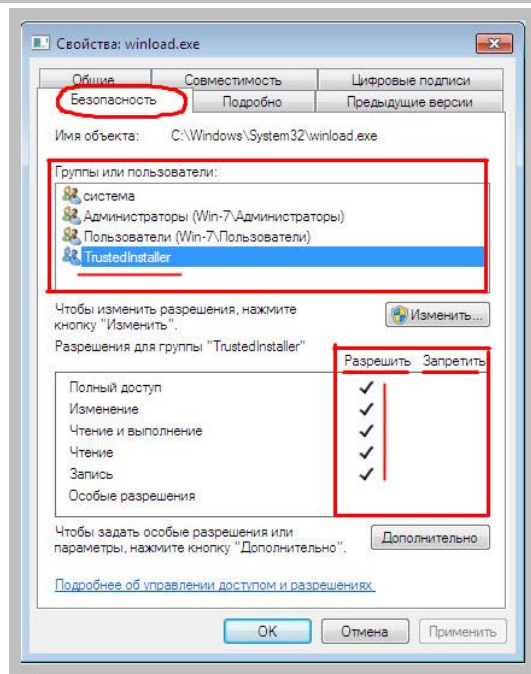
Операционная система не дает нам удалить этот файл (даже если мы пытаемся сделать это от имени администратора компьютера).

Почему так происходит? Дело в том, что многие важные файлы защищены самой ОС от удаления на уровне файловой системы NTFS.

Примечание: NTFS – (New Technology File System - файловая система новой технологии). Она имеет встроенные возможности разграничения доступа к данным для различных учетных записей и групп пользователей (при этом используются списки контроля доступа ACL - Access Control List). Также в ней можно назначать квоты (ограничения на максимальный объём дискового пространства, занимаемый теми или иными пользователями).

Давайте разберемся с этим моментом на конкретном примере. Нам ведь нужно все таки удалить этот злополучный winload.exe? Нажимаем на нем правой кнопкой мыши и из появившегося списка выбираем пункт «свойства».

Появится окно, в котором нам нужно будет перейти на вкладку «безопасность»:



Обратите внимание на области, заключенные в красные рамки. Верхняя содержит список групп пользователей, зарегистрированных на компьютере. Каждый пользователь компьютера обязан принадлежать, по крайней мере, к одной из групп (может и к нескольким одновременно). В зависимости от этой принадлежности он наделяется определенными правами в системе.

Нижняя обведенная область показывает нам текущие права доступа к конкретному объекту (в данном случае – к файлу winload.exe).

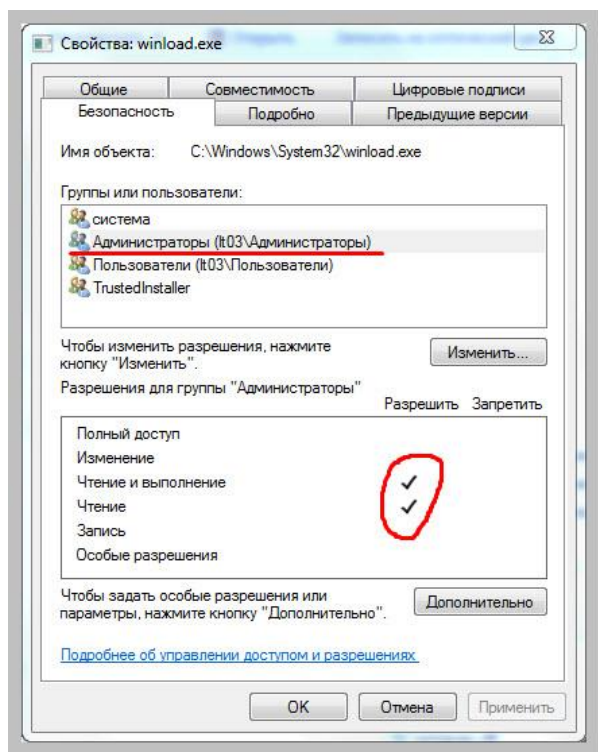
Что мы видим на фото выше? Группа пользователей «TrustedInstaller» (верхняя часть окна) имеет полный доступ к файлу winload.exe. Под полным доступом подразумевается:

- Изменение
- Чтение и выполнение
- Чтение
- Запись
- Полный доступ – разрешает управлять галочками, расположенными под ним

Видите, напротив всех этих пунктов стоят эти самые «галочки»? Убирая и ставя их мы можем тонко настраивать особые режимы доступа к файлам и папкам в файловой системе NTFS.

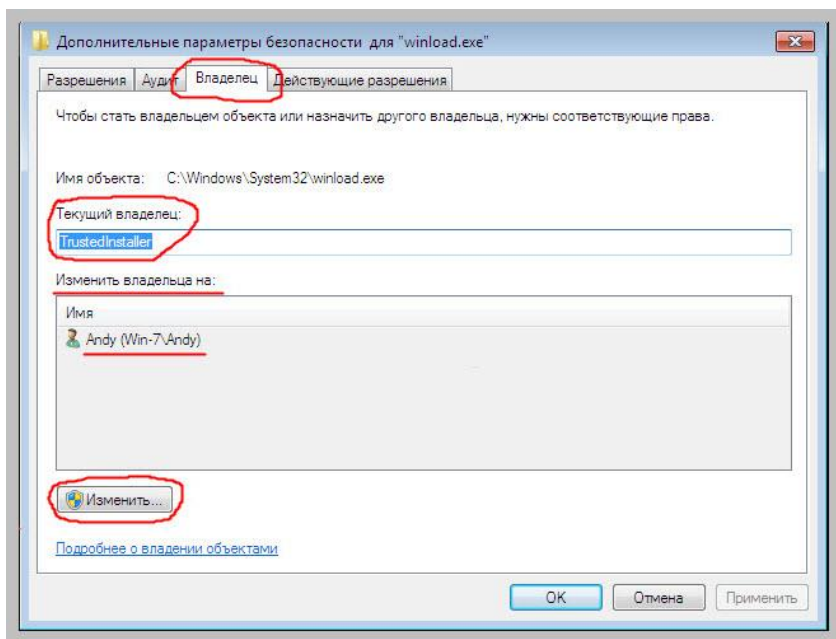
Примечание: группа «TrustedInstaller» является встроенной системной учетной записью с привилегированными правами, от имени которой в ОС выполняются некоторые действия и процессы.

Наша проблема состоит в том, что даже для группы «Администраторы» разрешения для файла по умолчанию выставлены, как «чтение и выполнение» и «чтение».



Что можно придумать? Давайте воспользуемся методом, который я всегда применяю в подобных ситуациях. Для этого на скриншоте выше нажимаем кнопку «Дополнительно» и в появившемся окне переходим на вкладку «Владелец».

Присмотримся к скриншоту ниже:



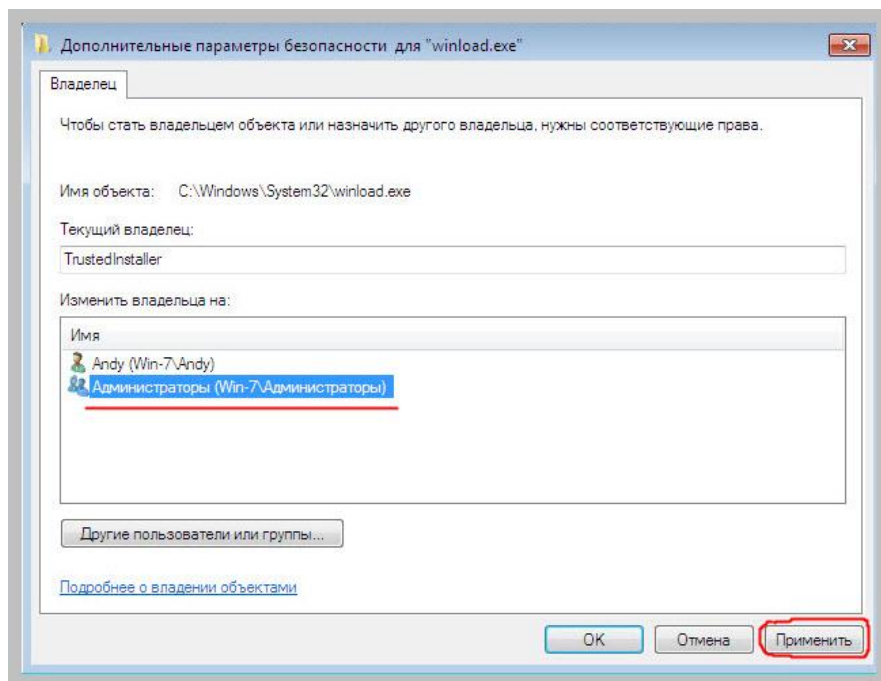
На нем мы видим, что текущим владельцем объекта (нашего файла winload.exe является все тот же TrustedInstaller).

Примечание: владелец объекта по умолчанию имеет неограниченный доступ к нему и может производить с объектом любые операции (удаление, изменение и т.д.)

