МИНОБРНАУКИ РОССИИ

ФГБОУ ВПО «ИЖЕВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ М. Т. КАЛАШНИКОВА»

Кафедра «Программное обеспечение»

Реферат

на тему «Резервное копирование информации»

Выполнил:

Студент группы Б01-191-1 Р.И. Мусин

Проверил: В.П. Соболева

Ижевск 2015

СОДЕРЖАНИЕ

[Введение 3](#_Toc438657703)

[1. Виды резервного копирования 4](#_Toc438657704)

[2. Схемы ротации 6](#_Toc438657705)

[2.1. Одноразовое копирование 6](#_Toc438657706)

[2.2. Простая ротация 6](#_Toc438657707)

[2.3. «Дед, отец, сын» 6](#_Toc438657708)

[2.4. «Ханойская башня» 7](#_Toc438657709)

[2.5. «10 наборов» 7](#_Toc438657710)

[3. Способы хранения резервной копии 8](#_Toc438657711)

[4. Причины утери информации 9](#_Toc438657712)

[4.1. Эксплуатационные поломки носителей информации 9](#_Toc438657713)

[4.2. Стихийные и техногенные бедствия 9](#_Toc438657714)

[4.3. Вредоносные программы 10](#_Toc438657715)

[4.4. Человеческий фактор 11](#_Toc438657716)

[5. Утилиты 12](#_Toc438657717)

[5.1. Acronis Backup & Recovery 10 Workstation 12](#_Toc438657718)

[5.2. Paragon Drive Backup 10 Workstation 15](#_Toc438657719)

[Заключение 17](#_Toc438657720)

[Список использованных источников 18](#_Toc438657721)

ВВЕДЕНИЕ

Каждый пользователь хранит на компьютере различную информацию. Практически у каждого пользователя на компьютере хранится важная информация, потеря которой может, как минимум, расстроить пользователя (личные фото, коллекция музыки, рабочие документы и т.д.).

К сожалению, информация не может абсолютно надежно храниться на компьютере. Отказ аппаратной части (жесткий диск) или вирусная атака и даже неаккуратность самого пользователя (случайное удаление информации) могут привести к потере важных данных. Чтобы обезопасить важную информацию необходимо делать резервное копирование данных.

Резервное копирование файлов и информации позволит вам защитить эти данные в случае, если произойдет выход из строя основного носителя информации (например, жесткий диск компьютера) или вирусной атаки.

Резервное копирование данных – процесс создания копий важной информации, которые хранятся в других хранилищах данных (флешка, жесткий диск, DVD-диск, облачный сервис и т.д.). Резервное копирование данных – очень важная операция, которую должен производить любой пользователь через определенный промежуток времени.

1. ВИДЫ РЕЗЕРВНОГО КОПИРОВАНИЯ

Существует множество способов делать резервные копии:

1. полное резервное копирование - обычно затрагивает всю систему и все файлы. Еженедельное, ежемесячное и ежеквартальное резервное копирование подразумевает создание полной копии всех данных. Обычно оно выполняется тогда, когда копирование большого объёма данных не влияет на работу организации. Последующие резервные копирования, выполняемые до следующего полного копирования, могут быть дифференциальными или инкрементными, главным образом для того, чтобы сохранить время и место на носителе;
2. дифференциальное резервное копирование (Differential backup) - каждый файл, который был изменен с момента последнего полного резервного копирования, копируется каждый раз заново. Дифференциальное копирование ускоряет процесс восстановления. Все копии файлов делаются в определенные моменты времени, что, например, важно при заражении вирусами;
3. инкрементное резервное копирование (Incremental backup) - при добавочном («инкрементном») резервном копировании происходит копирование только тех файлов, которые были изменены с тех пор, как в последний раз выполнялось полное или добавочное резервное копирование. Последующее инкрементное резервное копирование добавляет только файлы, которые были изменены с момента предыдущего. Инкрементное резервное копирование занимает меньше времени, так как копируется меньшее количество файлов. Однако процесс восстановления данных занимает больше времени, так как должны быть восстановлены данные последнего полного резервного копирования, а также данные всех последующих инкрементных резервных копирований. В отличие от дифференциального копирования, изменившиеся или новые файлы не замещают старые, а добавляются на носитель независимо;
4. клонирование - клонирование позволяет скопировать целый раздел или носитель (устройство) со всеми файлами и директориями в другой раздел или на другой носитель. Если раздел является загрузочным, то клонированный раздел тоже будет загрузочным;
5. резервное копирование в виде образа — точная копия всего раздела или носителя (устройства), хранящаяся в одном файле;
6. резервное копирование в режиме реального времени - позволяет создавать копии файлов, директорий и томов, не прерывая работу, без перезагрузки компьютера;
7. холодное резервирование - база данных выключена или закрыта для потребителей. файлы данных не изменяются, и копия базы данных находится в согласованном состоянии при последующем включении;
8. горячее резервирование - база данных включена и открыта для потребителей. Копия базы данных приводится в согласованное состояние путём автоматического приложения к ней журналов резервирования по окончании копирования файлов данных.
9. СХЕМЫ РОТАЦИИ

