

Областное государственное бюджетное профессиональное
образовательное учреждение
«ТОМСКИЙ ИНДУСТРИАЛЬНЫЙ ТЕХНИКУМ»

РЕЗЕРВНОЕ КОПИРОВАНИЕ ДАННЫХ

ОТЧЕТ

Специальность «10.02.01 — Организация и технология защиты информации»

Выполнили:

студенты группы № 362

Таран Семён Юрьевич

Бодашков Александр Евгеньевич

«__» _____ 2018 г.

Проверил:

Руководитель работы

Даниил Котырло Андреевич

«__» _____ 2018 г.

ОГЛАВЛЕНИЕ

| | |
|--|----|
| 1. ПРИНЦИПЫ РЕЗЕРВНОГО КОПИРОВАНИЯ | 5 |
| 2. ТОПОЛОГИЯ РЕЗЕРВНОГО КОПИРОВАНИЯ..... | 7 |
| 2.1 Децентрализованная схема резервного копирования данных | 7 |
| 2.2 Централизованная схема резервного копирования данных..... | 8 |
| 2.3 Смешанная схема резервного копирования данных..... | 10 |
| 3. ПРОГРАММЫ ДЛЯ РЕЗЕРВНОГО КОПИРОВАНИЯ | 12 |
| 3.1 Acronis True Image | 12 |
| 3.2 Backup4all | 12 |
| 3.3 Comodo BackUp | 13 |
| 3.4 Symantec Backup Exec | 13 |
| 4. АППАРАТНЫЕ КОМПЛЕКСЫ ДЛЯ РЕЗЕРВНОГО КОПИРОВАНИЯ . | 15 |
| 5. ПОПУЛЯРНЫЙ МЕТОД РЕЗЕРВНОГО КОПИРОВАНИЯ НА КОНКРЕТНОМ ПРИМЕРЕ..... | 18 |
| ЗАКЛЮЧЕНИЕ | 19 |
| СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ | 20 |

ВВЕДЕНИЕ

Резервное копирование - это процесс создания когерентной (непротиворечивой) копии данных. Резервное копирование становится все более важным на фоне значительного увеличения объема данных в компьютерной индустрии. Подсистема резервного копирования - очень важная часть любой информационной системы. При правильной ее организации она способна решить сразу же две задачи. Во-первых, надежно защитить весь спектр важных данных от утери. Во-вторых, организовать быструю миграцию с одного ПК на другой в случае необходимости, то есть, фактически обеспечить бесперебойную работу офисных сотрудников. Только в этом случае можно говорить об эффективной работе резервного копирования. Овладение тактикой резервного копирования - неотъемлемый атрибут профессионализма пользователя и системного администратора. Вытекает она из решения пользователем для себя, какими методами и на каком уровне будет сохраняться информация (от этого зависит требуемое программное и аппаратное обеспечение), объема необходимой к сохранению информации (от этого зависят выбираемые информационные носители), размера и структуры локальной сети (от этого зависит реальный механизм систематического выполнения копирования).

Для выполнения процедуры резервного копирования обычно создаются специальные программно-аппаратные подсистемы, называемые подсистемами резервного копирования. Они как раз и предназначены как для проведения регулярного автоматического копирования системных и пользовательских данных, так и для оперативного восстановления данных. Хранение информации отдельно от системных файлов уже является обязательным правилом. В случае обычного пользователя это означает, как минимум, разделение HDD на три логических диска: для системы, для приложений, для данных. В случае корпоративного сотрудника с большим объемом конфиденциальной информации - размещение информации на

других, не системных физических дисках. Эта мера облегчает и саму операцию архивирования данных. Принцип раздельного хранения информации относится и к файловым архивам, и к образам дисков. Их необходимо также хранить как минимум на несистемных разделах одного HDD. В случае корпоративного пользователя принцип раздельного хранения информации должен реализовываться еще жестче: как минимум одна из копий должна храниться в отдельном месте, чтобы не потерять корпоративную информацию в случае непредвиденных обстоятельств. Создавать резервные копии можно на USB-накопителях, внешних жестких USB дисках, компакт-дисках.

