

Резервное копирование для админа

Фленов Михаил aka Horrific <http://www.vr-online.ru>

Я думаю, что в каждой второй статье этого номера можно будет услышать высказывание о том, что администраторы ленивые создания. Я думаю, что они произошли на свет из камня. Причем из очень большого, потому что администратора сдвинуть очень сложно, особенно если в этот момент идет ожесточенная борьба в Quake, которую просто нельзя прервать ради какого-то резервного копирования. Я не буду лишней раз утруждать тебя разговорами о том, что резервировать надо, мы лучше поговорим, о теории, чтобы можно было все сделать оптимально быстро и осталось больше времени на прохождение очередного уровня или на убойный Deathmatch.

Угроза

Мы будем рассматривать резервное копирование с точки зрения администратора, а админы работают в каких-либо организациях или фирмах, где потеря данных грозит финансовыми потерями для биг босса. Если накроется годовая отчетность или вся бухгалтерская база данных и не будет резервной копии, то можешь ждать зонтика, который точно воткнется тебе в задний проход, и самое страшное – раскроется. И моли бога, чтобы босс еще не начал вращать этот зонтик.

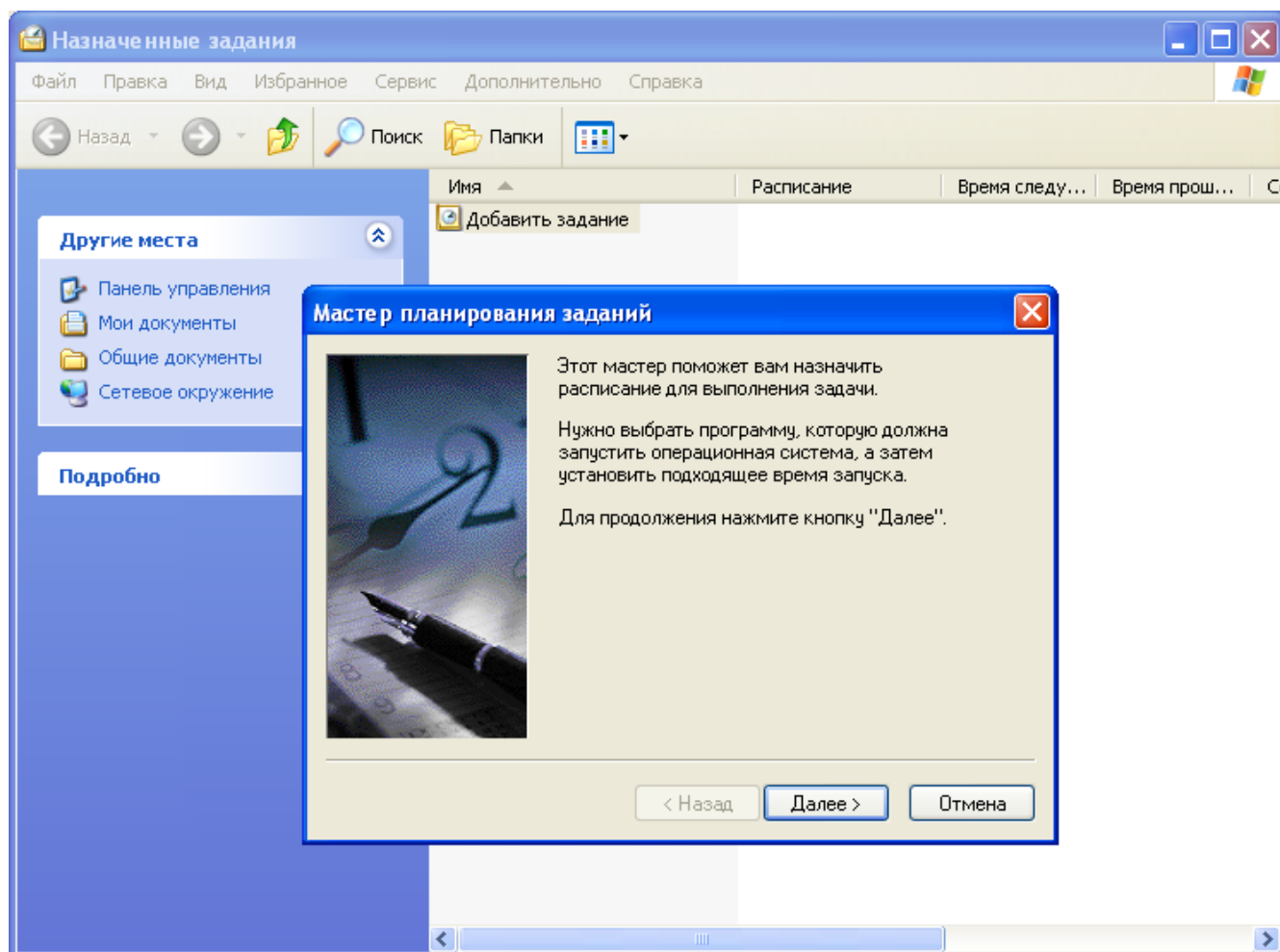
Для того чтобы финансовые потери от утраты данных были минимальными, нужно знать, откуда может прийти угроза. Помимо этого вы должны проанализировать данные, которые хранятся на сервере и рабочих станциях. От этого зависит, как часто нужно производить резервное копирование и каким методом.

Скорость восстановления работы после внештатной ситуации зависит от того, как хорошо ты подготовился к судному дню. Необходимо заранее проиграть все возможные варианты и желательно отработать процесс восстановления на практике, используя тестовую систему, чтобы не пришлось изучать практические действия.

