Владимир Безмалый

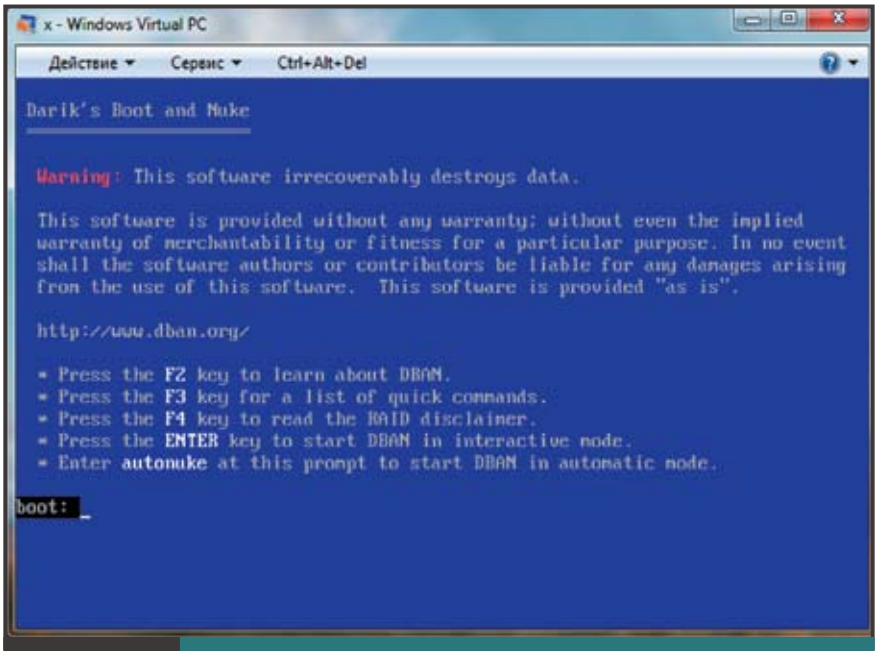
Полноценное удаление данных

Когда в компании или дома требуется обновить компьютер, мы стараемся сохранить более-менее пригодные рабочие комплектующие, а от нерабочих или устаревших избавляемся. И важно не забывать, что в этом случае также необходимо уничтожить и данные!

Неоднократно в новостях рассказывалось о том, как конфиденциальные данные были восстановлены из купленных на вторичном рынке жестких дисков.

Многие полагают, что если невозможно использовать жесткий диск в силу его неработоспособности, то, значит, и данные с него прочесть нельзя. Но это не так, и даже сломанной жесткий диск по-прежнему является лазейкой для нарушения информационной безопасности.

Жесткий диск состоит из набора магнитных пластин, которые содержат сектора, нечитаемые напрямую с помощью операционной системы. Когда файл удаляется, операционной системой фактически удаляется лишь указатель на него в памяти. Область, содержащая удаленные данные, помечается как свободное пространство, и, следовательно, пока новый файл не будет записан на это место, данные можно будет прочитать. Для восстановления и чтения удаленных данных используется специальное программное обеспечение. С его помощью осуществляется поиск секторов, содержащих любые данные удаленных файлов, а затем они восстанавливаются. Сделать это не слишком сложно, и, более того, в Интернете можно найти бесплатное программное обеспечение для восстановления данных. Здесь следует учесть, что программное обеспечение для восстановления данных на физически поврежденных секторах дисков не работает и что мы не можем использовать данное программное обеспечение без операционной системы.



Экран 1 Окно Darik's Boot and Nuke

Вот почему мы не можем полагать себя в безопасности, если просто выбрасываем поврежденные диски. Когда мы считаем, что диск сломался, надо помнить что фактически становится неисправным только какая-либо из микросхем или механические части внутри диска. А пластины, где хранятся все файлы, по-прежнему работоспособны, потому что диск находится в жестком футляре и пластины не имеют ни механических, ни электрических

ИЛЛЮСТРАЦИЯ STOCK.XCHNG

частей. Эксперты-криминалисты используют только пластины для восстановления удаленных файлов на сломанных дисках. Но при желании и не слишком опытный специалист в этом случае сможет восстановить файлы, потому что описания процедур восстановления вручную удаленных файлов распространены в Интернете.