Смена рабочего набора носителей в процессе копирования называется их ротацией. Для резервного копирования очень важным вопросом является выбор подходящей схемы ротации носителей (например, магнитных лент).

* 1. Одноразовое копирование

Простейшая схема, не предусматривающая ротации носителей. Все операции проводятся вручную. Перед копированием администратор задает время начала резервного копирования, перечисляет файловые системы или каталоги, которые нужно копировать. Эту информацию можно сохранить в базе данных, чтобы её можно было использовать снова. При одноразовом копировании чаще всего применяется полное копирование.

* 1. Простая ротация

Простая ротация подразумевает, что некий набор лент используется циклически. Например, цикл ротации может составлять неделю, тогда отдельный носитель выделяется для определенного рабочего дня недели. Недостаток данной схемы — она не очень подходит для ведения архива, поскольку количество носителей в архиве быстро увеличивается. Кроме того, инкрементальная/дифференциальная запись проводится на одни и те же носители, что ведет к их значительному износу и, как следствие, увеличивает вероятность отказа.

* 1. «Дед, отец, сын»

Данная схема имеет иерархическую структуру и предполагает использование комплекта из трех наборов носителей. Раз в неделю делается полная копия дисков компьютера («отец»), ежедневно же проводится инкрементальное (или дифференциальное) копирование («сын»). Дополнительно раз в месяц проводится еще одно полное копирование («дед»). Состав ежедневного и еженедельного набора постоянен. Таким образом, по сравнению с простой ротацией в архиве содержатся только ежемесячные копии плюс последние еженедельные и ежедневные копии. Недостаток данной схемы состоит в том, что в архив попадают только данные, имевшиеся на конец месяца, а также износ носителей.

* 1. «Ханойская башня»

Схема призвана устранить некоторые из недостатков схемы простой ротации и ротации «Дед, отец, сын». Схема построена на применении нескольких наборов носителей. Каждый набор предназначен для недельного копирования, как в схеме простой ротации, но без изъятия полных копий. Иными словами, отдельный набор включает носитель с полной недельной копией и носители с ежедневными инкрементальными (дифференциальными) копиями. Специфическая проблема схемы «ханойская башня» — ее более высокая сложность, чем у других схем.

* 1. «10 наборов»

Данная схема рассчитана на десять наборов носителей. Период из сорока недель делится на десять циклов. В течение цикла за каждым набором закреплен один день недели. По прошествии четырехнедельного цикла номер набора сдвигается на один день. Иными словами, если в первом цикле за понедельник отвечал набор номер 1, а за вторник — номер 2, то во втором цикле за понедельник отвечает набор номер 2, а за вторник — номер 3. Такая схема позволяет равномерно распределить нагрузку, а, следовательно, и износ между всеми носителями.

# СПОСОБЫ ХРАНЕНИЯ РЕЗЕРВНОЙ КОПИИ

Существует много способов хранения резервных копий. Вот некоторые из них:

1. лента стримера — запись резервных данных на магнитную ленту стримера;
2. «облачный» бэкап — запись резервных данных по «облачной» технологии через онлайн-службы специальных провайдеров;
3. DVD или CD — запись резервных данных на компактные диски;
4. HDD — запись резервных данных на жёсткий диск компьютера;
5. LAN — запись резервных данных на любую машину внутри локальной сети;
6. FTP — запись резервных данных на FTP-серверы;
7. USB — запись резервных данных на любое USB-совместимое устройство (такое, как флэш-карта или внешний жёсткий диск).
8. ПРИЧИНЫ УТЕРИ ИНФОРМАЦИИ
   1. Эксплуатационные поломки носителей информации

Описание: случайные поломки в пределах статистики отказов, связанные с неосторожностью или выработкой ресурса. Если важная информация уже потеряна, то можно обратиться в специализированную службу, но надёжность не стопроцентная.