Давайте посмотрим, откуда может прийти опасность:

- Случайное изменение или удаление файлов. Когда к серверу подключается новый пользователь, не имеющий достаточного опыта работы с компьютерами, то очень часто нелепые действия приводят к уничтожению данных. При правильной политике безопасности могут быть разрушены только собственные файлы пользователя, но и они могут иметь ценность для организации;

- Нарушение работы устройств. Когда я только начинал знакомиться с компьютерами, то в обиходе были дискеты 5,25 и жесткие диски максимальным размером в 20Мб. Если жесткие диски были достаточно надежны, то информация на дискетах постоянно пропадала из-за порчи поверхности. С переходом на дискеты 3,5 ситуация изменилась не сильно, а вот надежность жестких дисков повышалась. Но когда мы начали оперировать гигабайтами, то в определенный момент я реально увидел в глаза проблему испорченных блоков Bad Blocks. В определенный период, за пол года мне пришлось сменить несколько жестких диска размерами от 10 до 20 гигабайт разных производителей. Чаще всего это были Fujitsu, может помнишь, была серия 10 гигабайтных винтов, которые повально выходили из строя. Это было как набег саранчи, которая уничтожала информацию. В настоящее время надежность дисков снова стала улучшаться, но ее нельзя назвать идеальной. Всегда есть вероятность, что диск выйдет из строя;



С помощью заданий Windows можно запланировать резервирования и отдыхать

- Стихийные бедствия и потеря техники. Если посмотреть на конец 2004-го и 2005-й год, то замечаешь, что наша планета начинает преподносить страшные сюрпризы. Я имею ввиду участвовавшие наводнения, смерчи, землетрясения, пожары. Если раньше на это закрывали глаза, то сейчас мы уже ничему не удивляемся и перестали закрывать на эту проблему глаза. Россию пока это не трогало, но все может быть;

- Хакеры и эпидемии вирусов. Куда же без этого. Это чудо информационной жизни, без которого уже никуда не денешься, и приходится выстраивать всевозможные защиты. Но как бы ты не защищался, вирусы иногда побеждают. Какое средство чаще всего используют для защиты от вредоносного кода? Конечно же, антивирусы, которые запрещают выполнение любого известного вируса. Но хакеры придумывают новые программы и способы обхода антивирусов. И именно новые вирусы наносят максимальный ущерб, потому что для них нет еще эффективного метода лечения.

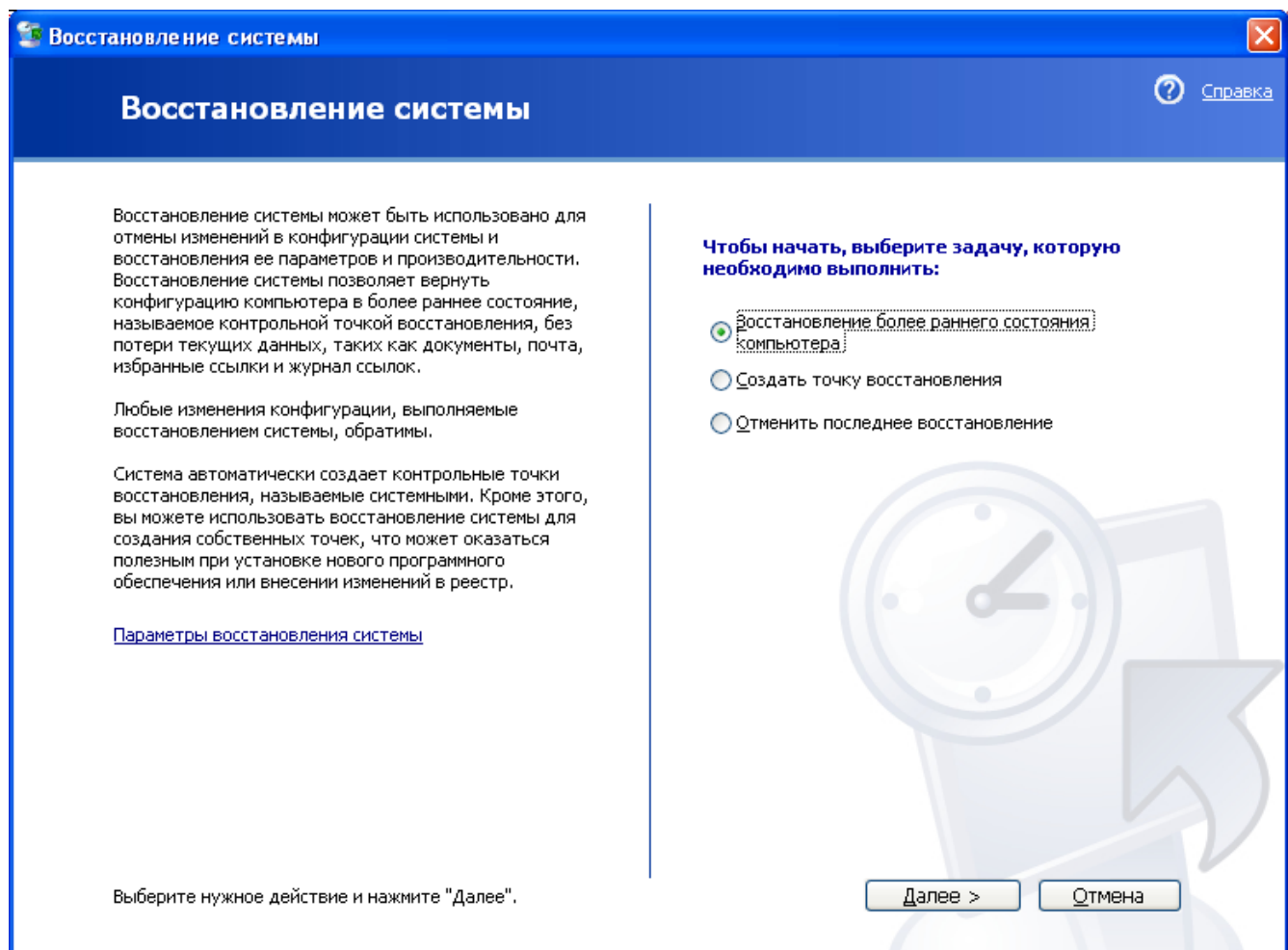
Этот список можно продолжать, но это основные угрозы, с которыми можно встретиться в реальной жизни.