Область, содержащая удаленные данные, на жестком диске помечается как свободное пространство, и эти сектора нельзя прочитать напрямую с помощью операционной системы, но использование специального программного обеспечения позволяет восстановить и прочитать удаленные данные

Что делать?

Пользователи и компании, желающие продать или подарить использованный жесткий диск отдельно или вместе с компьютером либо выбросить поврежденные диски, должны в первую очередь полностью очистить диск. Удаление данных с дисков — процесс безвозвратного удаления данных, находящихся на них. Существует два типа очистки жестких дисков — физическое стирание данных и уничтожение данных.

Физическая очистка

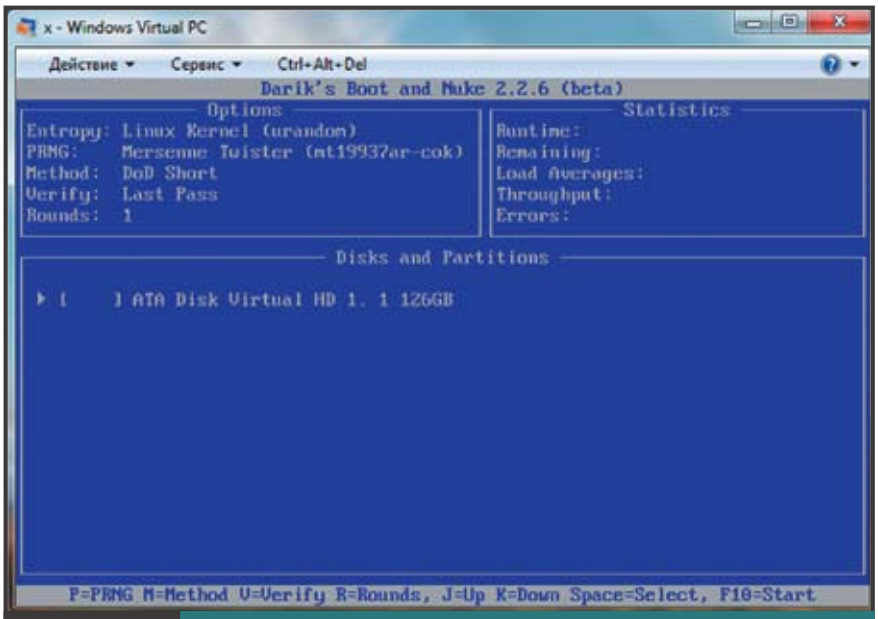
Самый быстрый вариант — размагничивание диска. Для этого можно задействовать специальные устройства, предназначенные для гарантированного уничтожения данных на магнитных носителях в конце срока их эксплуатации в целях обеспечения безопасности хранения и предупреждения утечки информации. В качестве примера могу упомянуть устройство «Лавина» производства украинской компании «Эпос».

В данном устройстве используется физический метод уничтожения данных, базирующийся на воздействии на накопитель мощного электромагнитного импульса. В результате все магнитные домены носителя однородно намагничиваются до состояния насыщения. Это приводит к исчезновению магнитных переходов, в которых кодируется записанная на носителе информация. Таким образом, полное разрушение исходной магнитной структуры носителя приводит к гарантированному уничтожению всех данных, когда-либо хранившихся на нем.

Автономный многофункциональный прибор EPOS DiskMaster Portable позволяет работать со всеми жесткими дисками с интерфейсами PATA, SATA, eSATA независимо от производителя, модели и емкости. Все операции выполняются с максимально возможной скоростью, которую поддерживает накопитель (скорость передачи данных до 8 Гбайт/мин). В отличие от программных средств с аналогичной функциональностью, прибор обеспечивает копирование и уничтожение данных в скрытой области жестких дисков HPA (Host Protected Area), а также на жестких дисках с дефектами на поверхностях.