1. ПРИНЦИПЫ РЕЗЕРВНОГО КОПИРОВАНИЯ

Резервное копирование обычно осуществляется в соответствии с одним из трех основных методов: полным, инкрементальным и дифференциальным.

При использовании полного резервирования каждый раз производится копирование всего набора данных. Например, копируется целиком файловая система, база данных или указанный каталог на диске. Данный метод занимает много времени при записи и ведет к большому расходу резервных носителей. С другой стороны, в этом случае восстановление информации осуществляется быстрее, чем при любом другом методе, поскольку резервная копия соответствует текущему состоянию всего набора данных (с учетом периодичности копирования). Полное копирование является наиболее привлекательным решением при резервном копировании системной информации и служит отправной точкой для других методов.

Дифференциальное резервное копирование помогает уменьшить размер последующих копий, делая их на основе дифференциального сравнения исходных файлов с файлами из последней резервной копии. Все добавленные или измененные файлы копируются в отдельный архив, рядом с полной копией. Важно понимать, что дифференциальные резервные копии являются накопительными. Каждое дифференциальное резервное копирование сохраняет в бэкап все, что отличается с момента последнего полного копирования, даже если эти файлы уже были включены в предыдущей дифференциальной копии. Тем не менее, даже с этим ограничением, дифференциальные бэкапы создаются гораздо быстрее и занимают меньше места, чем при использовании метода полного резервного копирования. Поэтому данный метод хорошо подходит для ежедневных или более частых регулярных заданий резервного копирования.

Инкрементальный (или добавочный) метод основан на последовательном частичном обновлении резервной копии. На первом этапе создается полная копия набора данных. Последующие сеансы резервного

копирования разделяются на два вида: частичное копирование и полное. При очередном частичном копировании на резервный носитель помещаются только файлы, которые были модифицированы по сравнению с предыдущей частичной копией. Модифицированными считаются файлы, у которых изменились содержание, атрибуты или права доступа. По истечении периода времени, заданного пользователем (или системным администратором) вновь создается полная копия, и затем цикл повторяется. Данный метод является самым быстрым с точки зрения создания промежуточных копий и ведет к минимальному расходу резервных носителей.

Однако процедура восстановления занимает много времени: информацию сначала требуется восстановить с полной копии, а затем последовательно со всех частичных (инкрементальных) копий. Тем не менее, это самый популярный метод резервного копирования

2. ТОПОЛОГИЯ РЕЗЕРВНОГО КОПИРОВАНИЯ

2.1 Децентрализованная схема резервного копирования данных

Ядром этой схемы является некий общий сетевой ресурс (см. рис. 1). Например, общая папка или FTP-сервер. Необходим и набор программ для резервного копирования, время от времени выгружающих информацию с серверов и рабочих станций, а также других объектов сети (например, конфигурационные файлы с маршрутизаторов) на этот ресурс. Данные программы установлены на каждом сервере и работают независимо друг от друга. Несомненным плюсом является простота реализации этой схемы и ее дешевизна. В качестве программ копирования подойдут штатные средства, встроенные в операционную систему, или программное обеспечение, такое как СУБД. Например, это может быть программа `ntbackup` для семейства Windows, программа `tar` для UNIX-like операционных систем или набор скриптов, содержащих встроенные команды SQL-сервера для выгрузки баз данных в файлы резервных копий. Еще одним плюсом является возможность использования различных программ и систем, лишь бы все они могли получить доступ к целевому ресурсу для хранения резервных копий.