Ранжирование данных

Прежде чем начинать что-то резервировать, необходимо четко разделить данные по

важность, по частоте изменения, и возможным способам резервного копирования. Как минимум, вы должны выделить следующие категории данных:

- Системные конфигурационные файлы. На первый взгляд, это не так важно, потому что в таких файлах нет секретной для организации информации. Но без возможности быстрого восстановления конфигурации компьютера или сервера, требуется много времени на конфигурирование ОС и всех программ с чистого листа. А это влечет за собой потери из-за простоя, что для некоторых компаний может исчисляться миллионами рублей за каждый час простоя;
- Документы пользователей. В домашних каталогах пользователей чаще всего находятся документы, которые обладают определенной ценностью. В организациях, в этих директориях могут быть отчетные документы или программы, которые используют пользователи в своей работе;



Мастер восстановления Windows помогает восстановить работоспособность, но от сбоя железа он не поможет

- Базы данных. Корпоративные данные хранятся в удобном для работы хранилище – базах данных. По практике, в таких базах хранятся наиболее важные данные, и любая компания может понести большие убытки в случае их потери;
- WEB. Любой динамично развивающийся сайт (от корпоративного до домашней страницы) или портал также содержит файлы и сценарии, потеря которых может оказаться

ощутимой в денежном эквиваленте.

- Во время разработки плана резервирования к каждой категории нужно подходить в отдельности. Обратите внимание, что здесь нет пункта "софт". Дело в том, что он должен быть в дистрибутивах и софт восстанавливается именно оттуда.

Железный друг

Одним из самых страшных случаев, который может случиться - нарушение работы оборудования. Тут может потребоваться замена оборудования с полной переустановкой системы. Чтобы этот процесс не отнял слишком много времени, лучше всего заранее иметь в наличии комплект комплектующих, которые могут выйти из строя – жесткий диск, память, материнская плата, процессор.

Если в сети каждая минута простоя сервера может оказаться фатальной, то можно поступить одним из следующих способов: построить кластер или содержать резервные сервера.

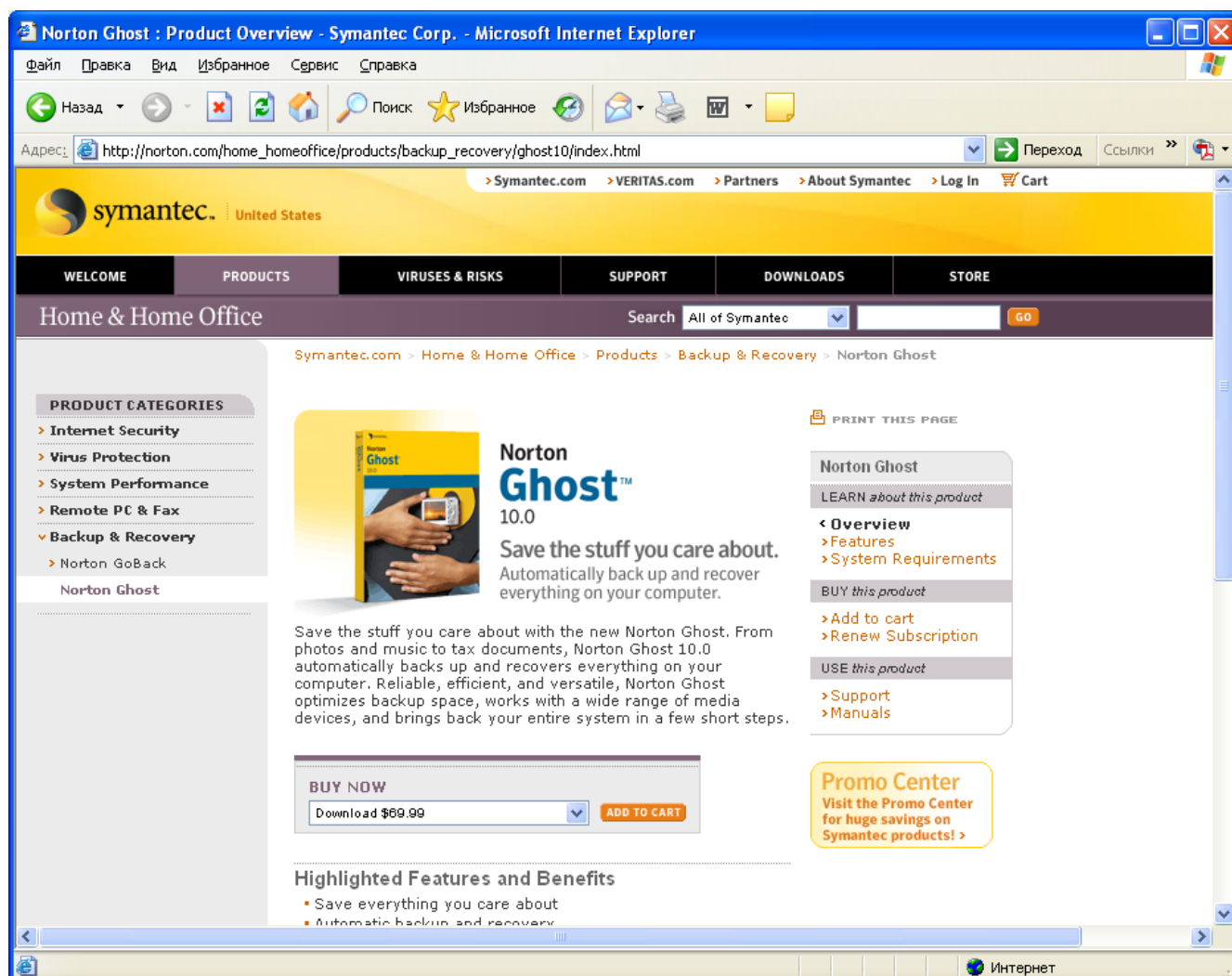
Наиболее надежным способом может быть построение кластера. Если один сервер выходит из строя, то его нагрузку берет на себя второй сервер. Это позволяет добиться практически 100% устойчивости оборудования от возможных неполадок. Но построение кластеров достаточно сложное и дорогое занятие, поэтому компании стараются найти любые другие возможные варианты.