Подобного рода уничтожители информации также выпускают компании Detector systems, «Инфосекьюр» и другие

Физическое уничтожение диска — метод надежного удаления дан-



Экран 2 Disks and Partition

ных. Это предпочтительный метод уничтожения данных при сбое других методов или при серьезном повреждении жесткого диска. Физическое уничтожение жестких дисков является быстрым и наиболее эффективным методом безопасного удаления данных, но при этом сам жесткий диск, естественно, в дальнейшем использоваться уже не будет.

Программная очистка данных

Программная очистка данных — процесс необратимого удаления данных, сохранившихся в области, логически считающейся свободным пространством, с использованием особых методов удаления данных. Процесс происходит во время загрузки компьютера, но после того, как загружается операционная система. Это рекомендуемый метод, если предполагается продать, подарить или повторно использовать диск.

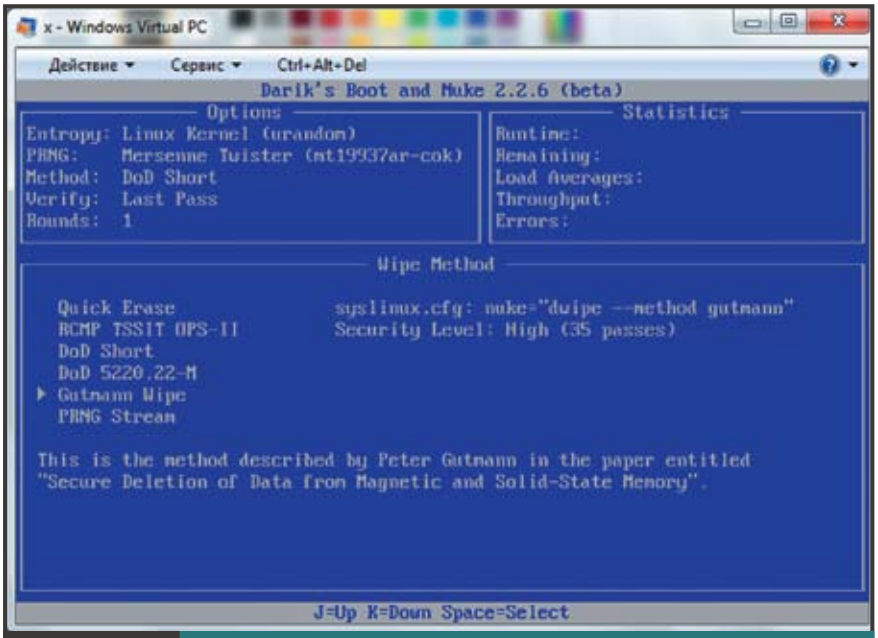
Вот первая тройка программного обеспечения для очистки жестких дисков:

- DBAN — программа очистки при загрузке системы, мультиплатформенная, бесплатная;
- DiskWipe — не требует установки, поддерживает Windows (XP, Vista, 7), бесплатная;
- CCleaner, поддерживает Windows (XP, Vista, 7), бесплатная.

Программное обеспечение для очистки данных превосходно работает на дисках, не имеющих плохих секторов. Оно не может стереть информацию на поврежденных дисках. Для эффективного уничтожения данных необходимо повторить процесс стирания данных по меньшей мере трижды. Полный цикл стирания может занять несколько часов или дней в зависимости от емкости диска.