Решение: хранить всю информацию (каждый файл) минимум в двух экземплярах (причём каждый экземпляр на своём носителе данных). Для этого применяются:

1. RAID 1, обеспечивающий восстановление самой свежей информации. Файлы, расположенные на сервере с RAID, более защищены от поломок, чем хранящиеся на локальной машине;
2. ручное или автоматическое копирование на другой носитель. Для этого может использоваться система контроля версий, специализированная программа резервного копирования или подручные средства наподобие периодически запускаемого cmd-файла.
   1. Стихийные и техногенные бедствия

Описание: шторм, землетрясение, кража, пожар, прорыв водопровода — всё это может привести к потере всех носителей данных, расположенных на определённой территории.

Борьба: единственный способ защиты от стихийных бедствий — держать часть резервных копий в другом помещении. В частности, помогает резервное копирование через сеть на компьютер, расположенный достаточно далеко (или в облачное хранилище данных).

* 1. Вредоносные программы

Описание: в эту категорию входит случайно занесённое ПО, которое намеренно портит информацию — вирусы, черви, «троянские кони». Иногда факт заражения обнаруживается, когда немалая часть информации искажена или уничтожена.

Борьба:

1. установка антивирусных программ на рабочие станции. Простейшие антивирусные меры — отключение автозагрузки, изоляция локальной сети от Интернета;
2. обеспечение централизованного обновления: первая копия антивируса получает обновления прямо из Интернета, а другие копии настроены на папку, куда первая загружает обновления; также можно настроить прокси-сервер таким образом, чтобы обновления кешировались (это всё меры для уменьшения трафика);
3. иметь копии в таком месте, до которого вирус не доберётся — выделенный сервер или съёмные носители;
4. если копирование идёт на сервер: обеспечить защиту сервера от вирусов (либо установить антивирус, либо использовать ОС, для которой вероятность заражения мала). Хранить версии достаточной давности, чтобы существовала копия, не контактировавшая с заражённым компьютером;
5. если копирование идёт на съёмные носители: часть носителей хранить (без дописывания на них) достаточно долго, чтобы существовала копия, не контактировавшая с заражённым компьютером;
6. использование носителей с однократной записью: CD-R, DVD-R, BD-R. Их объём недостаточен для серьёзных применений.
   1. Человеческий фактор

Описание: намеренное или ненамеренное уничтожение важной информации — человеком, специально написанной вредоносной программой или сбойным ПО.

Борьба:

1. тщательно расставить права на все ресурсы, чтобы другие пользователи не могли модифицировать чужие файлы. Исключение делается для системного администратора, который должен обладать всеми правами на всё, чтобы быть способным исправить ошибки пользователей, программ;
2. построить работающую систему резервного копирования — систему, которой люди реально пользуются и которая достаточно устойчива к ошибкам оператора. Если пользователь не пользуется системой резервного копирования, вся ответственность за сохранность ложится на него;
3. хранить версии достаточной давности, чтобы при обнаружении испорченных данных файл можно было восстановить;
4. перед переустановкой ОС следует обязательно копировать всё содержимое раздела, на которой будет установлена ОС, на сервер, на другой раздел или на CD/DVD;
5. оперативно обновлять ПО, которое заподозрено в потере данных.

# УТИЛИТЫ

Двумя основными лидерами среди утилит для резервного копирования информации являются Acronis Backup & Recovery 10 Workstation и Paragon Drive Backup 10 Workstation.

* 1. Acronis Backup & Recovery 10 Workstation

Компанию Acronis Inc. и ее продукты, наверное, никому представлять не нужно. Она является одним из лидеров российского рынка систем резервного копирования. В ее арсенале есть целый ряд программ, рассчитанных на различных потребителей. В том числе есть и серия корпоративных продуктов. В нее входит несколько серверных систем и две программы для рабочих станций - Acronis Backup & Recovery 10 Workstation и Acronis Backup & Recovery 10 Workstation Advanced, оба продукта издаются в России под маркой 1С: Дистрибьюция. Первая больше подходит для малых офисов. Вторая же является наиболее функциональной. Именно ее мы и выбрали для нашего обзора.