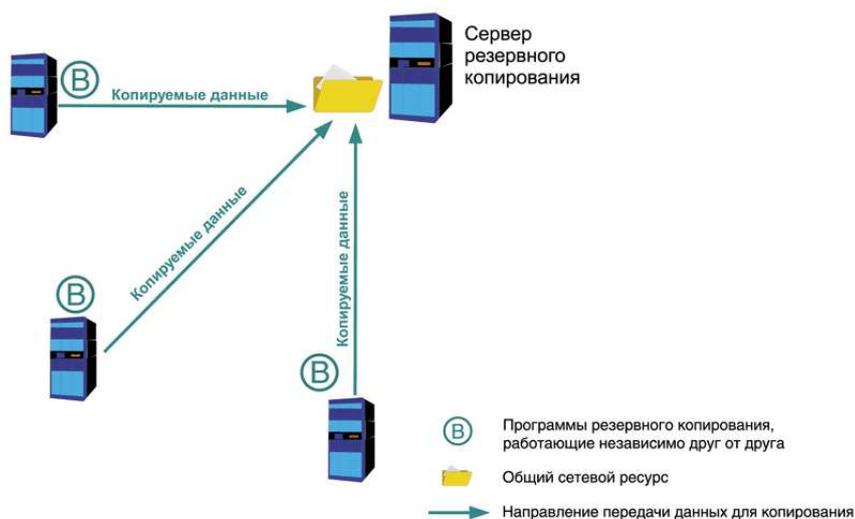


Рисунок 1. Децентрализованная схема резервного копирования

Минусом является неповоротливость этой схемы. Так как программы установлены независимо друг от друга, то и настраивать приходится каждую по отдельности. Довольно тяжело учитывать особенности расписания и распределять временные интервалы, чтобы избежать конкуренции за целевой ресурс. Мониторинг также затруднен, процесс копирования с каждого сервера приходится отслеживать отдельно от других, что в свою очередь может привести к высоким трудозатратам.

Поэтому данная схема применяется в небольших сетях, а также в ситуации, когда невозможно организовать централизованную схему резервного копирования имеющимися средствами.

2.2 Централизованная схема резервного копирования данных

В отличие от предыдущей схемы в этом случае используется четкая иерархическая модель, работающая по принципу «клиент-сервер». В классическом варианте на каждый компьютер устанавливаются специальные программы-агенты, а на центральный сервер – серверный модуль программного пакета. Эти системы также имеют специализированную консоль управления серверной частью. Схема управления выглядит следующим образом: с консоли создаем задания для копирования, восстановления, сбора информации о системе, диагностики и так далее, а сервер дает агентам необходимые инструкции для выполнения указанных операций.

Именно по такому принципу работает большинство популярных систем резервного копирования, таких как Symantec Backup Exec, CA Bright Storge ARCserve Backup, Bacula и другие.