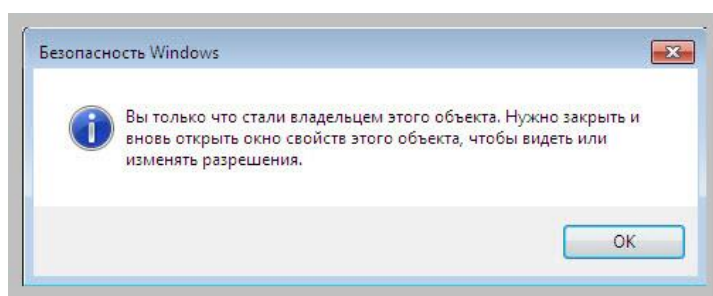
А группа «Администраторы» имеет возможность менять владельца объекта. И вот именно в этом кроется возможность, которая просится, чтобы ее использовали 😊

На скриншоте выше нажимаем кнопку «Изменить» и в текстовом поле, которое имеет название «Изменить владельца на», выбираем пользователя (или группу пользователей), который и станет новым владельцем объекта.

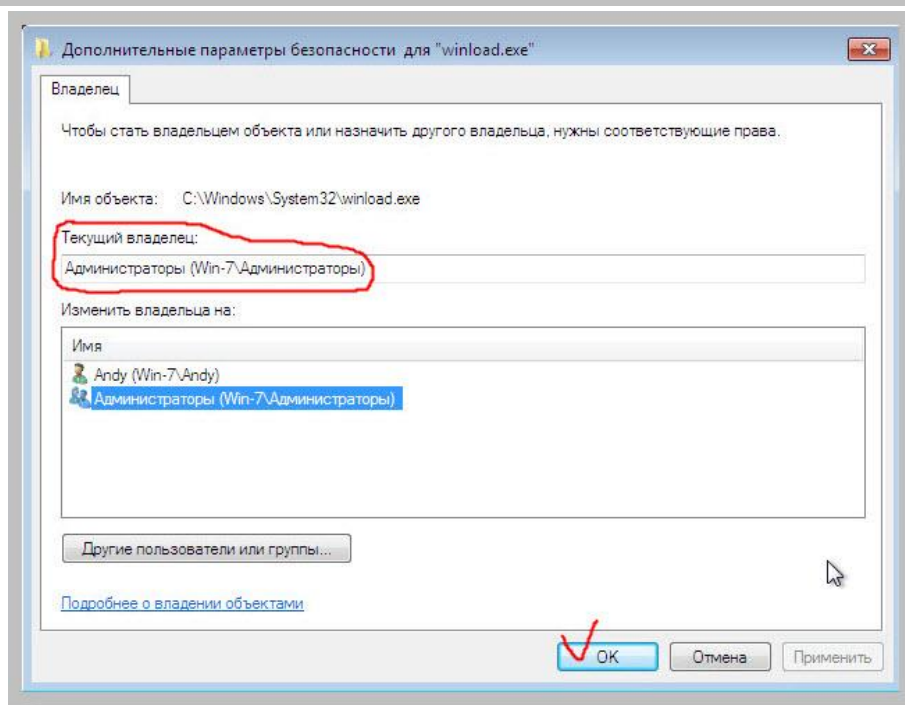
Я выбрал встроенную группу «Администраторы». Нажимаем кнопку «Применить».



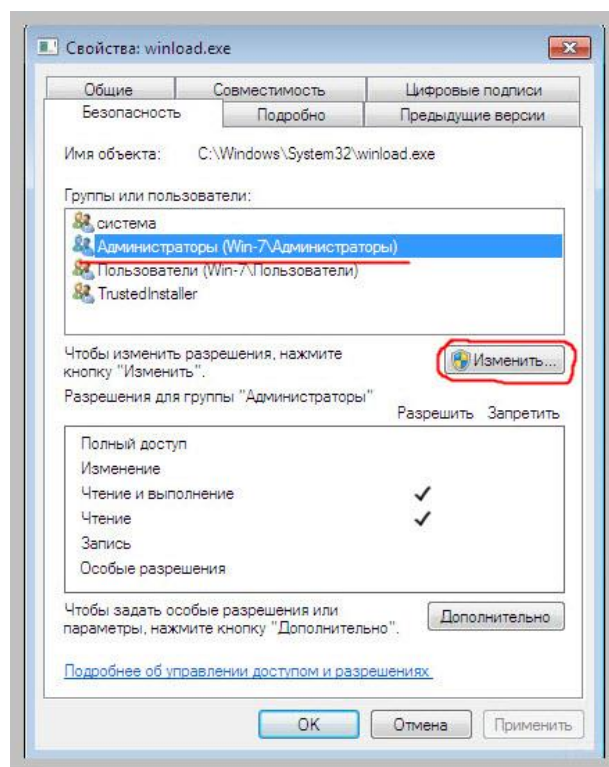
Увидим информационное окно следующего содержания:



Сделаем так, как нам предлагают и убедимся, что владелец объекта поменялся. Теперь файлом владеет группа «Администраторы», в которую мы и входим 😊



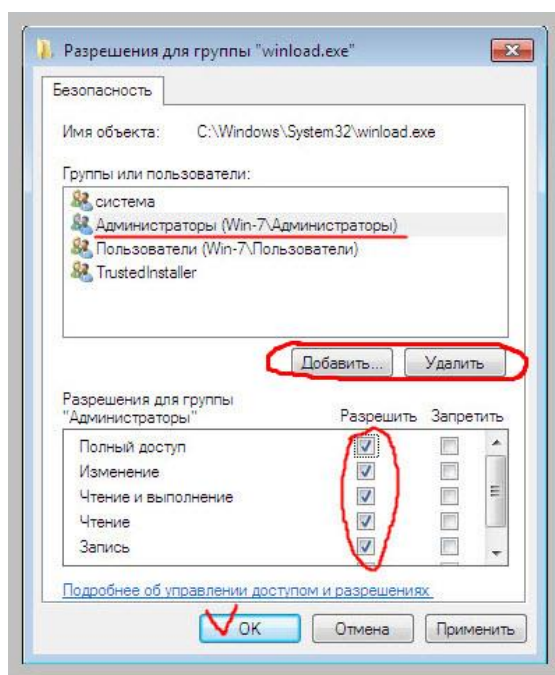
Нажимаем кнопку «ок» и возвращаемся в окно назначения прав:



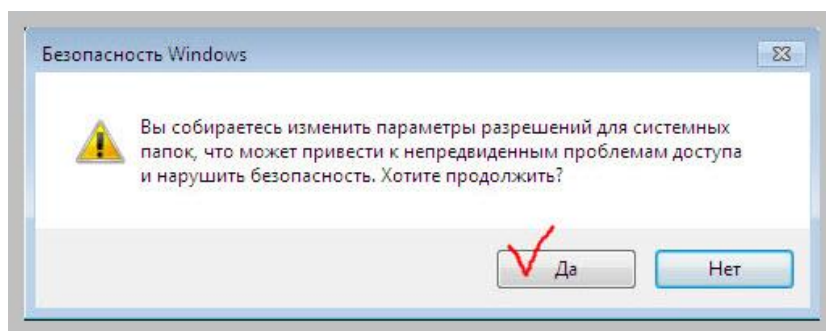
Визуально в нем, вроде бы, ничего не изменилось, НО, все же, есть одно очень важное отличие, которое становится очевидным после того, как мы нажмем на кнопку «Изменить».

Становятся доступными кнопки «Добавить» и «Удалить», которые до смены владельца файла были не активными для нашей учетной записи, а также – появляется возможность напрямую редактировать разрешения (выставить нужные нам галочки).

Даем группе «Администраторы» полный доступ к объекту winload.exe (ставим все пять галочек) и нажимаем кнопку «ОК».