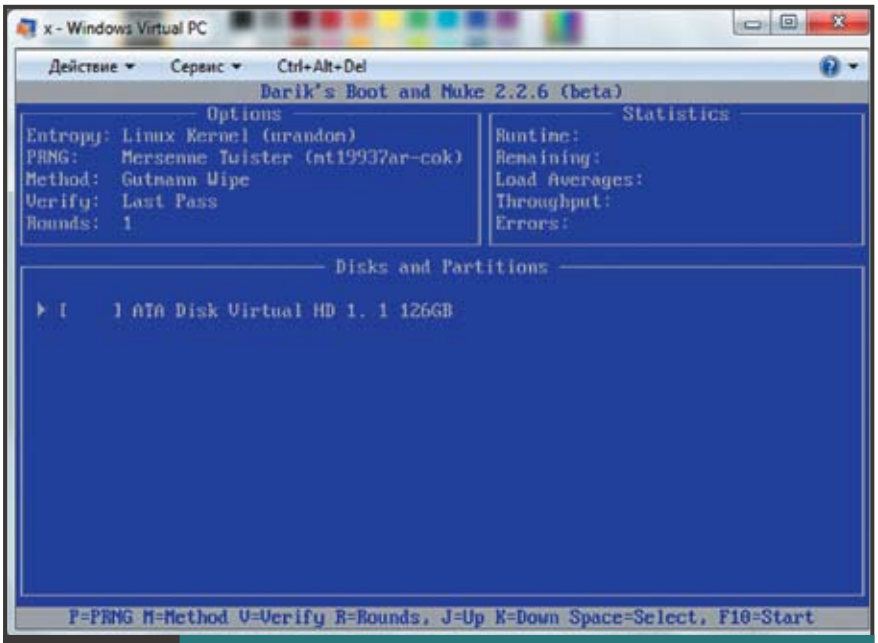
Darik's Boot and Nuke (DBAN)

Программное обеспечение Darik's Boot and Nuke (DBAN) можно загрузить по адресу http://sourceforge.net/projects/dban/files/dban/dban-2.2.6/dban-2.2.6_i586.iso/download. Здесь вы получите загружаемый образ ISO, который впоследствии можно записать на компакт-диск и, загрузившись с него, выбрать жесткий диск для удаления данных. Далее включите компьютер, жесткие диски которого хотите очистить, убедившись, что он будет загружаться с привода для компакт-дисков, а затем вставьте компакт-диск с DBAN.

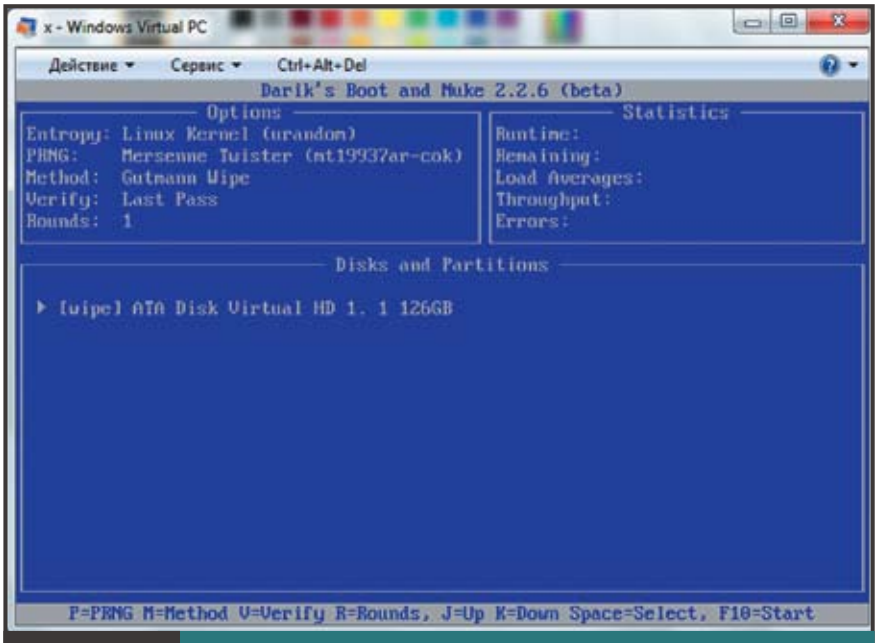


Экран 3 Выбор метода удаления Gutmann Wipe

1. Если вы корректно загрузитесь, то увидите экран приветствия и приглашение boot: _ (экран 1).
2. Нажмите Enter и перейдите в интерактивный режим DBAN, см. экран 2. Если ваш диск содержит конфиденциальную информацию или важные для бизнеса данные, то перейдите к пункту 3, иначе пропустите его и перейдите к шагу 4.
3. Нажмите клавишу «M» для ручного выбора метода очистки и выберите Gutmann Wipe, затем нажмите Enter. Этот метод рекомендуется для удаления конфи-



