Крис Касперски

СЕКРЕТЫ ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ

kk@sendmail.ru

Крис Касперски
kk@sendmail.ru

Секреты восстановление информации

– У меня не читается дискета
– Но вчера она ещё читалась...
– Да, а как Вы узнали?
"Ну юзер погоди!"
неизвестного автора

Народная мудрость гласит: "Беда не предупреждает о своем приходе". Перефразируя Булгакова можно сказать: мало того, что компьютер смертен, хуже всего, что он внезапно смертен и большинство отказов (и особенно трагических отказов) происходят без всяких видимых причин! Вирусы, космические лучи, сбои программного обеспечения, наконец, нелепые ошибки самих операторов – все это способно если не вывести ноутбук из строя, то, по крайней мере, угробить хранящуюся на нем **информацию**.

Катастрофа может произойти в любой момент, в том числе и накануне подписания судьбоносного контракта, единственный экземпляр которого хранится на том самом злощастном ноутбуке, а на составление нового проекта договора просто нет времени!

Конечно, "идеологически" правильнее отнести такой ноутбук в сервис-центр, где им займутся профессиональные мастера, но, увы, это не всегда возможно и передряги судьбы порой заводят нас в такие ситуации, когда остается рассчитывать лишь на самих себя, – на свои собственные силы, знания, умения и навыки...

Введение

Сегодня мы поговорим о **технике восстановления информации подручными программными средствами**, – теми, что входят в штатную поставку операционной системы и не требуют для работы с собой никакой особенной квалификации. Не стоит думать, что таким образом исправляются лишь простейшие, несерьезные сбои. Напротив! Мощная иммунная система современных операционных систем, даже тяжелейшие ранения восстанавливает самостоятельно, практически без всякой помощи со стороны пользователя. Зачастую все, что от вас требуется – это инициировать процесс автоматического восстановления и ниже мы расскажем как именно это сделать.

Поскольку техника восстановления информации чрезвычайно системно-зависима, то есть по разному реализована на Windows 95, Windows 98 и Windows 2000, мы не в состоянии рассказать обо всех системах сразу и потому решили оставить свой выбор лишь на одной из них – на Windows 98, наиболее массовой операционной системе, покорившей подавляющее большинство ноутбуков. Ну, а о Windows 2000/XP, давайте поговорим в следующий раз.

Что имеем – не храним, или штурм энтропии начинаем уже сегодня!

Восстановить информацию будет значительно проще, если заранее позаботиться об этом и предусмотрительно обзавестись всем необходимым, ведь ноутбуки, в отличии от настольных компьютеров, зачастую приходится реанимировать в сугубо "полевых" условиях: в гостиничном номере, в здании аэропорта, а то и в вовсе в летящем самолете (автобусе, поезде)!

Как минимум, вы должны иметь системную дискету или загрузочный CD-ROM (или zip-) диск из серии "Реаниматор", причем, учитывая, что дискеты имеют тенденцию "сыпаться" в самый неподходящий момент, системных дискет у вас должно быть по меньшей мере две. Как их создать? Да очень просто: в "Панели управления" дважды щелкните по иконке "Установка и удаление программ", затем в появившемся диалоговом окне перейдите к вкладке "Загрузочный диск" и нажмите кнопку "Создать диск", при этом будьте готовы к тому, что система попросит вставить дистрибутивный Windows-диск в привод CD-ROM. Дискеты предпочтительнее тем, что чрезвычайно компактны и легко помещаются в карман вашего пиджака (рубашки), в то время как для хранения CD-ROM'а потребуется постоянно иметь при себе кейс или дипломат. С другой стороны, на лазерный диск без труда влезает пакет "Нортоновских утилит", которые в случае дисковой аварии окажутся как нельзя кстати. Только убедитесь, что это действительно именно та версия утилит, которая вам нужна. Дело в том, что утилиты, ориентированные на Windows 95 (и уж тем более – на MS-DOS!) при встрече с Windows 98 необратимо грохают жесткий диск, только усиливая разрушения!

При наличии свободного места на жестком диске настоятельно рекомендуется скопировать туда папку WIN98 с дистрибутивного диска, что, во-первых, избавит вас от необходимости постоянно носить дистрибутивный диск с собой, а, во-вторых, если в результате тех или иных сбоев CD-ROM привод окажется недоступен (что зачастую и происходит) вы всегда сможете переустановить Windows с винчестера.