Большинство программ промышленного назначения уже имеют встроенные средства кластеризации. Их работа достаточно проста и дешева. В сети находится один сервер, который является мастером (Master) и один или более серверов подчиненных (Slave). Основной компьютер регулярно посылает в сеть информацию о своей работоспособности и передает подчиненным серверам изменения, которые происходят в базе данных, чтобы на всех серверах была одинаковая копия баз данных. В случае если связь с главным компьютером прерывается, то всю работу на себя берут подчиненные сервера.

Помимо повышения надежности работы, кластер может повышать и производительность, если все сервера будут работать параллельно, и подчиненные сервера будут брать на себя часть нагрузки. Это позволит более эффективно использовать оборудование и пропускную способность сети.

Более дешевым вариантом является использование резервных серверов. Допустим, что у есть один сервер, который должен быть всегда доступен пользователям. В этом сервере устанавливаем дисковый массив RAID, и обязательно с поддержкой зеркалирования (Mirroring), т.е. RAID 1 или RAID 1+0. В этом случае RAID заботиться о сохранности данных, т.к. запись данных производится на два диска одновременно. Если один из них выходит из строя, то информация сохраняется на втором диске.

А что если выйдет из строя материнская плата или процессор? Их замена потребует времени, а мы договорились, что это недопустимо. Чтобы сократить время простоя в случае нештатной ситуации, подготавливаем сервер, с подобной конфигурацией оборудования. В случае нарушения работы оборудования, достаточно подключить RAID массив к резервному серверу, переключить сетевой кабель и можно продолжать работу. Так как оборудование на обоих серверах одинаковое, переустановка системы не потребует времени, и RAID будет работать на другом железе без изменения конфигурационных файлов.



Norton Ghost позволяет резервировать весь диск

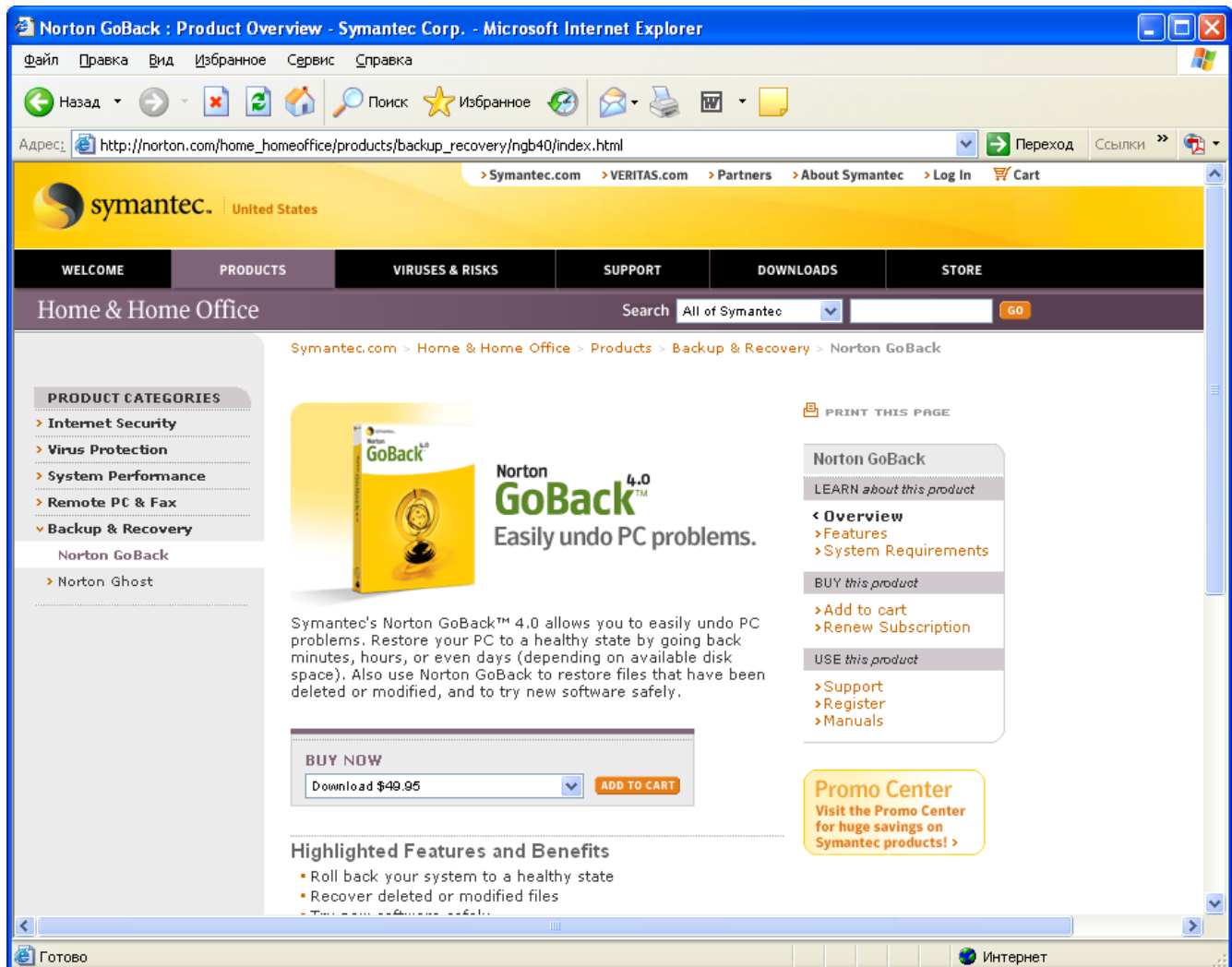
Если в сети несколько серверов с одинаковой конфигурацией, то один резервный сервер может служить заменой для любого из них. Таким образом, обеспечение доступности данных становится намного дешевле построения кластера.

В одном офисе я видел очень интересное решение. На всех клиентских компьютерах были установлены маленькие жесткие диски, жесткие диски на которых работала только ОС и ей необходимые файлы и программы. Помимо этого у всех были подключены большие диски через Mobile Rack (устройство, позволяющее сделать жесткий диск съемным). Администратор каждый вечер снимали жесткие диски, и запускал резервирование каждого диска в своем компьютере.