Экран 4 Выбор диска для удаления данных по Gutmann Wipe



Экран 5 Экран запуска процесса удаления данных

денциальных данных. При методе Gutmann Wipe осуществляется 35 проходов по жесткому диску (экран 3).

4. Проследите, чтобы изображение на экране соответствовало приведенному на экране 4.
5. Нажмите клавишу «Пробел» для перехода к экрану запуска процесса удаления данных (экран 5).
6. Убедитесь, что вы выбрали нужный диск (раздел) для удаления данных. Если все нормально, нажмите клавишу F10 для начала процесса удаления (экран 6).

Весь процесс удаления данных может занять до 12 часов

DiskWipe

Disk Wipe — это бесплатное приложение для Windows, предназначенное для гарантированного уничтожения данных, не требующее установки. Утилиту Disk Wipe можно загрузить по адресу http://www.diskwipe.org/. С Disk Wipe вы можете стереть все содержимое диска и сделаете невозможным восстановление данных. Disk Wipe позволяет удалить данные как с раздела, так и со всего жесткого диска, используя алгоритмы Dod 5220-22.M, US Army, Peter Guttman. Поддерживаются интерфейсы S-ATA (SATA), IDE (E-IDE), SCSI, USB, FIREWIRE (экран 7).

CCleaner

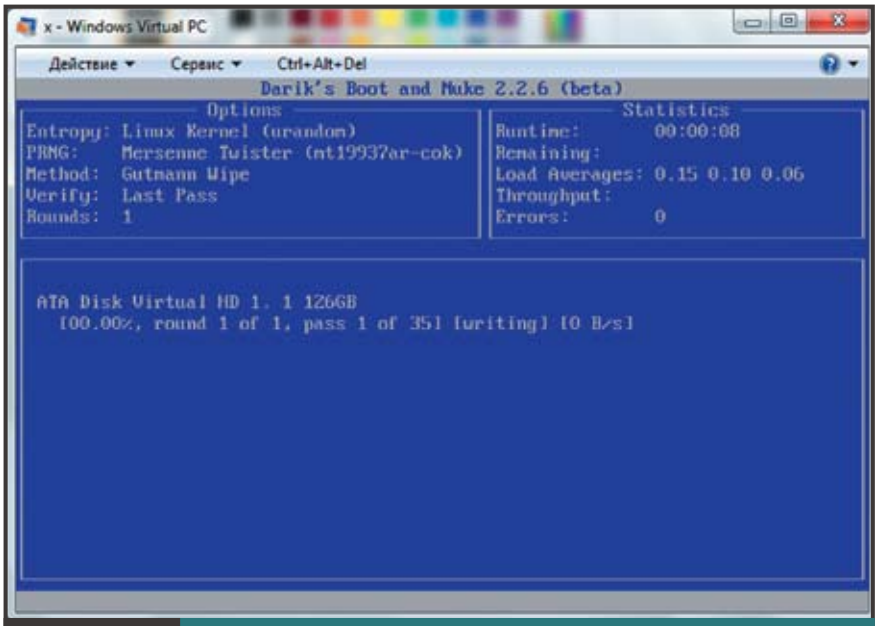
CCleaner — это бесплатная программа для оптимизации компьютера, совмещающая в себе модуль очистки системы, удаляющий все ненужные и временные файлы, и полнофункциональный модуль очистки реестра. CCleaner чистит следующие компоненты системы:

1. Internet Explorer — временные файлы кэша, историю посещений, cookies-файлы, скрытые файлы Index.dat, историю загрузок.
2. Корзину Recycle Bin.
3. Буфер обмена.
4. Временные файлы Windows.
5. Журналы Windows.
6. Список последних документов (в меню «Пуск»).
7. Историю исполненных команд (в меню «Пуск»).
8. Историю помощника поиска в Windows XP.
9. Устаревшие данные функции Prefetch в Windows XP.
10. Дампы памяти после сбоев Windows.
11. Фрагменты файлов, остающиеся после работы команды Chkdsk.

Дополнительные функции позволяют очистить:

- кэш очередности меню;
- кэш сообщений системного лотка;
- кэш размеров и адресов Windows;
- историю помощи пользователю;
- файлы журналов IIS;
- дополнительные папки.

CCleaner не только удаляет старые файлы и другие данные стандартных компонентов Windows, но и позволяет производить очистку временных файлов и списков последних документов во многих других программах: Firefox, Opera, Safari, Media Player, eMule, Kazaa, Google Toolbar, Netscape, Microsoft Office, Nero, Adobe Acrobat Reader, WinRAR, WinAce, WinZip и других.



Экран 6 Процесс удаления данных

CCleaner использует модуль очистки реестра для обнаружения различных проблем и несоответствий в системе. Он проверяет расширения файлов, элементы управления ActiveX, ClassIDs, ProgIDs, программу удаления, общие DLL, шрифты, ссылки файлов помощи, пути приложений, значки, неправильные ярлыки.

Кроме того, предоставляется функция безвозвратного удаления файлов с несколькими циклами перезаписи, что не позволяет восстановить их никаким способом (экран 8).

Как показано на экране 8, для безопасного затирания свободного места на диске можно использовать следующие алгоритмы:

- простое стирание (1 проход);
- DOD 5220.22-M (3 цикла);
- NSA (7 циклов);
- Gutmann (35 циклов).

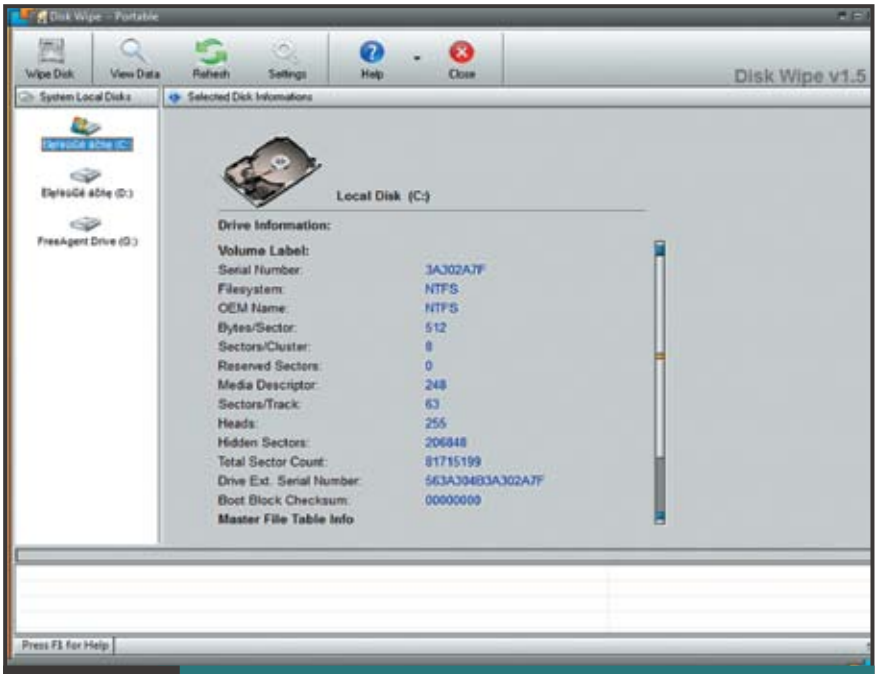
Вы можете выбрать для себя оптимальный алгоритм затирания свободного пространства, исходя из требований скорости/безопасности.