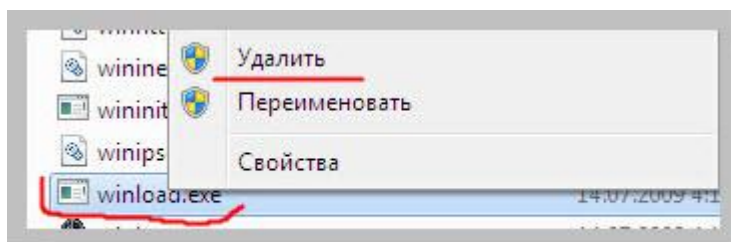


Windows начинает «нервничать» и показывает нам вот такое предупреждение:

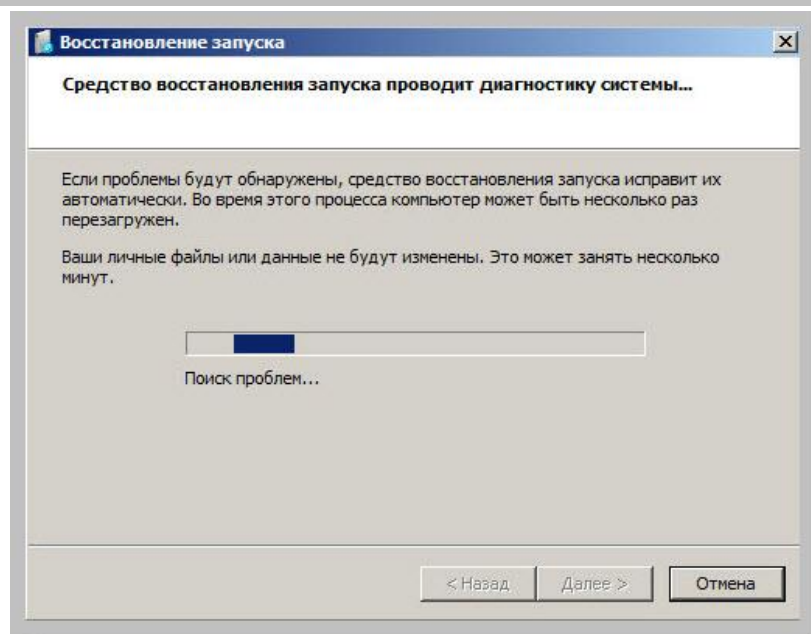


Полностью осознавая всю тяжесть возможных последствий, и находясь в здравом уме и твердой памяти, нажимаем «ОК» ☺

После этого, еще раз нажимаем на файле winload.exe правой кнопкой мыши и из раскрывшегося меню выбираем пункт «Удалить».

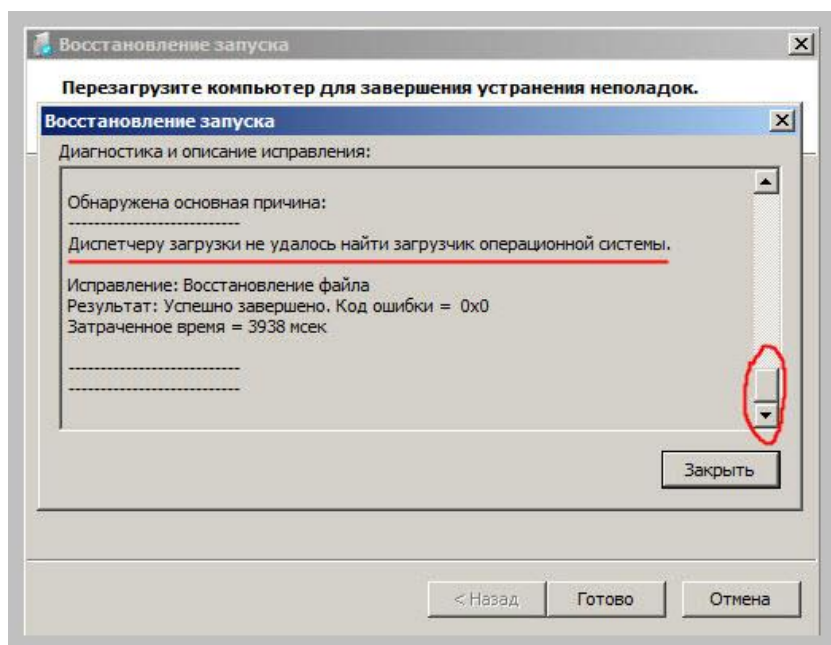


Ура! На этот раз мы беспрепятственно удалили один из компонентов загрузчика Windows ☺ Для того, чтобы что-то «почувствовать» нужно перезагрузиться. Сделаем это!



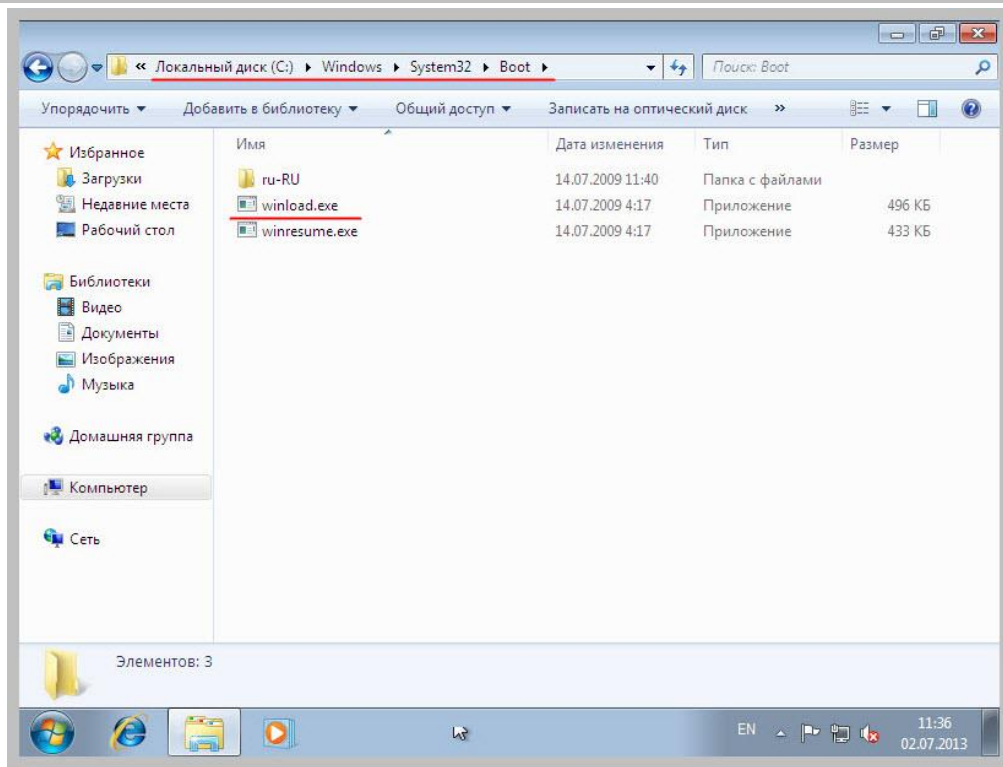
После перезагрузки мы увидим окно запустившейся WRE (Windows Recovery Environment – среды восстановления Windows). О ней мы говорили в начале данной статьи, так что не будем повторяться.

После окончания автоматической проверки и самовосстановления системы мы увидим окно в котором будет ссылка «Показать подробности восстановления», если мы нажмем ее то появится еще одно окно, прокрутив книзу которое, мы увидим причину неисправности и информацию о результатах восстановления:

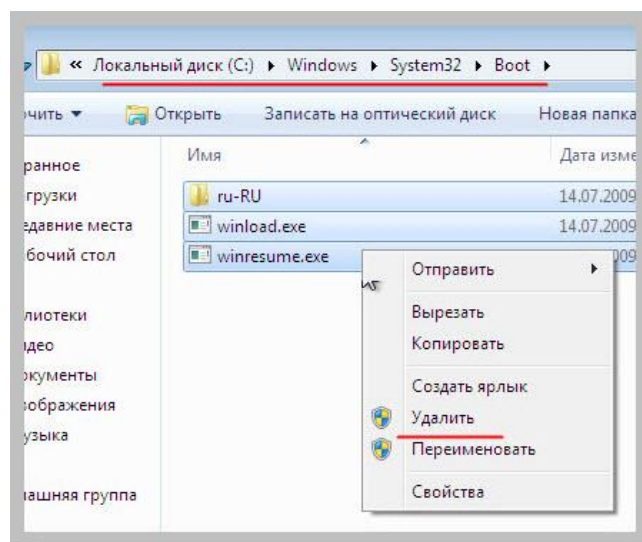


Закрываем это окно и перезагружаемся. Система Windows 7 успешно запустится. Удаленный нами файл winload.exe был восстановлен автоматически!

Также нам стоит знать, что полная резервная копия данного файла находится по адресу `\\windows\system32\boot\winload.exe`



Возможно, Windows 7 восстанавливает его именно оттуда? Давайте проверим это предположение! На всякий случай, я удалил все, что было в каталоге boot на своем компьютере (для этого придется прибегнуть к описанной нами выше процедуре смены владельца и назначения прав доступа).