В случае проблем с компьютером или ОС, жесткий диск снимается, и переносится на другой компьютер. Для этого у администратора всегда есть подготовленный системный блок, который может заменить испорченное оборудование.

Если хранение целого системника слишком дорого, то можно завести хотя бы жесткий диск, на котором уже будет установлена ОС. В случае сбоя, достаточно подменить жесткие диски и перенести на новый диск, с уже установленной ОС и программами документы из резервной копии и можно приступать к работе. Только в этом случае нужно еще помолиться всем

всевышним, чтобы компьютер загрузился. Если на резервном диске ОС установлена на несовместимом оборудовании, то окна могут не загрузиться. Бывают случаи, что во время загрузки просят кучу драйверов, но даже если все указать правильно, полноценный старт ОС остается невозможным.



С помощью программы Norton GoBack можно откатить систему, как в XP, но в более старых версиях окон

Хранение резервных копий

Несмотря на использование RAID 1 и кластера, резервное копирование никто не отменял и его делать необходимо. Но куда резервировать данные? Однажды меня на работе вызвали в другой отдел восстановить данные после выхода из строя жесткого диска (я был программером и это не входило в мои обязанности, но я пошел). Восстановить данные, конечно же, не удалось, потому что жесткий диск вышел из строя окончательно и без поворотно, поэтому я задал вполне логичный вопрос – «А где резервная копия?». Ответ был прост, как и владельцы компьютера – резервная копия производилась на тот же диск, но только в другой раздел. Некоторым людям очень тяжело объяснить, что если ломается диск, то ломаются все его разделы, а не только один из них.

Но самое интересное во всей этой истории то, что диск начал рассыпаться уже достаточно давно. Так уже получилось, что основной раздел был в начале диска, а раздел для резервной копии в самом конце. Уже несколько месяцев во время резервирования происходили ошибки доступа, и никто не обращал на это внимание. Диск явно начал сыпаться, начиная с раздела, на котором хранилась резервная копия, и постепенно испорченные блоки покрыли весь жесткий диск.

Резервную копию всегда нужно делать на отдельный носитель. Это может быть как отдельный жесткий диск, благо на них цены падают не по дням, а по часам, или любой сменный носитель достаточного объема, например, CD-RW или DVD-RW.

Хранение на отдельном носителе позволяет защититься от проблем с оборудованием, но не гарантирует защиту от воровства или стихийных бедствий. Меня поражают администраторы, которые используют сейфы для хранения абсолютно бесполезных бумаг, гарантийных талонов, а резервные копии помещают в простой деревянный ящик. Хочется спросить таких людей – «А зачем вы защищаете сервер всеми возможными средствами, когда кто-нибудь может просто украсть резервную копию из шкафчика?».

Резервная копия должна быть надежно защищена. Лучше всего, если это будет несгораемый шкафчик, тогда даже большинство стихийных бедствий не сможет уничтожить ваши данные.