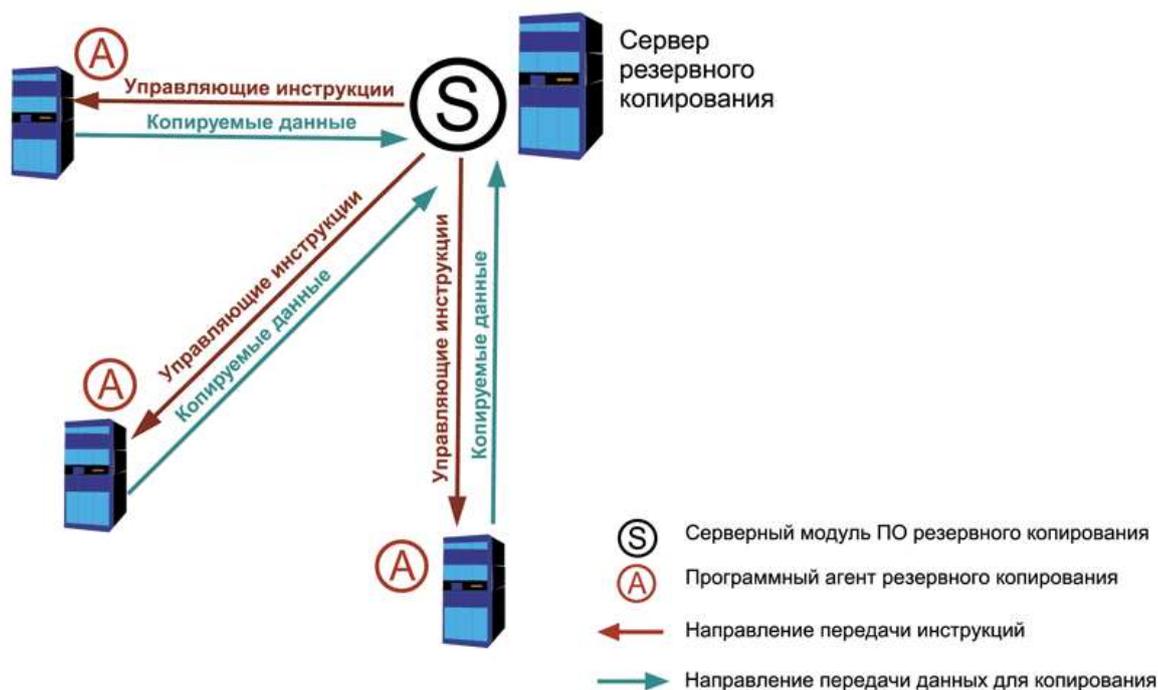


Рисунок 2. Централизованная схема резервного копирования

Помимо различных агентов для большинства операционных систем существуют разработки для резервного копирования популярных баз данных и корпоративных систем, например, для MS SQL Server, MS Exchange, Oracle Database и так далее.

Для совсем небольших компаний в некоторых случаях можно попробовать упрощенный вариант централизованной схемы резервного копирования без применения программ-агентов. Также эта схема может быть задействована, если не реализован специальный агент для используемого ПО резервного копирования. Вместо этого серверный модуль будет использовать уже существующие службы и сервисы. Например, «выгребать» данные из скрытых общих папок на Windows-серверах или копировать файлы по протоколу SSH с серверов под управлением UNIX-систем. Данная схема имеет весьма существенные ограничения, связанные с проблемами сохранения файлов, открытых для записи. В результате подобных действий открытые файлы будут либо пропущены и не попадут в резервную копию, либо скопированы с ошибками. Существуют различные методы обхода

данной проблемы, например, повторный запуск задания с целью скопировать только ранее открытые файлы, но нет ни одного надежного. Поэтому такая схема подходит для применения только в определенных ситуациях.

Например, в небольших организациях, работающих в режиме 5x8, с дисциплинированными сотрудниками, которые сохраняют изменения и закрывают файлы перед уходом домой. Для организации такой усеченной централизованной схемы, работающей исключительно в среде Windows, неплохо подходит ntbackup. При необходимости можно использовать подобную схему в гетерогенных средах или исключительно среди UNIX-компьютеров.