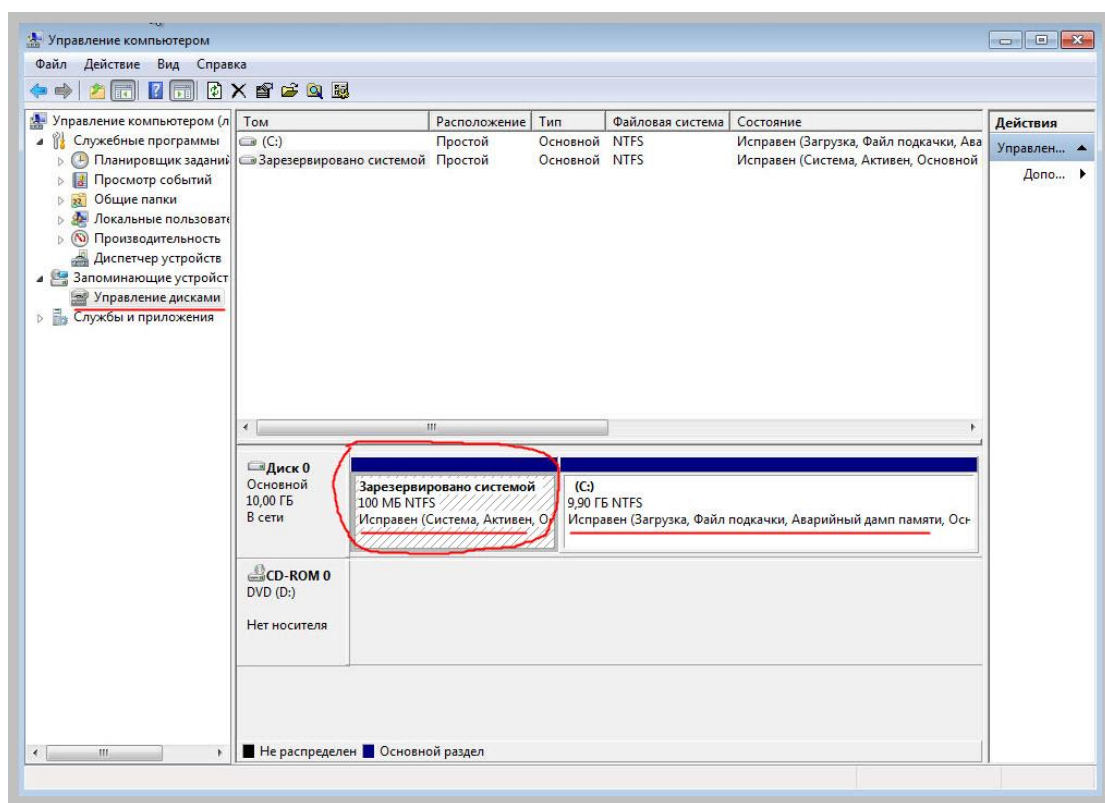
После этого – снова убрал ранее восстановленный файл «winload.exe» из каталога «system32» и перезагрузил компьютер. Но и после этого система была успешно восстановлена в автоматическом режиме! Что интересно: в каталоге «boot» файл «winload.exe» больше не появился, так что будьте осторожнее с его удалением оттуда (просто знайте, что он там есть) ☺

Так откуда же Windows берет этот файл, если мы даже удалив его резервную копию не можем «положить» систему?

Самое время вспомнить о том небольшом скрытом разделе жесткого диска в 100 мегабайт, который Windows 7 создает при своей первоначальной установке. Возможно, именно на этом разделе и находится WRE (среда восстановления), которая и запускается в нужный момент при проблемах с загрузкой?

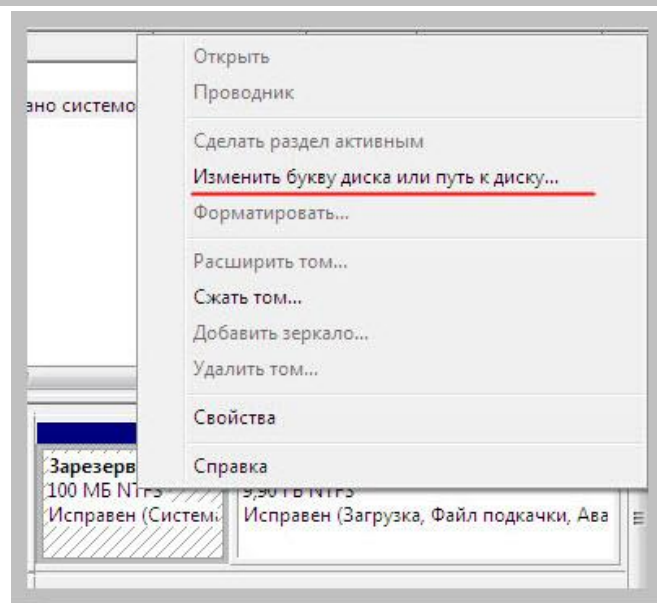
Давайте проверим и это высказывание!

Нажимаем правой кнопкой мыши на пиктограмме «Мой компьютер», расположенной на рабочем столе и из появившегося меню выбираем пункт «Управление». В появившемся окне (оснастке) переходим в раздел «Управление дисками»:

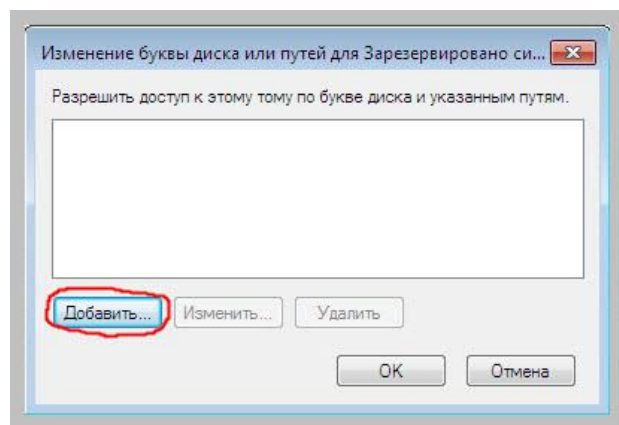


Мы четко видим, что перед основным диском «C» у нас находится область в 100 мегабайт. Причем, этот небольшой раздел отмечен как системный и активный (тот, с которого и происходит загрузка Windows)! Что же там на нем спрятано? Полюбопытствуем! ☺

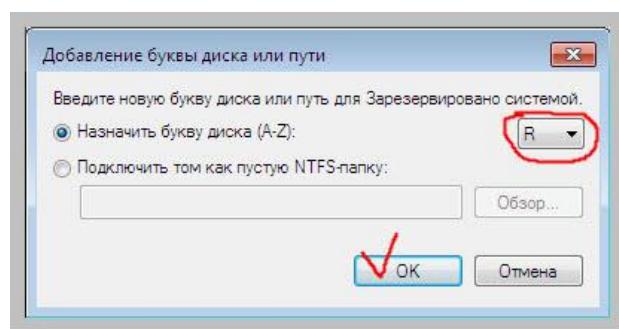
Нажимаем на нем правой кнопкой мыши и из появившегося меню выбираем пункт «Изменить букву диска или путь к диску»:



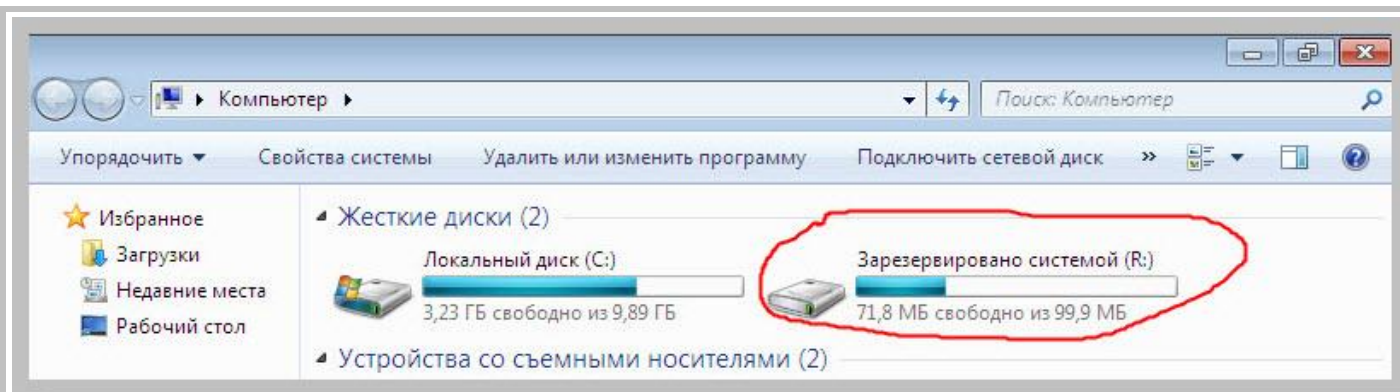
Появится окно, где нам предложат присвоить разделу любую незанятую букву диска. Нажимаем на кнопку «Добавить»:



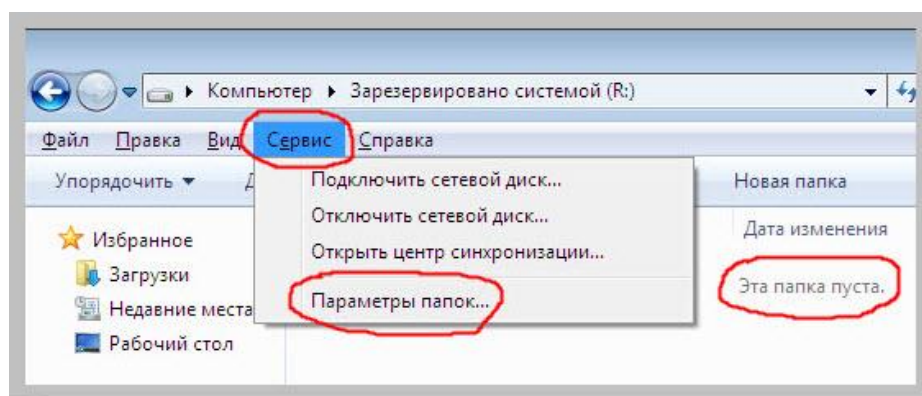
В следующем небольшом окошке из раскрывающегося списка справа выбираем любую понравившуюся букву и нажимаем кнопку «ОК»:



После этого наш диск появится в проводнике Windows под той буквой, которую мы ему назначили!