Также имеет смысл создать резервную копию операционной системы и/или используемых ею приложений. Вся хитрость в том, что восстановление системы с резервной копии происходит на два порядка быстрее, чем ее переустановка. И как вы, вероятно, уже знаете по собственному опыту, в некоторых ситуациях времени на переустановку может просто не быть! Создать резервную копию можно двояко: самое простое (но, увы, отнюдь не самое лучшее) воспользоваться автоматической архивацией данных, запустив одноименное приложение, входящее в комплект штатной поставки Windows ("Пуск" → "Программы" → "Стандартные" → "Служебные" → "Архивация данных"). Пропустив "ругательство" об отсутствии ленточных накопителей мимо ушей, мы создаем новое задание архивации нажатием кнопки "OK", затем перемещаем радиокнопку с положения "Архивация всех файлов и папок" в положение "Архивация только выбранных файлов и папок", подтверждая серьезность своих намерений установкой галочек напротив папок "Windows" и "Program File", указываем местоположение для формирования архива (естественно, лучше всего сохранять архив на zip- или CD-R/RW диске, но на худой конец можно ограничится и винчестером) и, победно щелкнув мышкой по кнопке запуска, берем короткий тайм-аут на "перекурить" в ожидании пока оно все не зарезервируется.

Существенный недостаток такого подхода в том, что для восстановления архива вы должны иметь хотя бы минимально работоспособную Windows, поскольку из "чистой" MS-DOS "Архивация данных" не работает! А значит, она полезна лишь для исправления незначительных сбоев и бессильна справиться с тотальным разрушением системы. Поэтому, лучше вообще отказаться от использования "Архивации данных" и осуществлять резервирование/восстановление самостоятельно. Для этой цели в частности хорошо подходит архиватор WinRAR. Запустите его, упакуйте папки Windows и Program Files и преобразуйте полученный архив в SFX (самораспакующийся файл), обязательно указав в "Выборе SFX модуля" – DOS.SFX, в противном случае вы просто не сможете запустить его под DOS'ом! (живого Windows'а в случае серьезной аварии у вас просто не будет!).

Windows вообще не загружается

Если при включении ноутбука вместо привычной эмблемы Windows, горделиво развевающейся на фоне кучевых облаков, ноутбук, грустно мерцая унылым черным экраном, сообщает о невозможности загрузки системы – не волнуйтесь! Вполне возможно, что через несколько минут систему удастся благополучно оживить!

Загрузившись с заботливо припасенной системной дискеты (она всегда должна храниться в вашем нагрудном кармане вместе с паспортом и другими документами удостоверения личности!), первым делом посмотрите, уцелел ли основной раздел: "dir C:\".

Если в ответ на введенную команду система сообщит, что никакого диска "Цэ" здесь и в помине нет, срочно доставайте из кармана валидол, ибо произошло едва ли не самое худшее, что только могло произойти! OK, немного успокоившись, достаем отвертку (у вас ведь есть отвертка, правда?) и аккуратно развинтив нотебук (естественно, не забыв перед этим его обесточить), проверяем надежность соединения всех кабелей и шлейфов. Отсутствие контакта – частый виновник "невидимости" вашего жесткого диска. Если же это не поможет, тогда запускаем Norton Disk Doctor и даем ему возможность проявить себя во всей красе. Впрочем, техника восстановления диска Доктором – тема отдельного большого разговора, которому не место в маленькой статье. Хотим ли мы того или нет, но нам придется ограничится рассмотрением лишь самой благоприятной ситуации, той самой, когда в ответ на команду "dir C:\" по экрану ноутбука пробегают любимые вашему сердцу имена папок и каталогов. Если так, то диск, по всей видимости, еще можно восстановить. Тяпнув пивка для храбрости, наберите следующую команду: "FDISK /MBR" (создание главной загрузочной записи: MBR– Master Boot Record) и пере... нет, креститься не нужно – просто перезагрузитесь.

Помогло? Нет?! Тогда, вновь загрузившись с системной дискеты, испытайте счастье еще раз, попытавшись сформировать сектор начальной загрузки "SYS C:" (чином пониже главной загрузочной записи будет).

Ну, если и это не поможет, тогда просто переустановите операционную систему.