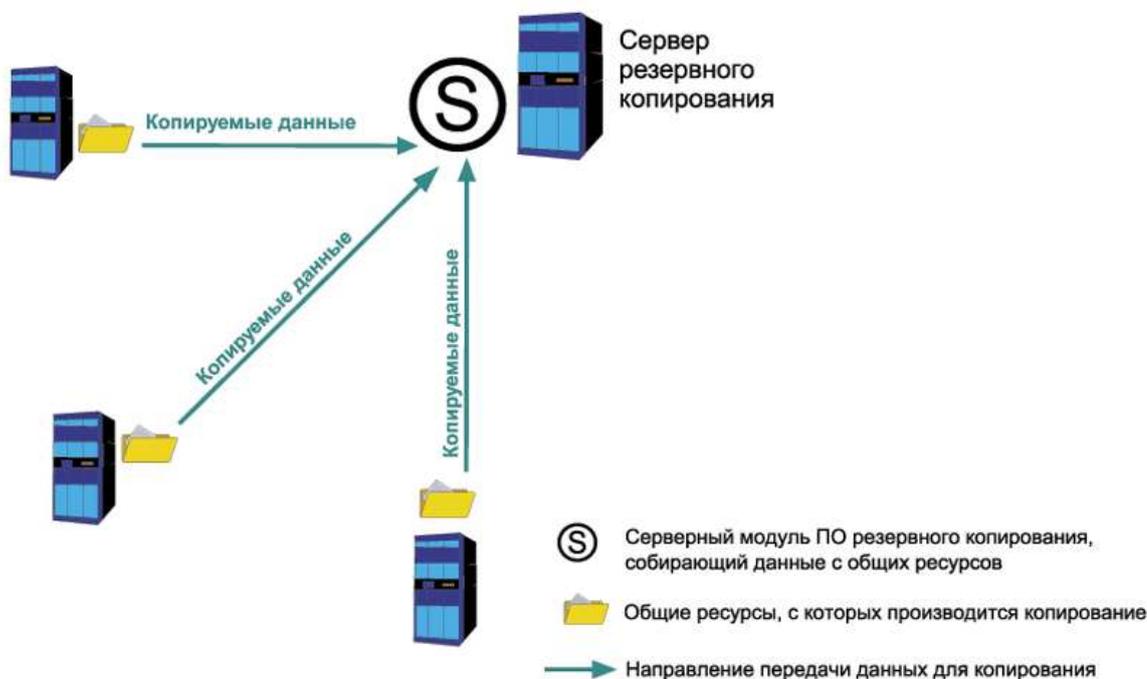


Рисунок 3. Упрощенная централизованная схема резервного копирования

2.3 Смешанная схема резервного копирования данных

Иногда организуют смешанную схему резервного копирования. Например, с серверов, для которых есть в наличии программы-агенты резервного копирования, данные собираются посредством этих агентов. Для всех остальных ресурсов используется децентрализованная схема, то есть

когда локальные программы складывают копии данных на некий общий ресурс сервера с установленным агентом, и далее посредством этого агента информация заносится в общее хранилище резервных копий.



Рисунок 4. Смешанная схема резервного копирования

3. ПРОГРАММЫ ДЛЯ РЕЗЕРВНОГО КОПИРОВАНИЯ

3.1 Acronis True Image

Одна из самых мощных и популярных утилит, пользующаяся заслуженным успехом и доверием многих юзеров, хоть и относится к программам начального уровня. Тем не менее, возможностей у нее хватает.

После запуска приложения пользователь попадает в основное меню, где можно выбрать несколько вариантов действий. В данном случае нас интересует раздел создания резервной копии и восстановления (в меню есть еще дополнительные утилиты, которые сейчас по понятным причинам рассматриваться не будут). После входа активируется "Мастер", который и поможет создать бэкап. В процессе можно выбрать, копию чего именно нужно создать (система для восстановления «с нуля», файлы, настройки и т. д.). В "Типе копирования" лучше выбирать "Инкрементное", поскольку оно поможет сэкономить место. Если объем носителя достаточно велик, можно использовать полное копирование, а для создания нескольких копий – разностное. При создании копии системы будет предложено сделать загрузочный диск.

Вот что интересно: утилита показывает достаточно высокие показатели по скорости создания бэкап-копии, времени, сжатию. Так, например, на сжатие данных порядка 20 Гб понадобится в среднем 8-9 минут, а размер конечной копии составит чуть более 8 Гб.

3.2 Backup4all

Бесплатная утилита, позволяющая, так сказать, одним махом сделать резервные копии для всего, что может понадобиться в дальнейшем одновременно.

Эта утилита интересна тем, что позволяет сохранять копии не только на внешних или внутренних носителях, но и в сетях, или даже на FTP-серверах. Здесь имеется достаточно много редактируемых параметров и настроек, среди которых можно выделить четыре метода копирования, а

также поддержку файловой системы UDF. Кроме того, интерфейс очень прост, а отображение папок и заданий представлено в виде древовидной структуры по типу "Проводника". Также пользователь может разделять копируемые данные по категориям вроде документов, рисунков и т. д., присваивать каждому проекту собственный ярлык. Естественно, имеется и "Планировщик задач", в котором можно указать, например, создание копий исключительно в момент низкой нагрузки на процессор.

3.3 Comodo BackUp

Утилита, способная конкурировать даже с коммерческими продуктами. Ее главной особенностью является наличие целых пяти режимов работы и огромное количество настроек.

Утилита способна реагировать на изменения в файлах, входящих в состав бэкапа, в режиме реального времени. Как только исходный файл изменяется и сохраняется, приложение тут же создает его копию, добавляя и замещая конечный элемент в бэкапе. Не говоря о планировщике, отдельно можно отметить старт создания копий либо в момент старта, либо при выходе.