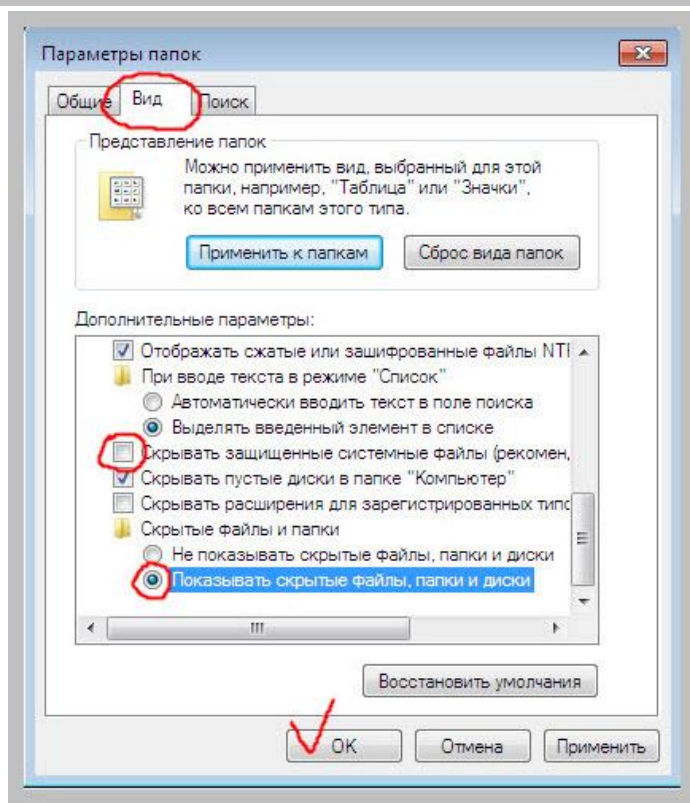


Зайдем на него! Досадно, но никаких файлов мы там не увидим. Все они – скрыты.



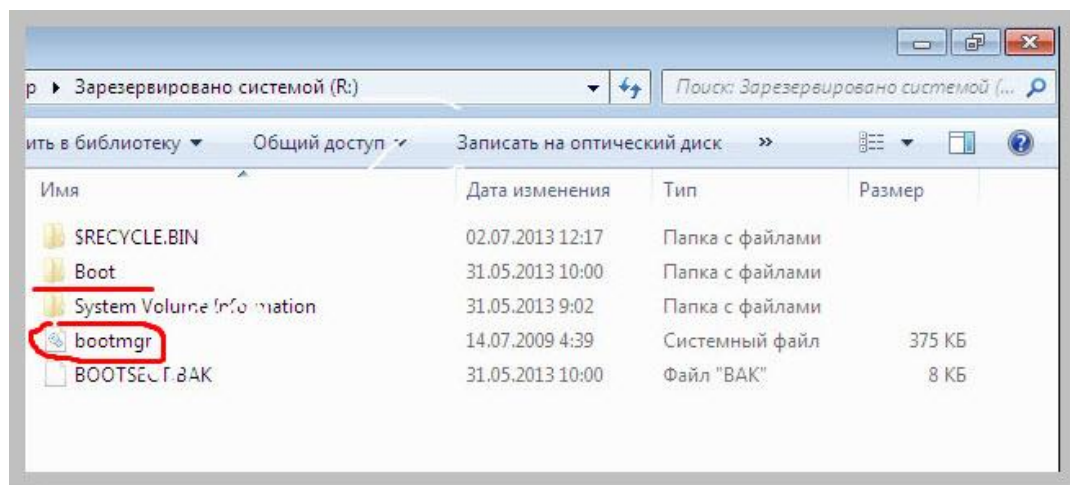
Но такой пустяк нас, как сам себе админов, останавливать не должен, поэтому нажимаем на клавиатуре клавишу «**Alt**» и из появившегося за этим верхнего меню проводника выбираем пункт «**Сервис**». В его меню переходим к пункту «**Параметры папок**».

В появившемся окне переходим на вкладку «**Вид**» и среди многочисленных параметров отображения папок находим два, интересующие нас в данный момент: «**Скрывать защищенные системные файлы**» (снимаем галочку возле него) и «**Показывать скрытые файлы, папки и диски**» (выбираем).



Нажимаем кнопку «ОК».

После этого все наши «невидимые» файлы сразу же появляются!



Здесь в каталоге boot мы можем найти хранилище данных конфигурации - BCD (Boot Configuratin Data) – одноименный файл куста реестра, о котором мы говорили в начале данной статьи. А вот и сам, спрятанный от шаловливых рук и дурного глаза, диспетчер загрузки – файл **bootmgr** ☺

Что мы с ним сделаем? Правильно – удалим немедленно! ☺ Про процедуру смены владельца и назначения прав доступа помним? Вот и отлично!

После удаления файла bootmgr и перезагрузки системы мы вместо загрузки Windows увидим вот такую надпись:

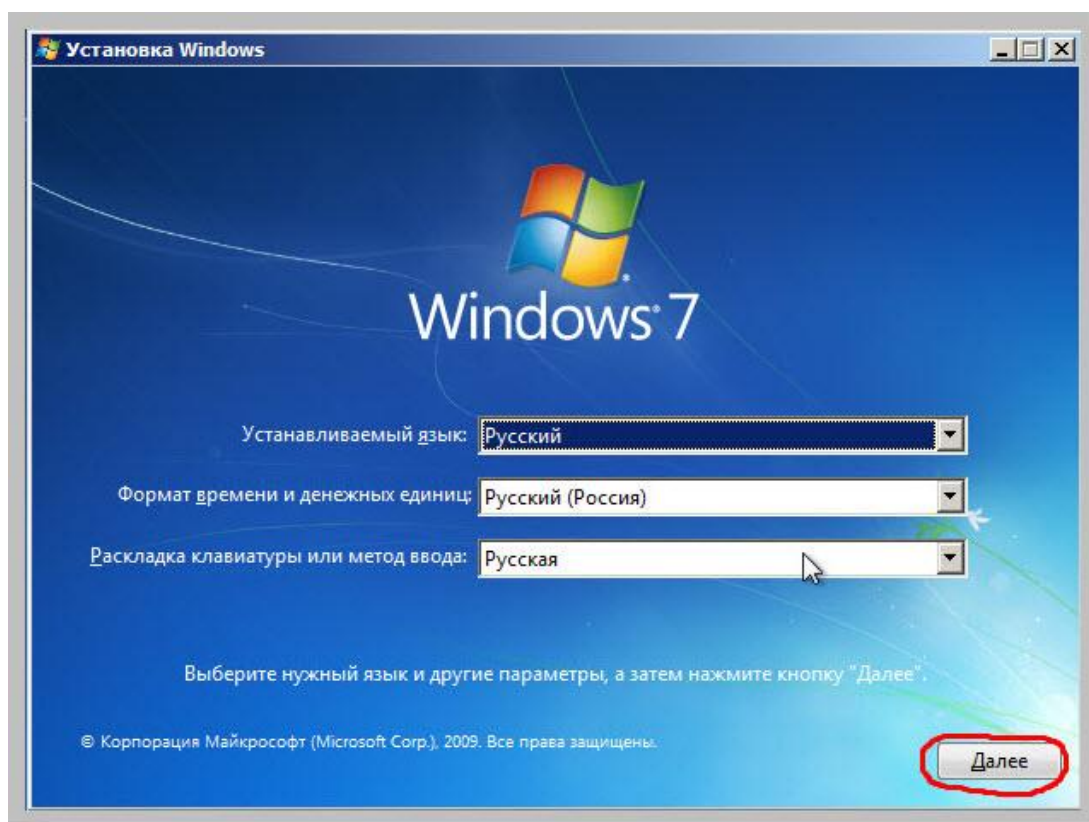
```
BOOTMGR is missing
Press Ctrl+Alt+Del to restart
```

Можем себя поздравить: мы только что таки «уложили» Windows 7! Правда, для этого пришлось изрядно пощелкать мышкой ☺