Ноутбук виснет во время загрузки Windows

Зависание компьютера в процессе загрузки Windows чаще всего объясняется полным или частичным разрушением системного реестра. К счастью, Windows 98 выгодно отличается от своей предшественницы тем, что автоматически резервирует реестр при каждом перезапуске и всегда сохраняет последние шесть копий. Причем, если старт системы оказывается неуспешным, резервирования не происходит! Таким образом, имеющиеся копии – это копии *гарантированно работоспособного реестра*. Чтобы их восстановить, вы должны либо загрузится с системной дискеты, либо, удерживая <**Shift-F5**> во время запуска Windows, отказаться от загрузки графической оболочки. Короче говоря, для восстановления реестра вам потребуется чистая командная строка. Дождавшись появления курсора, одиноко мерцающего на черном экране, наберите: "SCANREG /RESTORE" и в появившемся диалоговом окне выберите копию реестра для восстановления за любую "понравившуюся" вам дату. При этом следует учитывать, что все изменения конфигурации системы (включая установку/удаление приложений и драйверов устройств),

выполненные после указанной даты, окажутся безвозвратно утерянными. Кажется вполне логичным, выбрать для восстановления наиболее свежую копию. Но задумайтесь: а что, если разрушение реестра как раз этим и было вызвано? Тогда – лучше остановить свой выбор на наиболее древней копии!

Если после восстановления реестра система все равно продолжает виснуть, попробуйте загрузиться в так называемом "**Безопасном**" или "**Защищенном**" режиме, в котором загружается лишь необходимый минимум системных компонентов и драйверов. Это можно сделать двояко: либо нажать <**F5**> при загрузке системы, либо нажатием <**Shift-F8**> вызвать стартовое меню и выбрать пункт "Safe mode". К сожалению, полноценная работа с нотебуком в "Защищенном" режиме невозможна и его можно рекомендовать лишь как временную меру, не спасающую от необходимости переустановки всей системы. Впрочем, полная переустановка абсолютно необязательна! Если вы не поленились и заранее зарезервировали систему, упаковав ее в самораспакующийся архив, вам останется лишь загрузиться с системной дискеты и запустить его! (Восстановление из активной системы невозможно, поскольку Windows запрещает перезапись открытых файлов).

Зависание восстановленной таким образом системы, равно как и зависание в "Безопасном" режиме, обычно указывает на аппаратную неисправность нотебука. Это может быть как плохой контакт (ау, где наша большая отвертка?!), так и присутствие контакта там, где ему присутствовать не положено (посмотрите: не попал ли на печатную плату посторонний токопроводящий мусор, вездесущий зверь таракан, некоторая жидкость или просто грязь).

Windows загружается, но периодически зависает во время работы или работает неправильно

Нестабильная работа системы – что может быть хуже? Источник ошибок подобного рода вообще очень трудно выявить и устранить. Это могут быть и сбои аппаратуры, и некорректная работа приложений, и искажение конфигурации системы, и... еще много чего! Переход в "Защищенный режим" позволяет сузить круг подозреваемых: если ноутбук продолжает зависать то, с большой степенью вероятности виновата аппаратура, в противном же случае, напротив, источник сбоев – программная среда.

Поскольку, основные неисправности аппаратуры мы уже рассмотрели (см. статью "Как изгоняют демонов"), перейдем непосредственно к самой программной среде. В каталоге Windows\System хранится малоизвестная, но чрезвычайно полезная утилита SFC, осуществляющая проверку целостности системных файлов и восстанавливающая разрушенные файлы в случае необходимости. Запустим ее! В появившемся диалоговом окне нажмем кнопку "Настройка" и взведем галочки напротив следующих пунктов: "Проверка файлов на наличие изменений" и "Проверка на наличие удаленных файлов" (см. рис. 1). Теперь "OK" и "Начать".