3.4 Symantec Backup Exec

Резервное копирование данных служит гарантией их безопасности, а возможности быстрого и простого восстановления любой информации заставляет задуматься о выборе соответствующего надежного инструментария для эффективного решения этих задач. Компанией Symantec разработан уникальный продукт - Backup Exec 2012, ставший одним из признанных лидеров среди подобных разработок. Symantec Backup Exec 2012 - единое унифицированное решение для резервного копирования и восстановления данных, позволяющее компаниям существенно снизить затраты на их хранение, грамотно выстроив процедуры создания резервных копий. Symantec Backup Exec 2012 прекрасно подойдет как средство, обеспечивающее постоянную защиту данных для Microsoft SharePoint,

Microsoft Exchange, Microsoft SQL, Active Directory, файловых серверов, настольных компьютеров и ноутбуков. Благодаря интегрированным технологиям дедупликации и архивирования упрощается управление процессами резервного копирования данных и расширяются возможности их моментального восстановления. Symantec Backup Exec 2012 значительно сокращает время простоев в работе системы, обеспечивая высокий уровень защиты данных в физической и виртуальной среде. Symantec Backup Exec 2012 особенно оптимален для компаний с быстрорастущим объемом данных, работающих на Windows.

4. АППАРАТНЫЕ КОМПЛЕКСЫ ДЛЯ РЕЗЕРВНОГО КОПИРОВАНИЯ

При унификации и консолидации инфраструктуры резервного копирования и восстановления данных решение большинства задач существенно облегчается; внедрение аппаратно-программных комплексов сопряжено с минимумом рисков — самодостаточное решение можно построить параллельно с уже имеющимся и провести миграцию, исключая риски, связанные с потерей старых резервных копий. С их использованием возможен быстрый старт — первые задания по резервному копированию могут быть запущены через несколько часов после включения устройства. Следует учесть и невысокую зависимость аппаратно-программных комплексов от персонала — наличие одной точки входа по вопросам технической поддержки уменьшает требования к квалификации и численности специалистов, обслуживающих такой комплекс. Например, вместо администратора операционной системы, специалиста по системам хранения и библиотекам, а также специалиста по резервному копированию в штате компании достаточно иметь одного эксперта. Использование встроенных в большинство комплексов алгоритмов дедупликации позволит уменьшить объемы физически хранимых данных, а также повысить скорость операций по резервированию и восстановлению данных.

Аналитики IDC обычно разделяют готовые решения для резервного копирования (Purpose Built Backup Appliance, PBBA) на два типа: целевое устройство резервного копирования (Target PBBA), предназначенное исключительно для хранения резервных копий и требующее дополнительных компонентов инфраструктуры, например ПО резервного копирования, сервер управления и т.п.; интегрированное устройство резервного копирования (Integrated PBBA), представляющее собой законченное решение, включающее устройство для хранения и программные инструменты управления функциями резервного копирования и восстановления.

Производители предлагают разные подходы к построению аппаратно-программных комплексов резервного копирования и восстановления. Так, семейство EMC DataDomain представляет собой целевое устройство, требующее выстраивания дополнительных элементов инфраструктуры для получения полноценной системы резервного копирования и восстановления данных, но зато позволяющее работать с ПО резервного копирования от различных поставщиков. Компания Symantec предлагает интегрированные устройства — например, NetBackup Appliance 5230, сочетающее в себе ПО для резервного копирования и восстановления с масштабируемым хранением и функцией сквозной дедупликации.

Symantec NetBackup Appliance (NBU) построен на базе модулей 2U (два шестиядерных процессора Intel E5-2620, память до 14 Тбайт, диски полезной емкости до 14 Тбайт с возможностью расширения до 36 Тбайт). Управление NetBackup Appliance осуществляется средствами специализированной ОС (ядро SUSE Linux в фиксированной, безопасной конфигурации, специально доработанное с учетом оптимизации производительности и задач ввода-вывода).