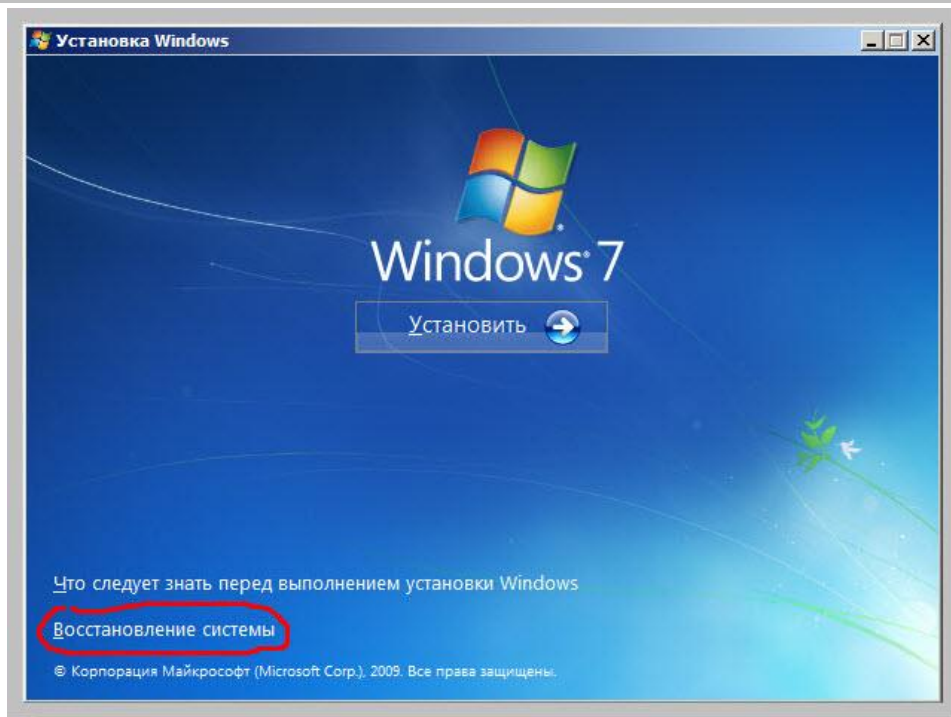
Как видите, без данного файла среда восстановления не смогла запуститься в автоматическом режиме. Оно и понятно: ее загрузчик-то отсутствует.

Не беда! Давайте немного поможем Windows! Берем установочный диск (тот с которого мы инсталлировали систему) и помещаем его в привод оптических дисков. Выставляем в bios-е с него загрузку и перезагружаемся.

При старте нам будет предложено нажать любую кнопку, чтобы выполнить загрузку с DVD. Нажимаем. После этого начнется чтение информации с нашего компакт диска и через некоторое время мы увидим окно мастера установки системы:

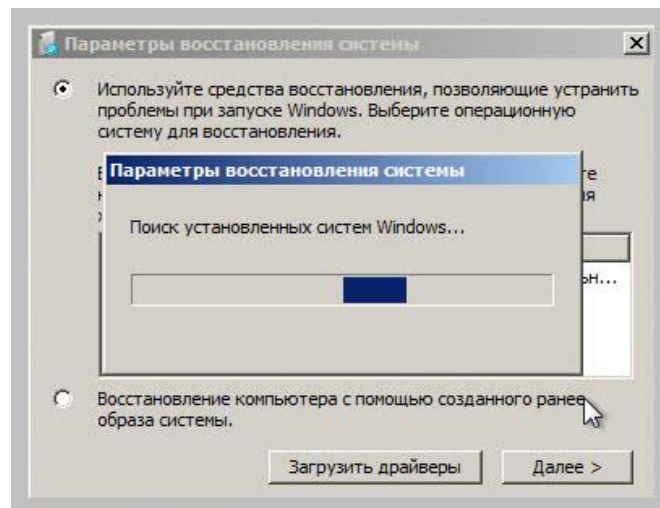


Нажимаем кнопку «Далее» и переходим к следующему шагу:

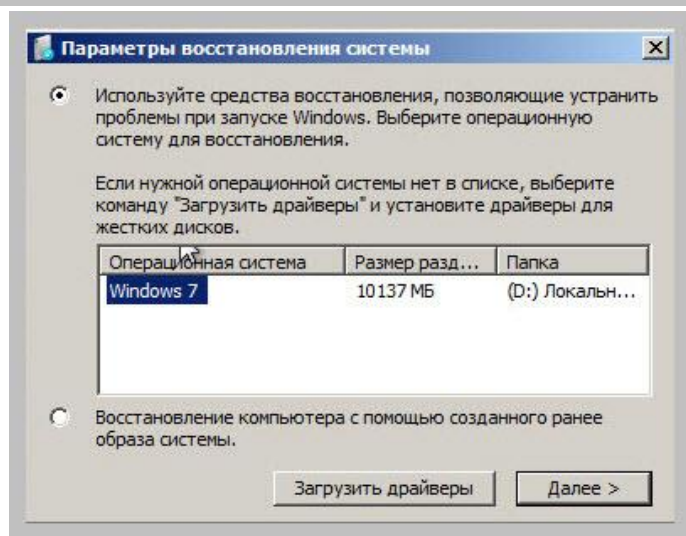


Вот здесь нам нужно будет нажать на ссылку «Восстановление системы», после чего запустится расширенная среда восстановления (WRE), находящаяся на компакт диске.

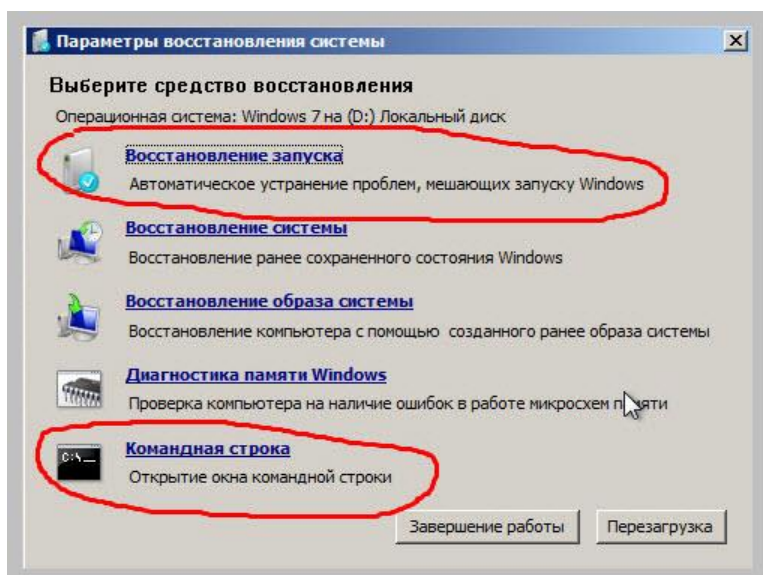
Первым шагом в ней будет выполнен поиск установленных на компьютере операционных систем:



На скриншоте ниже видим этот список:

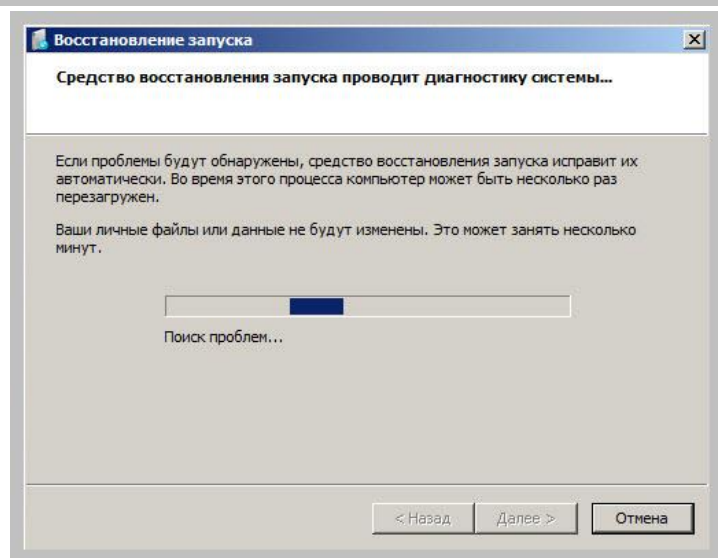


После того, как система будет найдена, нам остается нажать кнопку «Далее». Появится окно, в котором мы можем выбрать один из вариантов восстановления:

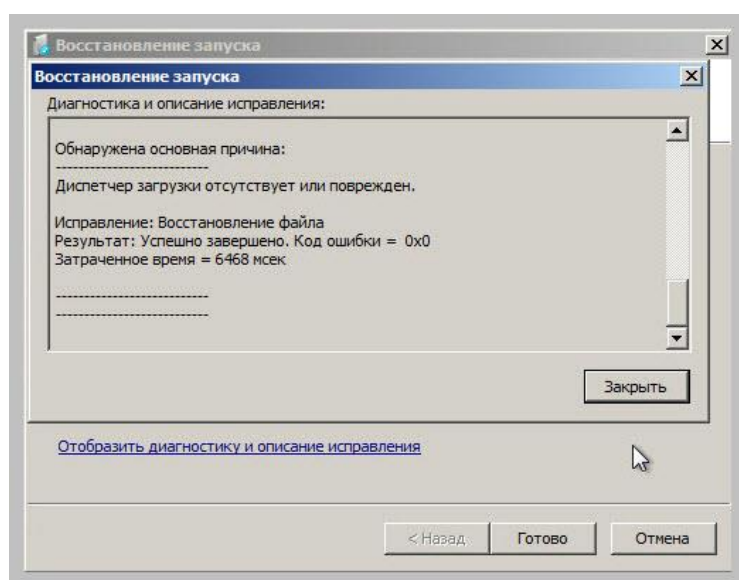


Сразу скажу, что нам, в первую очередь, интересны первый и последний пункты (именно их мы и рассмотрим). Для реализации второго пункта нам надо иметь сохраненное состояние системы (мы этого не делали). Третий пункт отпадает по той же причине: заранее подготовленного образа ОС у нас тоже нет (да и «накатывать» поверх образ всей системы, когда нужно восстановить всего один файл...?) Диагностика памяти нам здесь не поможет это – понятно.