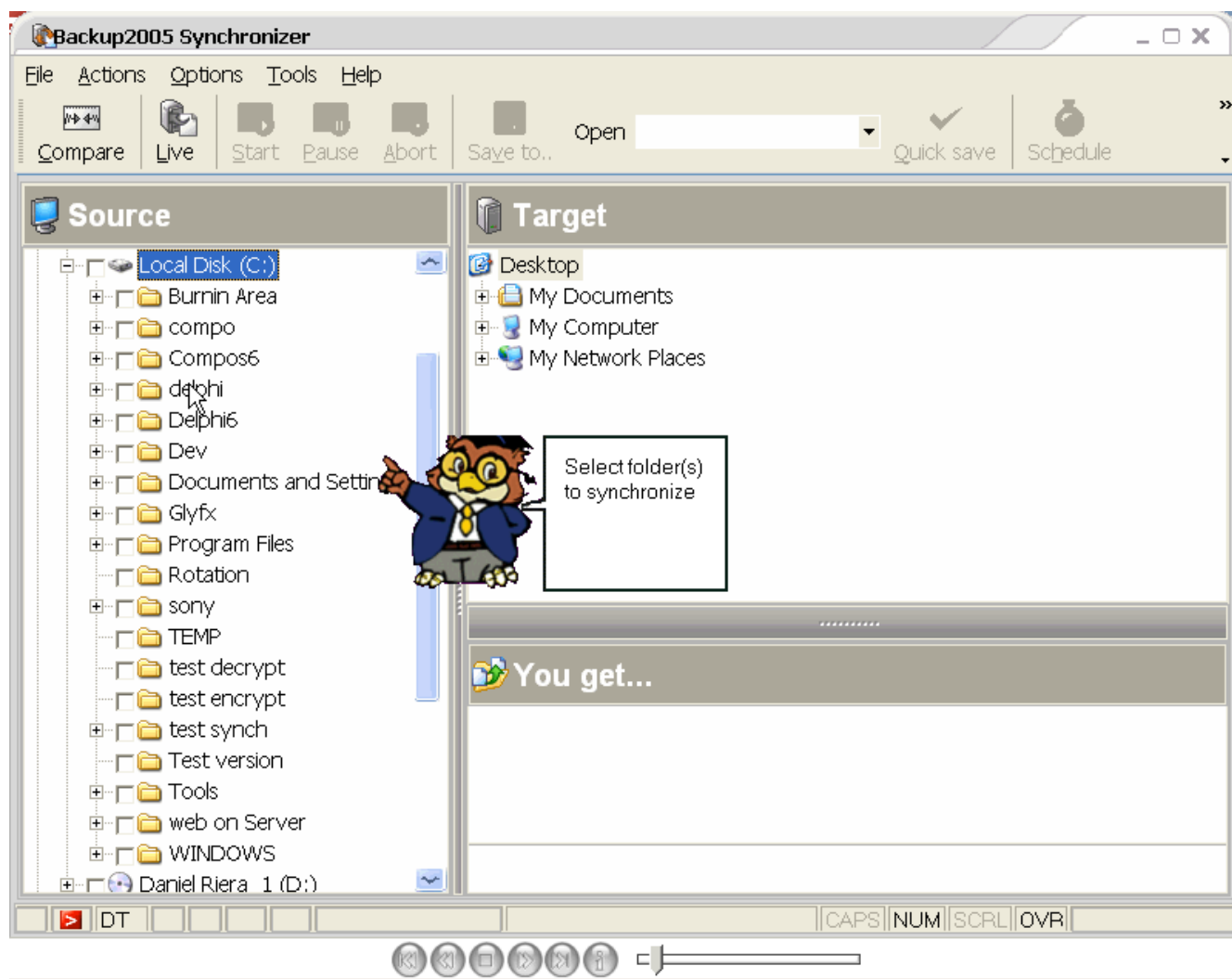
Технология iDisk от Apple

В настоящее время в Интернете снова начинают развиваться сервисы по предоставлению дискового пространства. Сделав резервную копию на такой диск, можно быть уверенным, что данные будут надежно защищены. Владельцы сервисов защищают такие диски с помощью RAID массивов, поэтому на сервере данные исчезнуть не могут.

Можно с уверенностью сказать, что подобные диски будут развиваться, потому что компания Apple с помощью своей новой технологии iDisk сделала Интернет диски удобными и доступными для своих пользователей и пользователей MS Windows. На очереди и остальные системы. Подробнее о технологии iDisk можно узнать на сайте компании Apple http://www.mac.com/1/iTour/tour_idisk.html.

Политика резервного копирования

От того, как правильно будешь резервировать данные, зависит скорость резервирования и потери после восстановления. Если данные на сервере занимают сотни гигабайт, то необходимо достаточно много времени на копирование всех данных и при этом будет происходить большая нагрузка на сервер. Если копирование происходит по сети, то нагрузка будет и на сеть, что сделает сервер менее доступным.



@Home Backup 2005 - простая и удобная утилита для домашнего копирования

Наша задача построить резервирование максимально эффективным методом, чтобы оно занимало как можно меньше времени, и создавалась копия всех необходимых данных.

При планировании резервирования, необходимо учитывать, что если произойдет поломка жесткого диска, то все изменения, внесенные с момента создания последней резервной копии, будут потеряны. В связи с этим, необходимо сохранять копии важных данных как можно чаще, но при этом не забывать, что этот процесс достаточно накладен для сервера.

Итак, сколько носителей информации нам понадобится, как часто их использовать и как ими пользоваться? Это зависит от многих факторов:

- хранящейся информации;
- как часто она изменяется;
- есть ли возможность ручного восстановления большого количества потерянных данных;
- как долго сервер может быть недоступен;
- какие данные изменяются чаще всего.

И этот список можно продолжить, но мы остановимся пока на них. А начнем рассмотрение с последнего. Нужно четко себе представлять, какие данные в системе изменяются и с какой периодичностью. После этого разделите их на три категории: часто изменяемые, редко изменяемые и изменяемые с определенной периодичностью.

Основные директории, которые должны резервироваться:

- \Windows - содержит конфигурационные файлы;
- \Document and Settings – пользовательские файлы;
- директория, содержащая WEB файлы;
- другие директории с пользовательскими данными.

Редко, но метко

К редко изменяемым файлам можно сразу отнести конфигурационные файлы. Они изменяются достаточно редко. В большинстве серверов массовое изменение конфигурации происходит на этапе установки сервера. После этого все может работать годами, и изменения происходят в случае обновления программ или внесения каких-то корректировок.

Для хранения конфигурации хватит даже самого небольшого носителя с невысокой скоростью. Главное его достоинство должно быть возможность перезаписи. Я для хранения конфигурации использую ZIP и JAZ диски. В заархивированном виде достаточно одной дискеты.

Так как конфигурация изменяется редко, то можно делать копии сразу после внесения изменений. Для этого достаточно сразу же скопировать измененный файл на диск, без копирования всех конфигурационных файлов.

При восстановлении данных необходимо всегда начинать с конфигурации.

Редко, но метко

Часто изменяемыми данными могут быть базы данных и основные файлы и документы

пользователей, которые изменяются каждый день. Их резервные копии можно и нужно создавать каждый день. Если процесс копирования отнимает слишком много времени, то следует это делать после рабочего дня, или в обеденный перерыв, когда нагрузка на сервер ниже. Чтобы не сидеть над компьютером в такие моменты, можно создать сценарии, которые будут выполняться по запланированному заданию. Если производить резервирование два раза в день (в обеденный перерыв и в конце рабочего дня), то в случае аварии, рискуешь потерять изменения только за пол дня, с момента резервирования до момента сбоя системы.

Для этих данных я использую 7 перезаписываемых носителей. Каждый из них я называю днями недели, потому что в понедельник копирую данные на диск с надписью «Понедельник», во вторник пишу на диск «Вторник» и так далее. Помимо этого, каждый понедельник все данные записываются на одноразовый носитель типа CD-R или DVD-R.

Часто, но не все

Далеко не все пользовательские файлы изменяются ежедневно. Большинство из них может храниться без изменений годами. Чтобы не тратить каждый раз время на не измененные данные, можно использовать программы, которые позволят копировать только измененные данные. Самый простой вариант - выбрать все файлы, у которых дата изменения находится в определенном промежутке времени.