Защита данных реализована средствами RAID6, а управление представлением дисковых ресурсов осуществляется при помощи решения Symantec Storage Foundation. Атаки злоумышленников отражает система обнаружения и защиты от вторжений на базе Symantec Critical System Protection. Управление функциями создания резервных копий реализуется при помощи ПО Symantec NetBackup, которое может быть сконфигурировано как в роли сервера передачи данных (media server), так и в роли управляющего сервера инфраструктуры резервного копирования и восстановления данных (master server). Symantec NBU преднастроено с аппаратным обеспечением, что позволяет оптимально задействовать каналы глобальной сети при передаче трафика, несущего резервную копию на другую площадку (технология Auto Image Replication автоматизации создания копий между несколькими доменами NetBackup или площадками).

В Symantec NBU также присутствует встроенная интеграция с VMware vStorage API для защиты данных, позволяющая сразу («из коробки») работать с окружениями, построенными на ПО от VMware. Наконец, все компоненты связаны общим интерфейсом управления, предлагающим единый подход к установке программных обновлений, что означает отсутствие необходимости в «заплатах», отдельно устанавливаемых на ОС, NetBackup и т. д.

Создание системы резервного копирования и восстановления данных с нуля. Для создания инфраструктуры резервного копирования с нуля достаточно одного устройства NetBackup Appliance, играющего роль управляющего сервера, сервера передачи данных и устройства хранения. В решении имеются интерфейсы Ethernet и FC-AL, что позволяет настроить резервное копирование как с использованием локальной сети, так и без нее. Данный сценарий интересен небольшим организациям и удаленным филиалам.

Использование в качестве строительного блока системы резервного копирования и восстановления данных. В крупных организациях, которым необходимо быстро нарастить инфраструктуру резервного копирования, готовые интегрированные решения могут выступать в качестве строительных блоков, способных штатными средствами без дополнительного кластерного ПО осуществлять балансировку нагрузки и поддержку отказоустойчивости.

5. ПОПУЛЯРНЫЙ МЕТОД РЕЗЕРВНОГО КОПИРОВАНИЯ НА КОНКРЕТНОМ ПРИМЕРЕ

| Тип организации | Штат сотрудников | Кол-во единиц техники | Средний объем накопителя на единицу техники |
|-----------------|------------------|--|---|
| государственная | 400 чел. | 480 ПК, 6 серверов, из них 4-для хранения данных | 250 Гб |

В данном случае более выгодным является инкрементное копирование, так как средние размеры накопителей единиц техники не позволяют делать резервные копии большего размера. Резервное копирование следует выполнять каждую неделю (например, каждую пятницу).

ЗАКЛЮЧЕНИЕ

Резервное копирование — это процесс формирования резервных копий. На сегодня сформировано несколько технологий резервного копирования, которые используются в зависимости от определенной ситуации. Полное резервное копирование выступает в качестве главного и основополагающего метода формирования резервных копий. При методе инкрементного копирования происходит копирование не всех данных (файлы, сектора и так далее), а только тех, которые были модифицированы с момента последнего копирования. Дифференциальное резервное копирование предполагает копирование данных с последнего момента выполнения полного бэкапа. Данные при этом помещаются в архив «нарастающим итогом». Современные системы резервного копирования реализуются как программно, так и аппаратно, а также в сочетании программных и аппаратных компонентов. Резервное копирование рассматривается как важный процесс в жизни любой ИТ-структуры. В то же время резервное копирование применяется для формирования своего рода исторического архива бизнес-деятельности предприятия на протяжении определенного периода ее жизни. В процессе организации резервного копирования преследуются две главные задачи: восстановление инфраструктуры при сбоях и ведение архива данных для будущего обеспечения доступа к информации за прошлые периоды. При выборе систем резервного копирования выставляется ряд требований к характеристикам процессов резервирования и хранения, которые описываются в контракте с поставщиком. Степень защиты предприятий своих данных обычно определяется тем, насколько важна для нее эта информация, а также от финансовых возможностей компаний. Практически в каждой организации ежегодно требования к хранению данных растут огромными темпами.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Бережной А. Оптимизируем работу MS SQL Server. //Системный администратор, №1, 2008 г. – С. 14-22

Бережной А. Организуем систему резервного копирования для малого и среднего офиса. //Системный администратор, №6, 2009 г. – С. 14-23

Маркелов А. Linux на страже Windows. Обзор и установка системы резервного копирования BackupPC. //Системный администратор, №9, 2004 г. – С. 2-6