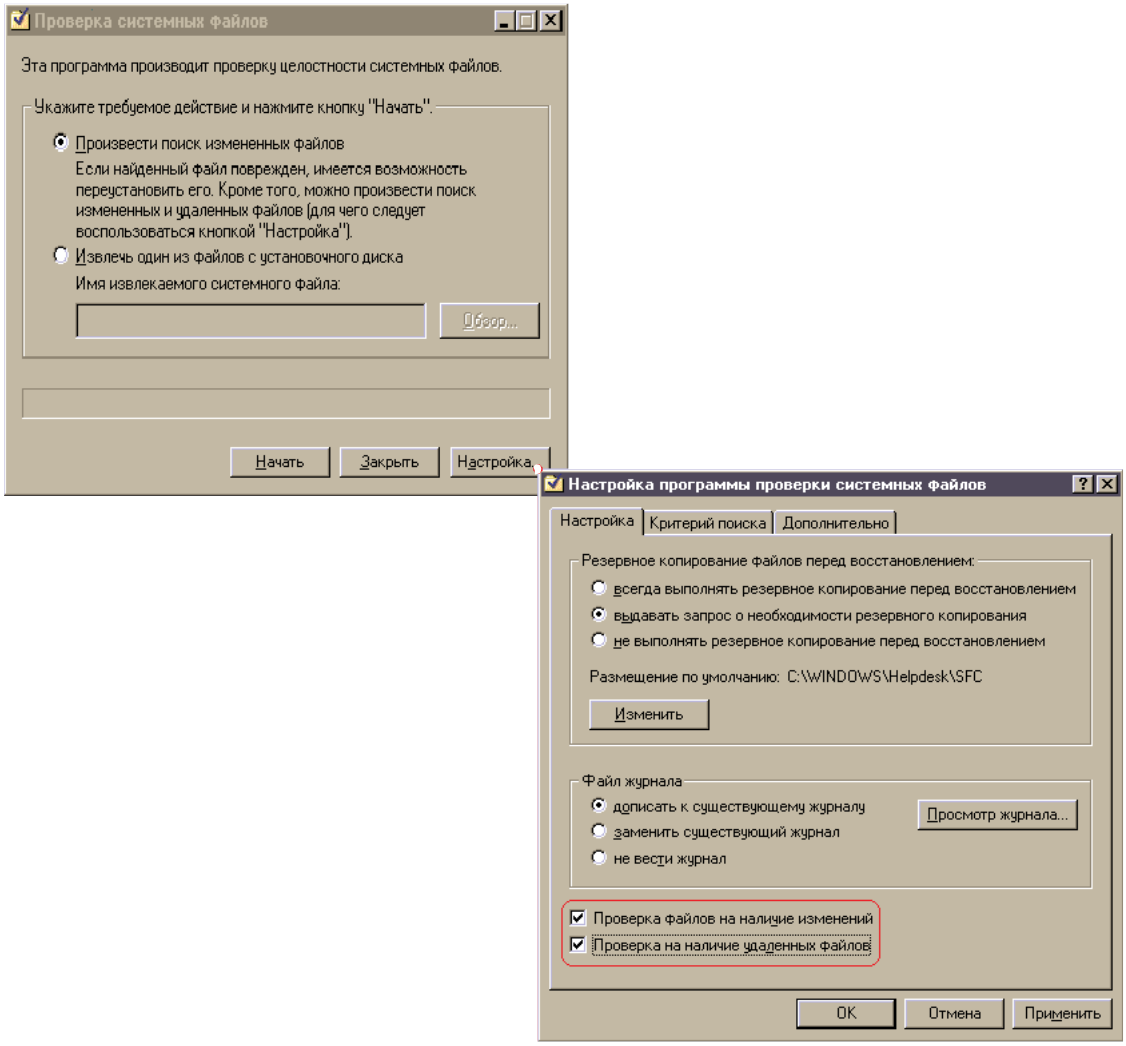

Рисунок 1. *Настройка утилиты проверки целостности файлов SFC*

Обнаружив присутствие измененных файлов на диске, утилита предложит либо обновить данные о файле (чего делать ни в коем случае не надо, за исключением тех случаев, когда мы точно знаем природу произошедших изменений и абсолютно уверенны в ее легальности), либо восстановить файл с дистрибьютивного диска (вот это – то, что нам надо, если конечно у нас имеется под рукой такой диск), либо проигнорировать изменение и продолжить (бывает полезно, если мы хотим восстановить испорченные файлы вручную), либо же обновить данные проверки для всех изменившихся файлов (чего делать в данном случае по меньшей мере неразумно).

Стоит заметить, что SFC служит не только весьма эффективным диагностическим, но еще и антивирусным средством! Ничего не зная о существовании вирусов, она, тем не менее, легко обнаруживает сам факт изменения файлов, а обнаружив – предлагает восстановить. Однако, запуск SFC не заменяет, а всего лишь дополняет постоянную проверку диска самыми свежими антивирусами. Почему? Так ведь, SFC исследует не все, а лишь системные файлы. Вирус же может сидеть в ***любом*** файле!

Если SFC обнаруживает многочисленные изменения файлов на диске (причем, изменяется не только дата, но еще содержимое и размер), а антивирус ничего не находит, – немедленно обновите антивирус, и, если это не поможет, – отошлите один, самый крошечный, измененный файл разработчикам антивируса, чтобы те получили возможность проанализировать и включить его в антивирусную базу. (Кстати, периодические сбои и зависания системы зачастую как раз и объясняются наличием вирусов).