The screenshot displays the Acronis website interface. At the top, there's a navigation bar with links for 'Для прессы', 'Партнерам', 'Компания', 'Работа в Acronis', and a language/region selector. Below this is a search bar and a main menu with 'Начало', 'Продукты', 'Загрузить', 'Купить', 'Поддержка', 'Покупка онлайн', and 'Мой профиль'. The main banner features the 'Решения Acronis' (Acronis Solutions) title, listing 'Копирование и восстановление' (Backup and Recovery), 'Безопасность' (Security), and 'Управление дисками' (Disk Management). To the right of the banner, a promotional offer for 'Acronis True Image 9.0' and 'Acronis Drive Cleanser' is shown with a 30% discount. Below the banner, the website is organized into several columns. The first column, 'Корпоративные решения' (Corporate Solutions), lists products like 'Acronis True Image' (with sub-options for Corporate Workstation, Enterprise Server, Server for Windows, and Server for Linux), 'Acronis Snap Deploy', 'Acronis Drive Cleanser', and 'Acronis Privacy Expert Corporate'. The second column, 'Малый бизнес и дом' (Small Business and Home), lists 'Acronis True Image', 'Acronis Disk Director Suite', 'Acronis Power Utilities', and 'Acronis Privacy Expert Suite'. The third column, 'ОЕМ-решения' (OEM Solutions), lists 'Acronis LiveMedia', 'Acronis True Image OEM', 'Acronis Easy Boot', and 'Дополнительная информация'. The fourth column, 'Новые продукты' (New Products), features 'Acronis True Image 9.0' with a description of its backup capabilities and a 'Купить!' (Buy!) button. The fifth column, 'Отзывы покупателей' (Customer Reviews), includes a testimonial from a user named 'True Image'. The bottom section of the website contains a 'Центр загрузки' (Download Center) with links to 'Обновление продуктов' (Product Updates), 'Обновление базы программ-шпионов' (Spyware Database Updates), and 'Центр загрузки' (Download Center), as well as a 'Служба Поддержки' (Support Service) link.

Acronis True Image - отличная утилита для резервирования отдельной папки, раздела или целого диска

При использовании такой политики, можно действовать следующим методом:

- в конце недели производится полное копирование директорий с пользовательскими

данными;

- каждый день можно сохранять измененные файлы. В случае аварии восстановление должно происходить точно в той последовательности, в которой происходило резервирование. Сначала восстанавливается полная копия. Потом последовательно возвращаем на родину все файлы из резервных копий, в которых находятся изменения. Если последовательность будет нарушена, то ты рискуешь перезаписать новый файл более старым.

Копирование файлов по дате изменения удобно, но доступно не всегда. В большинстве утилит есть только обновление существующей копии. В этом случае сначала создается полная копия, а потом с помощью специального ключа задается обновлением. При этом в полной копии обновляются файлы, которые были изменены.

Этот способ хорош, но он заменяет все старые файлы. После этого нельзя откатиться назад и узнать, что было до последнего резервного копирования. С другой стороны, в директории в резервной копии находится полная копия и при восстановлении достаточно скопировать ее в систему и работа может продолжаться.

Благодаря сохранению изменений (каждый день изменяется не так уж много файлов), резервирование будет происходить достаточно быстро и его можно делать в процессе работы сервера. Но в данном случае рискуем испортить файлы. Допустим, что есть два жестко связанных файла, информация в которых должна быть связанной. Например, если в один файл записываются данные, то в другом должны быть такие же данные. Если во время копирования одного файла будет изменен другой файл, то в резервную копию первый попадает измененным, а второй нет. При восстановлении будут серьезные проблемы, потому что нарушится целостность и работа после восстановления может быть нарушена.

Периодичность

Данные, которые изменяются с определенной периодичностью, нужно резервировать в зависимости от изменений. Например, некоторые файлы могут использоваться во время ежемесячной отчетности. Как правило, они достаточно большого размера и создавать регулярную резервную копию не имеет смысла. Намного эффективнее делать копию в конце формирования отчетности, и потом весь месяц не тратить ресурсы на лишнее резервирование, не изменяемых данных.

Полное копирование


Наиболее надежным способом является создание полной копии всего жесткого диска. В этом случае, информация может сохраняться в не зависимости от файловой системы, потому что программа копирует весь диск один к одному через прямой доступ к дорожкам. Восстановление полной копии гарантирует, что все права восстановлены четко и программы сразу же готовы к использованию.

У этого способа достаточно много недостатков:

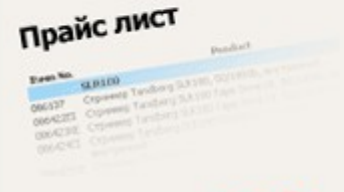
- необходимо много времени;
- слишком большая нагрузка на сервер;
- невозможно реализовать средствами ОС. В большинстве ОС нет необходимых программ, и приходится обращаться к сторонним разработчикам;
- в резервную копию попадают все файлы, и даже те, которые не являются необходимыми, например временные файлы директорий /tmp в Linux и Windows\Temp в Windows.

BackUp.ru ■ О фирме ■ Новости ■ Цены ■ Акции ■ Запрос ■ FAQ
BACKUP.RU

у с т р о й с т в а д л я р е з е р в н о г о х р а н е н и я д а н н ы х



TANDBERG DATA
на защите информации



специальное предложение

03 октября 2005 г. Теперь компактные стриммеры **Tandberg 420LTO** поставляются в комплекте с ПО **Veritas Backup Exec Quickstart**
Все новости...

Каталог оборудования

TANDBERG DATA

Ленточные накопители LTO

840LTO Новейшие ленточные накопители LTO Ultrium3. [Подробнее...](#)

440LTO Ленточные накопители LTO второго поколения (LTO Ultrium2). [Подробнее...](#)


420LTO Ленточные накопители LTO Ultrium2 половинной высоты. [Подробнее...](#)


240LTO Ленточные накопители на платформе LTO Ultrium базового уровня. [Подробнее...](#)

Ленточные накопители SLR™

SLR140 Накопитель, демонстрирующий потенциал платформы SLR: запись на один картридж до 140 Гигабайт* информации со скоростью до 12 Мб*/с. [Подробнее...](#)