Рассмотрим "корпоративные" функции продукта, в первую очередь, отметив организацию резервного копирования. Здесь можно сказать о системе дублирования создаваемых программой архивов, то есть информация может одновременно копироваться в два хранилища, например, в сетевое и локальное. Такой подход позволяет обеспечить "резервное копирование" самих архивов, а это в свою очередь увеличивает надежность работы системы резервирования без дополнительных затрат (приобретения дополнительных емкостей для хранения архивов), тем более что чаще всего на жестких дисках офисных компьютеров есть много свободного пространства.

Следующий важный момент – модуль дедупликации (он приобретается отдельно). Дедупликация – один из наиболее эффективных способов уменьшения объемов резервных копий за счет исключения дублей – одинаковой информации. В некоторых случаях с ее помощью можно заметно уменьшить требуемый для хранения архивов объем NAS, а значит существенно сократить затраты на приобретение и обслуживание оборудования, а также на оплату электроэнергии. Стоит отметить, что во многих программах для резервного копирования, включая и рассматриваемый продукт, есть другие средства для сокращения размера архивов: сжатие данных, исключение из них файлов определенных типов, инкрементное копирование, автоматическое удаление устаревших копий и пр. Однако у дедупликации есть одна очень важная особенность. Если все остальные способы работают исключительно с одним источником, то она способна находить дублирующиеся данные на всех рабочих станциях и серверах сети. Но часто бывает, что сотрудники для удобства работы копируют какие-то данные на свои машины. В результате в корпоративной сети могут находиться десятки копий одних и тех же данных. В этом случае дедупликация может оказать значительную помощь.

Далее можно рассмотреть функции, направленные на обеспечение бесперебойной работы сотрудников. Речь идет о ситуациях, связанных с выходом из строя программного или аппаратного обеспечения рабочих компьютеров. Первая проблема решается путем создания образов операционной системы со всем установленным и настроенным ПО. В случае необходимости он разворачивается поверх поврежденной ОС буквально за несколько минут. Но это еще не все - подобная функциональность есть и во многих "домашних" продуктах. В Acronis Backup & Recovery 10 Workstation функциональность по работе с образами заметно расширена таким образом, чтобы позволить решить проблему с повреждением аппаратного обеспечения. Во-первых, она дополнена системой виртуализации. Созданный образ в любой момент можно конвертировать в формат виртуальной машины (поддерживаются форматы VMware, Microsoft Hyper-V, Citrix XenServer и Parallels). Далее остается только запустить эту виртуальную машину на любом ПК, и сотрудник сможет продолжать работу в привычном окружении. Во-вторых, у Acronis Backup & Recovery 10 Workstation есть модуль Universal Restore (приобретается отдельно). Он обеспечивает возможность разворачивания образа на любом компьютере вне зависимости от состава его аппаратного обеспечения. Кстати, данный модуль может помочь не только для переноса системы в случае поломки ПК, но и для быстрого разворачивания новых рабочих мест.

Следующий очень важный аспект функционирования корпоративной системы резервного копирования – интеграция в существующую информационную систему предприятия. Для этого в Acronis Backup & Recovery 10 Workstation предусмотрено несколько инструментов. Особенно стоит отметить автоматическое выполнение команд до начала процедуры резервирования и после ее завершения. С их помощью можно, к примеру, остановить какую-то систему на время копирования, а потом запустить ее снова. Конечно, такая необходимость возникает не так часто, однако иногда она бывает (особенно при работе с некоторым специальным ПО). Также в некоторых случаях весьма полезной бывает возможность работы из командной строки с поддержкой скриптов.

Нельзя забывать и о процедурах развертывания и администрирования системы резервного копирования. Для увеличения эффективности работы ИТ-персонала и сокращения издержек на обслуживание в Acronis Backup & Recovery 10 Workstation реализовано сразу же несколько очень важных функций. В первую очередь, стоит отметить возможность удаленной инсталляции программы на рабочих станциях. Причем осуществляться она может в фоновом режиме (для пользователей) и без перезагрузки. Это позволяет очень быстро развернуть систему резервирования в сети практически любого размера, не останавливая работу офиса.

Помимо этого, в рассматриваемом продукте существует возможность централизованного управления резервированием. Причем она не ограничивается примитивным подключением к рабочим станциям с последующей "ручной" настройкой агента. Речь идет о полноценном администрировании на основе создания политик для целых групп рабочих станций. Отдельно стоит отметить поддержку технологии Wake-on-LAN, которая позволяет включать выключенные машины перед запуском процесса архивирования. Но и это еще не все. Acronis Backup & Recovery 10 Workstation предоставляет сотрудникам ИТ-отдела широкие возможности по управлению резервными копиями, размещенными в различных хранилищах. Администраторы могут проверять архивы, осуществлять слияние резервных копий вручную или же настроить эту процедуру на автоматическое выполнение.