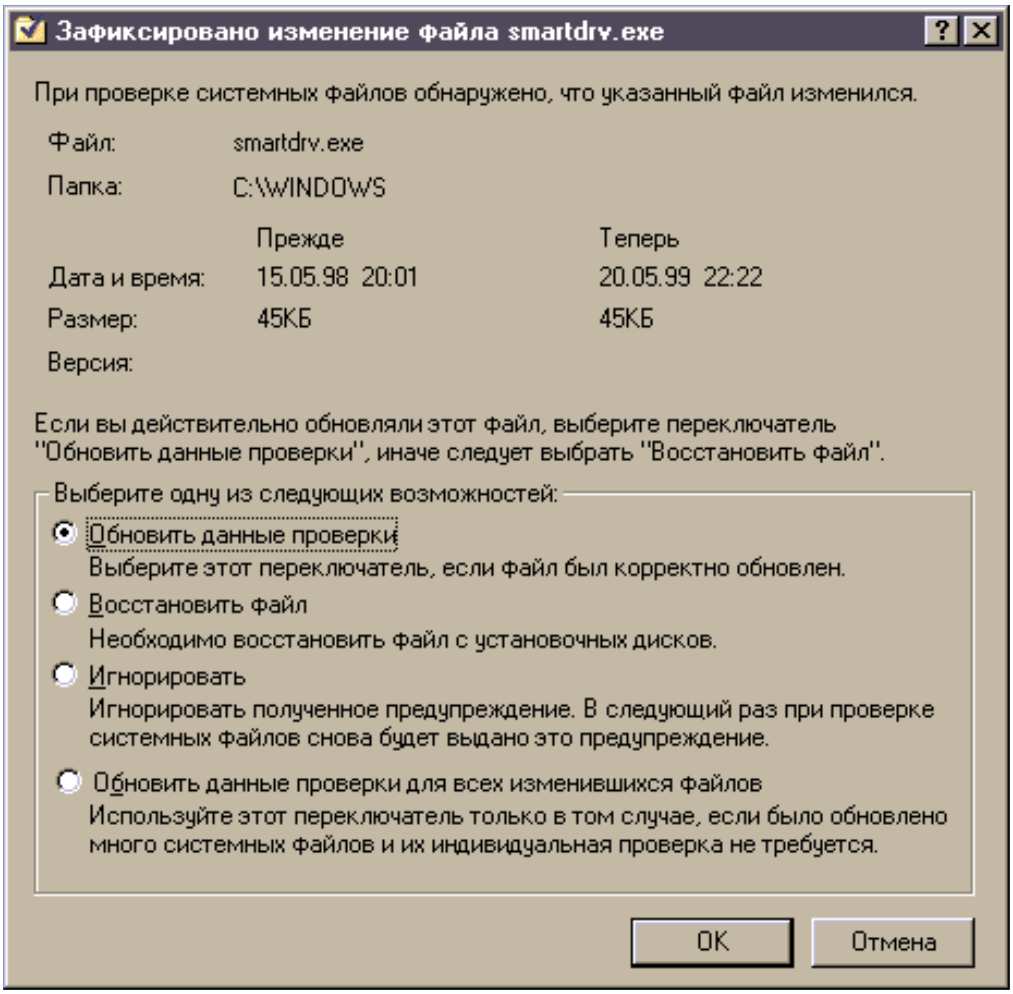

Рисунок 2. *Реакция утилиты SFC на изменение системных файлов*

В том случае, если SFC не обнаружит никаких изменений, или же вы окажетесь не удовлетворены результатами лечения, просто переустановите систему с дистрибьютивного диска или заранее созданной резервной копии (если она у вас есть).

На худой конец, запустите полную проверку диска (системные области + проверка поверхности), воспользовавшись либо штатной утилитой SCANDISK, либо Norton Disk Doctor. Винчестеры ноутбуков в силу всех передряг кочевой жизни склонны покрываться BAD-секторами, а ведь даже один-единственный нестабильно читающийся сектор может стать причиной буйного помешательства системы со всеми отсюда вытекающими последствиями.

Заключение

Разумеется, в рамках журнальной статьи подробно рассказать обо всех видах сбоев просто невозможно, а потому не исключено, что несмотря ни на какие ухищрения, вернуть свои данные к жизни вам так и не удастся... Пускай, это достаточно маловероятно, но и к такому развитию вам следует себя подготовить, как психологически, так и физически. Психологически все очень просто: без проблем и чрезвычайных происшествий жизнь была бы серой, скучной и вообще неинтересной. Физически: ежедневное резервирование всей сколь нибудь ценной информации на съемные накопители (дискеты, zip'ы, CD-R/RW) хоть и утомительно, зато позволяет быстро "отжаться" после любого "падения", в том числе и падения ноутбука с большой высоты, скажем, с летящего самолета ;-)