SLR100 Стриммер Тандберг SLR100 обладает емкостью до 100 Гигабайт* и скоростью записи до 10 Мб*/с. [Подробнее...](#)





apkaqa
Официальный дистрибьютор
TANDBERG DATA с 1993 года

С. Петербург:
(812) 449-7750
Москва:
(095) 792-5542
E-mail: info@backup.ru

www.backup.ru – коммерческий сайт по железу и софту для резервного копирования

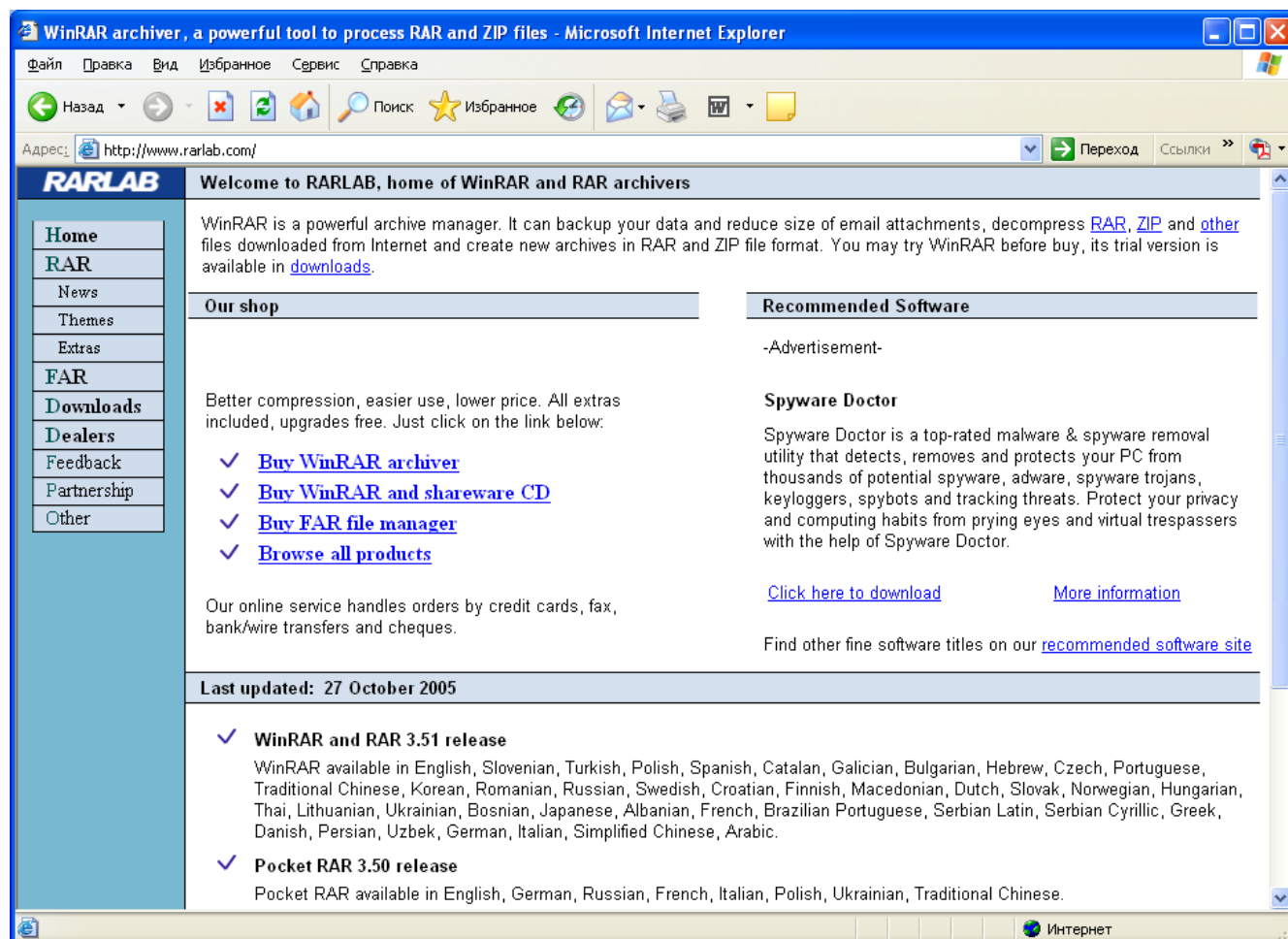
Резервирование полной копией очень удобно использовать для переноса данных на другой сервер или тиражировании конфигурации. Например, вам необходимо настроить несколько клиентских компьютеров со схожей конфигурацией. Настрой один компьютер, сделай его полную копию и восстанови на всех компьютерах, на которые нужно тиражировать конфигурацию. Такой метод надежнее, чем простой перенос файлов с одного компьютера на другой. Классикой резервирования всего диска является Norton Ghost. Подумай о его использовании.

Носители

Теперь рассмотрим, сколько носителей нам понадобится для хранения всех резервных копий. Для каждого типа данных нужны свои носители, потому что их копирование происходит с разной периодичностью и рассматривать их надо отдельно:

- Конфигурационные файлы. Мы уже определились, что для них достаточно ZIP или JAZ носителя. Желательно иметь две одинаковых копии, потому что любые дискеты могут портиться и выходят из строя намного чаще, чем жесткие диски;
- Периодично обновляемые данные. Такие данные лучше всего записывать на носитель и

хранить год, а то и более. Я для этих целей использую CD-R, потому что его объема достаточно для моих данных и при этом диск нельзя стереть. Каждый месяц происходит запись диска со всеми периодически обновляемыми данными, и храниться в течение года. Таким образом, я в течение года по резервной копии могу просмотреть, какие данные были на любой отчетный период;



Резервные копии чаще всего занимают много места, поэтому их нужно резервировать и WinRAR тут как раз к лицу

- Часто обновляемые данные. При выборе носителя главным фактором должна быть скорость работы, потому что чаще всего эти данные имеют большой размер. Резервное копирование должно производиться максимально короткое время, чтобы сервер не ощутил долговременных лишних нагрузок.

Удачного копирования

Как видишь, политика резервирования зависит от многих данных. Я постарался показать вам основные принципы, по которым вы должны строить свою политику. Предложенная мной политика не сможет одинаково подойти для всех систем, но ее можно использовать как базу.

Мы рассмотрели только теорию и основы. Базы данных – это вообще отдельная тема, потому что тут есть журналы транзакций, системные таблицы, пользовательские данные и все это может резервироваться по отдельности. В общем, не откладывай журнал, он расскажет тебе еще много интересного.