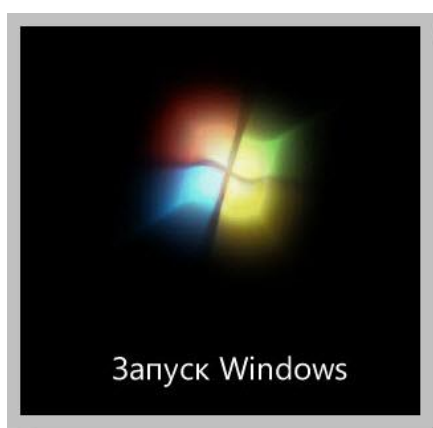
Итак, выбираем первый пункт «**Восстановление запуска**». Появится классическая WRE и Windows автоматически попытается устранить проблему:



После окончания работы программы мы, как всегда, можем посмотреть отчет о результате:



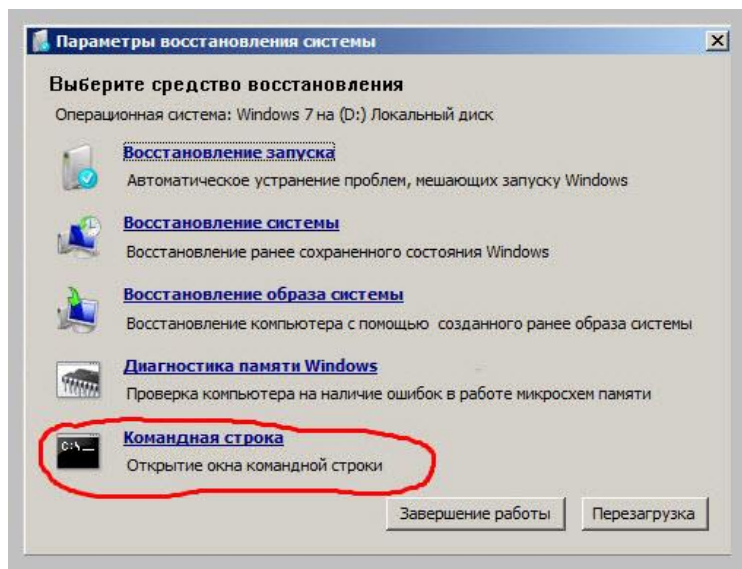
Нажимаем «Готово», компьютер перезагрузится и мы увидим, что загрузка Windows снова успешно восстановлена.



Вы, наверное, замечали, что в пиратских копиях Windows 7 периодически «слетают» «кряки»? И связано это, в первую очередь, с автоматическим запуском среды

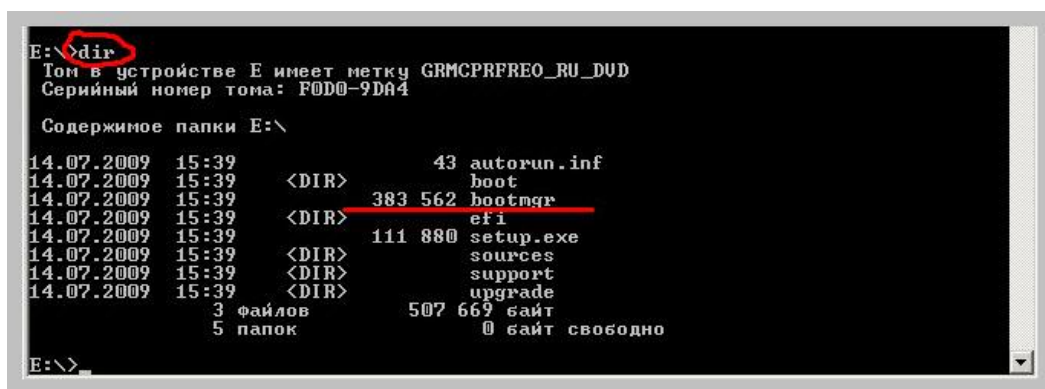
восстановления (WRE «видит», что важные системные файлы были модифицированы и, до кучи, заменяет и их оригинальными копиями), в результате чего «кряк» просто «слетает».

Но возвращаемся к нашим экспериментам! Теперь давайте рассмотрим, что будет, если на одном из этапов мастера мы выберем другой пункт – «**Командная строка**»?



Нажимаем на эту ссылку и поверх окна мастера у нас появится консоль интерпретатора команд Windows. Мы уже разбирали работу с ней в наших уроках и статьях на сайте, поэтому тут ничего нового нет. Нам нужно будет просто скопировать диспетчер загрузки (bootmgr) с диска - в корень нашего 100 мегабайтного раздела, т.е. – вернуть файл на свое место.

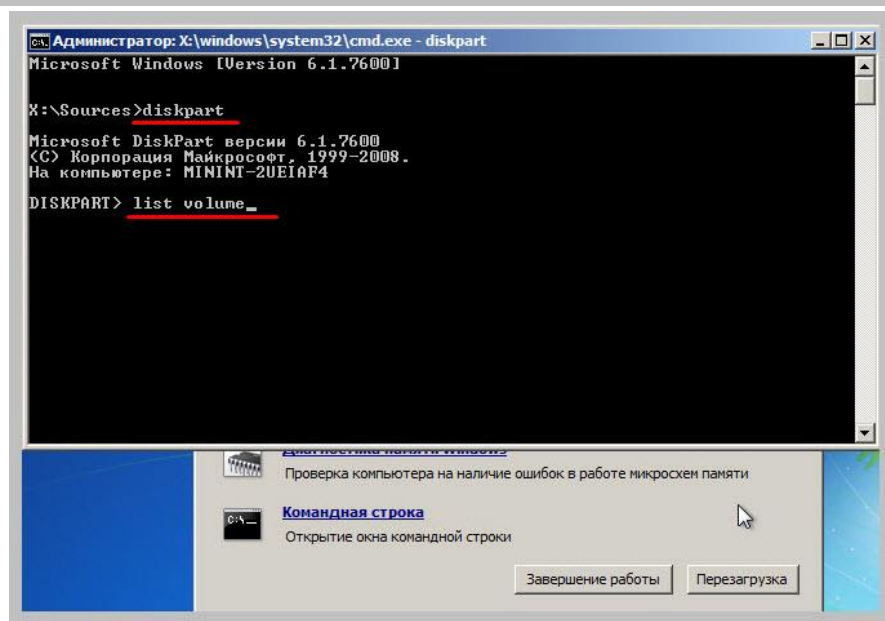
Примечание: файл bootmgr располагается в корне любого установочного диска Windows 7.



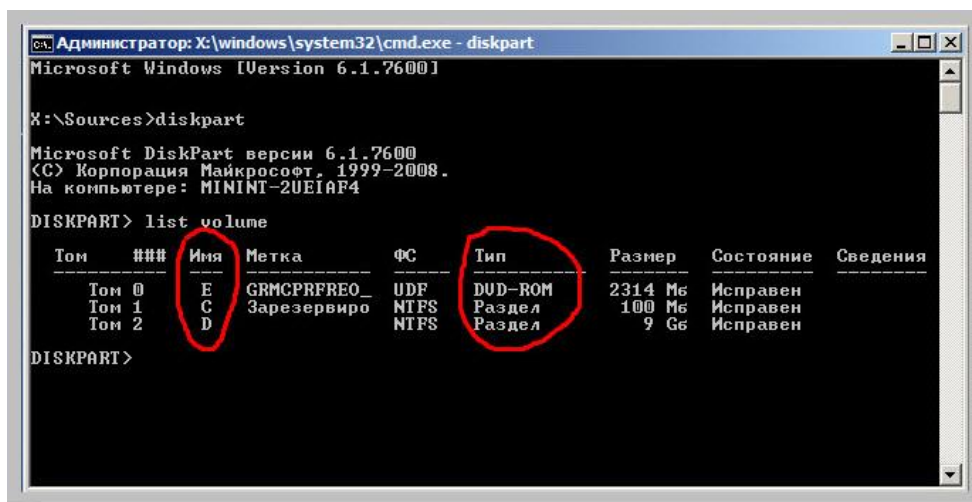
Давайте определимся с тем, откуда и куда нам нужно копировать файл?

Вводим в интерпретаторе команду «diskpart», а затем – «list volume».

Примечание: diskpart это – утилита командной строки, которая является расширением графической оснастки «управление дисками».