Acronis Backup & Recovery 10 Workstation – очень и очень мощный продукт, в котором реализован широкий спектр функций для построения корпоративной системы резервного копирования. Именно это и является его главной особенностью. Благодаря описанным функциям, данный продукт может с легкостью интегрироваться в информационные системы любого размера.

* 1. Paragon Drive Backup 10 Workstation

Компания Paragon – еще один весьма известный игрок на рынке ПО для работы с жесткими дисками. Есть среди них и целый ряд утилит для организации резервного копирования. В том числе, и Paragon Drive Backup 10 Workstation – программа, предназначенная для корпоративных пользователей. Именно ее мы и взяли для нашего сравнения.

Итак, Paragon Drive Backup 10 Workstation. Как и уже рассмотренная нами программа, данный продукт является полнофункциональным решением, то есть в ней есть все необходимое для организации полноценной системы резервного копирования, обеспечивающей не только сохранность данных, но и бесперебойную работу сотрудников.

В первую очередь стоит отметить те возможности, которые направлены на обеспечение непрерывности бизнес-процессов. Среди них особое место занимает технология адаптивного восстановления. Благодаря ей восстановить заархивированную операционную систему со всеми установленными в ней приложениями можно на любой аппаратной платформе. Это позволяет ИТ-отделу при поломке компьютера быстро перевести сотрудника на другой со всем привычным ему окружением. Также нельзя не упомянуть технологию восстановления на гранулярном уровне. С ее помощью пользователи могут начать работать на компьютере, не дожидаясь полного восстановления резервной копии из архива.

В плане организации хранения резервных копий Paragon Drive Backup 10 Workstation ничем особым среди конкурентов не выделяется. В ней реализованы только "стандартные" функции для сокращения размеров архивов. К ним относятся инкрементное и дифференцированное копирование и фильтры для исключения "лишней" информации (к слову сказать, система фильтрации в данной программе весьма мощная и удобная), а если компании будет необходима дедупликация, то придется воспользоваться дополнительным программным или аппаратным обеспечением.

Централизованное управление системой резервного копирования, построенной на базе Paragon Drive Backup 10 Workstation, возможно. Но для этого требуется приобретение специальной программы – Paragon Remote Management. С помощью этого средства можно организовать администрирование процесса архивирования на всех рабочих станциях и серверах корпоративной сети. При этом сотрудникам ИТ-отдела доступны такие возможности, как удаленная установка программы, управление хранилищем архивов и пр. Кроме того, помочь во внедрении рассматриваемого продукта в информационную систему предприятия могут помочь скрипты, которые представляют собой описания последовательно выполняющихся действий. Они могут использоваться для автоматического выполнения различных операций на рабочих станциях сети.

ЗАКЛЮЧЕНИЕ

Резервное копирование информации – очень важный процесс, о котором ни в коем случае нельзя забывать. При небрежительном отношении к этому процессу, любой пользователь может потерять очень важные данные, хранящиеся на его устройстве.

К сожалению, сейчас большинство людей не осознают необходимость резервного копирования, считая, что все проблемы пройдут мимо них. Однако, стоит лишь раз человеку потерять важную информацию по случайности, как он начинает винить себя в том, что не делал никаких резервных копий, а ведь можно было бы всё исправить, если бы этот человек имел хоть одну копию, сделанную недавно.

В настоящее время существует множество программ, которые позволяют почти полностью автоматизировать процесс резервного копирования информации, благодаря чему люди, пользующиеся такими программами, могут больше времени уделять своей работе, забывая о необходимости резервного копирования, а при неудачном ходе событий, когда теряется какая-либо важная информация, могут быстро её восстановить и продолжать работу вместо того, чтобы восстанавливать свою работу из старых копий, или вовсе начинать делать всё сначала.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. <http://www.aif.ru/> Аргументы и факты;
2. <https://ru.wikipedia.org/wiki/Резервное_копирование/> Википедия;
3. <http://compress.ru/> Резервное копирование и восстановление информации;
4. <http://habrahabr.ru/> Хабрахабр;
5. <http://www.handybackup.ru/> Handy Backup.