Нельзя забывать и о встроенном средстве невосстановимого стирания из состава операционной системы. Команда

```
Cipher/W: каталог
```

обеспечивает невосстановимое стирание свободного места в выбранном каталоге; она существует в семействе Windows начиная с версии Windows 2000. Однако следует учесть, что в данном случае осуществляется быстрое стирание.

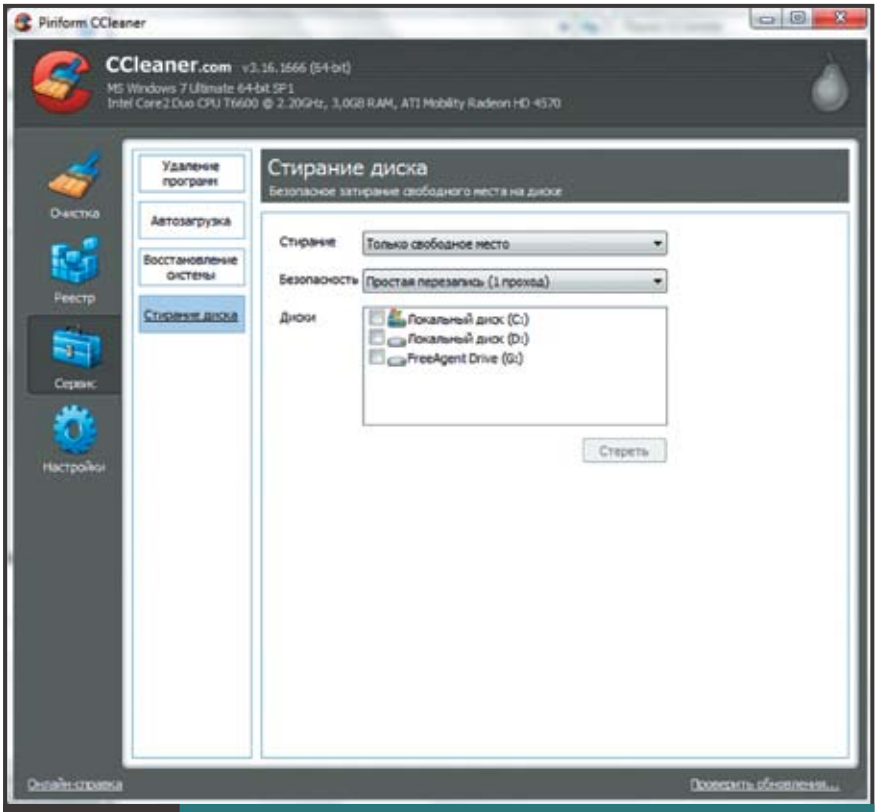
На самом деле удалять данные без возможности восстановления совсем несложно. Важно понимать достоинства и недостатки выбранного подхода к удалению (программное или аппаратное). Программное стирание позволяет вам использовать диски повторно, однако отнимает массу времени и может использоваться лишь на рабочих жестких дисках. Аппаратное осуществляется намного быстрее, позволяет обрабатывать нерабочие (нечитаемые) диски. Однако при применении на рабочих дисках всегда есть вероятность из-за слишком сильного магнитного импульса сделать так, что диски выйдут из строя навсегда.



Экран 7 Окно Disk Wipe

Таким образом, необходимо ориентироваться на оба подхода, так как только их сочетание может принести гарантированный успех. Кроме того, исключительно важно просто не забывать о необходимости удалять данные регулярно!

Владимир Безмалый (vladb@windowslive.com) — специалист по обеспечению безопасности, имеет звания MVP Consumer Security, Microsoft Security Trusted Advisor



Экран 8 Невосстановимое стирание с помощью CCleaner