Нажимаем клавишу «Enter». Появится текстовое меню, где мы наглядно сможем увидеть, каким устройствам и дискам назначены те или иные буквы:



Видим, что под буквой «Е» у нас – устройство компакт дисков (DVD-ROM), буква «С» это – 100 мегабайтный загрузочный раздел, а «D» раздел размером 9 гигабайт, на котором установлена Windows 7. Выходим из утилиты diskpart, дав команду «exit».

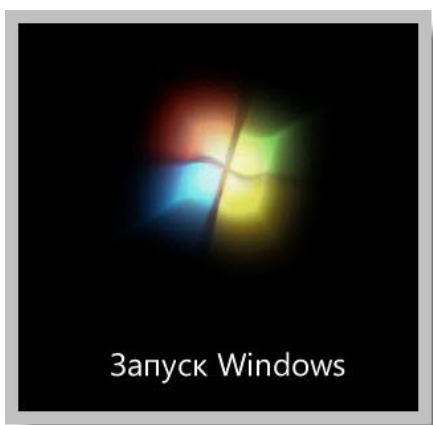
Теперь, точно зная откуда и куда копировать, переходим на устройство компакт дисков (e: – «enter») и, находясь там, даем команду копирования: **copy bootmgr c:**



Что мы сделали? Скопировали диспетчер загрузки (файл bootmgr), находящийся на установочном DVD диске, в корень зарезервированного (100 мегабайт) раздела «С», который и отвечает за загрузку операционной системы.

На скриншоте выше можно видеть надпись об успешном завершении операции копирования данного файла.

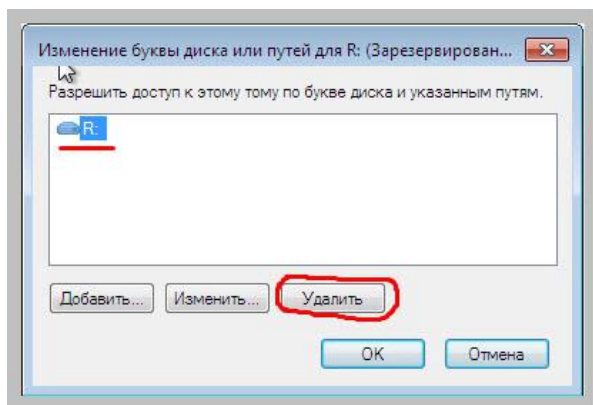
Теперь, перезагрузим наш компьютер и убедимся в том, что работа Windows восстановлена:



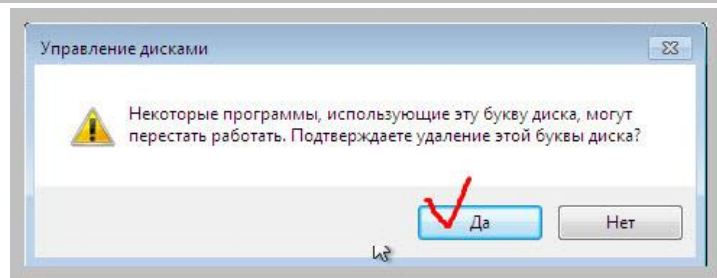
Давайте окончательно «заметем следы» своего вмешательства в загрузку операционной системы и снова «спрячем» системный раздел с диспетчером загрузки, удалив букву диска, которую мы ему перед этим присвоили.

Для этого нажимаем правой кнопкой мыши по пиктограмме «Мой компьютер», расположенной на рабочем столе, из раскрывшегося меню выбираем пункт «Управление» и в появившейся оснастке переходим в раздел «Управление дисками». Там нажимаем правой кнопкой мыши на нашем 100 мегабайтном разделе и из меню выбираем пункт «Изменить букву диска или путь к диску».

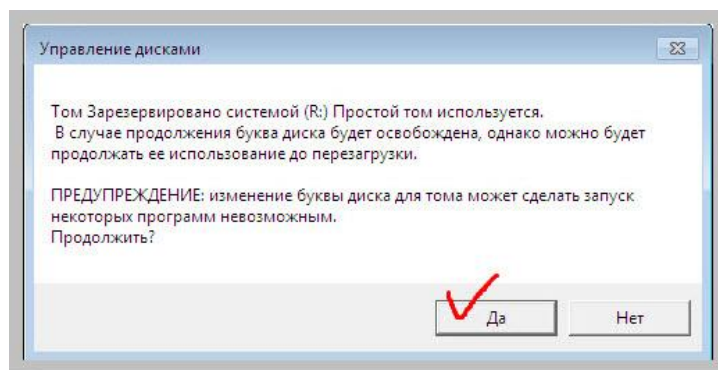
Появится вот такое окно:



В нем отмечаем наш диск и нажимаем кнопку «Удалить». Появится предупреждение:

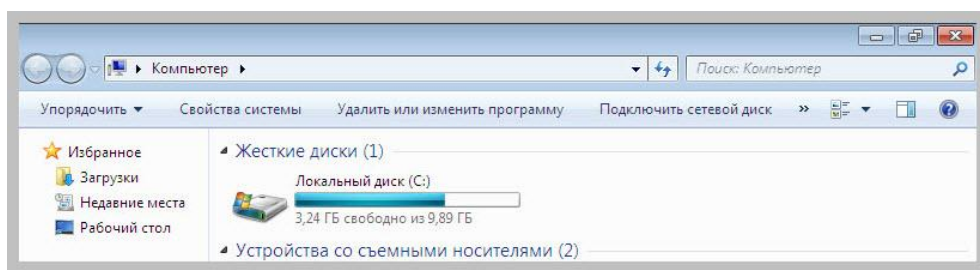


Мы ведь точно знаем что делаем, правда? Нажимаем «Да» и... появляется еще одно предупреждение!



Вот она – отеческая забота Microsoft о конечном пользователе! Нам только что подгузник сменить не предлагают ☺ Нажимаем «Да».

После этого заходим в проводник и видим, что у нас, как и в самом начале наших экспериментов, в наличии только один диск «С»:

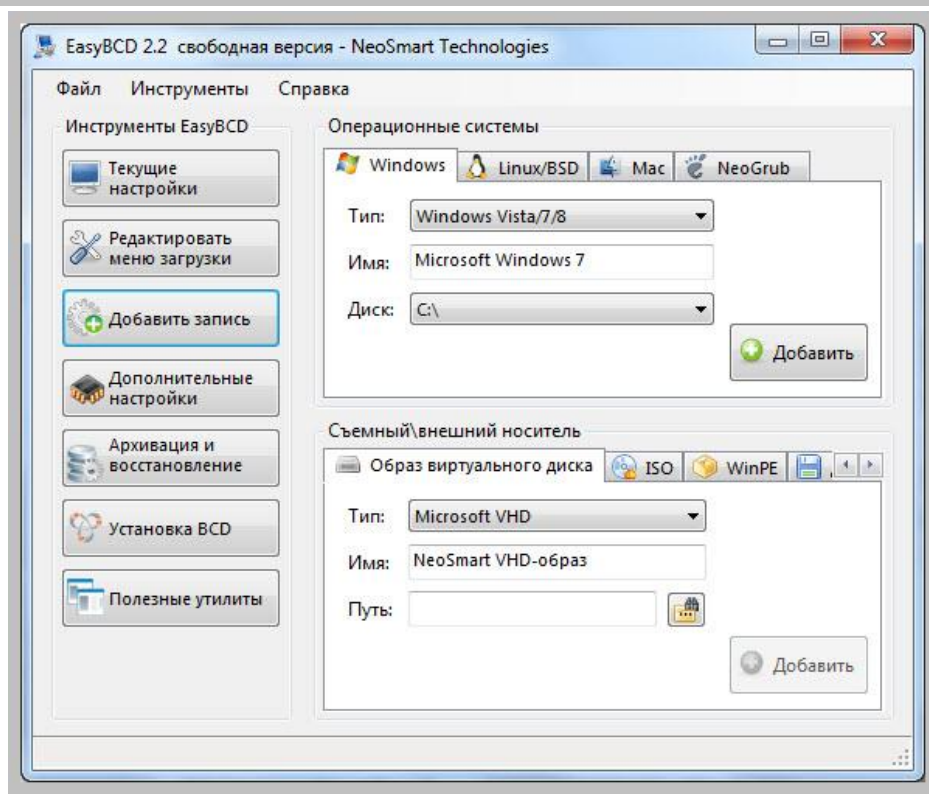


На всякий случай перезагрузимся. Убеждаемся в том, что система работает нормально и все наши действия на стабильность ее работы никак не повлияли.

Вот и все, собственно! Надеюсь, Вы теперь лучше представляете себе, как это все работает на самом деле и будете с успехом применять это знание в своей практике.

Напоследок, я хочу предложить Вашему вниманию замечательную программу «**Easy BCD**», в которой под удобным GUI (графическим) интерфейсом собраны многие утилиты командной строки Windows для работы с различными загрузчиками (причем не только от Microsoft).

Скачать программу можно здесь: <https://sebeadmin.thelogos.in.ua/soft/easybcd.zip>



Программа – очень здоровская! Если возникнет необходимость, можно будет даже написать по ней отдельную статью на нашем сайте.

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

До встречи в следующих уроках !