ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ

ВОРОНЕЖСКОЙ ОБЛАСТИ

государственное бюджетное профессиональное образовательное учреждение Воронежской области
«Воронежский государственный промышленно-гуманитарный колледж»
(ГБПОУ ВО «ВГПГК»)

Методические рекомендации
по выполнению практических заданий
по МДК.04.01 Организация администрирования информационных систем
«ПМ.04 Эксплуатация и поддержка функционирования информационных систем»

Для студентов с инвалидностью по специальности 09.02.04 «Информационные системы»,
очной формы обучения

Часть 7

Воронеж

ББК 32.81.26-04.15
Е47

Печатается по решению методического совета
Воронежского государственного
промышленно-гуманитарного колледжа

Составители: Е. Н Рысцова, А.А. Руднева, А.Е.Овсянникова.

Е
47 **«МДК.04.01 Организация администрирования информационных систем «ПМ.04 Эксплуатация и поддержка функционирования информационных систем»: Методическое пособие по выполнению практических заданий** для студентов с инвалидностью по специальности 09.02.04 «Информационные системы» оч. формы обучения в 8-х частях / департамент образования, науки и молодеж. политики Воронеж. обл., Воронеж. гос. пром.-гуманитар. колледж ; [сост. Е. Н Рысцова, А.А. Руднева, А.Е.Овсянникова]. – Воронеж: ВГПГК, 2021. 17–с.

Изложены цели и задачи изучения МДК04.01; основные требования к практической работы; порядок выполнения, проверки и оценки; список основной и дополнительной рекомендуемой литературы.

ББК 32.81.26-04.15

Содержание

Практическая работа № 14

Тема: АРХИВАЦИЯ ДАННЫХ

ЦЕЛЬ РАБОТЫ: изучение основ архивации данных на локальных или удаленных системах

ЗАДАЧИ РАБОТЫ

1. Изучить типы и методы резервного копирования данных на локальных или удаленных системах Windows Server.
2. Освоить методы восстановления из архивов поврежденных и потерянных данных.

ПЕРЕЧЕНЬ ОБЕСПЕЧИВАЮЩИХ СРЕДСТВ

1. ПК.
2. Программное обеспечение: Oracle VirtualBox, ОС Windows Server.
3. Учебно-методическая литература.

ОБЩИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Для создания архивов данных на локальных или удаленных системах в Windows Server включена программа «Архивация (Backup)». Она годится для архивирования файлов и папок. Для их восстановления из архивов, для доступа к архивным накопителям, для доступа к удаленным ресурсам из окна «Сетевое окружение (My Network Places)», создания образа состояния системы для последующей архивации и восстановления, планирования архивации с помощью «Планировщика заданий (Task Scheduler)» и создания аварийного диска.

Для выполнения архивации и восстановления данных, потребуются необходимые права и полномочия. Члены групп «Администраторы (Administrators)» и «Операторы архива (BackupOperators)» могут архивировать и восстанавливать файлы любого типа независимо от того, кто владеет файлом и какие файлу назначены разрешения. Кроме того, файл в праве архивировать его владельцы и те, у кого есть разрешения: «Чтение (Read)», «Чтение и выполнение (Read and Execute)», «Изменить (Modify)» или «Полный доступ (Full Control)» для этого файла.

Локальным учетным записям доступна только локальная система, а доменные имеют более высокие полномочия. Поэтому члены локальной группы администраторов могут работать только с файлами на локальной системе, а члены группы администраторов домена — с файлами во всем домене.

Программа Архивация (Backup) предоставляет расширения для работы с особыми типами данных:

- данные состояния системы — важные системные файлы, необходимые для восстановления работоспособности локальной системы;
- данные Exchange Server — файлы данных и хранилища информации Exchange. Нужно сохранить эти данные для восстановления работы Exchange Server. Этот тип данных предоставляют только системы с Exchange Server;
- данные о съемных ЗУ, которые располагаются в папке

%SystemRoot%\System32\NtmsdaLa. Если вы их сохраните, то сможете воспользоваться расширенными возможностями программы «Архивация (Backup)» для восстановления конфигурации съемных ЗУ;

- данные удаленных хранилищ хранятся в папке %System-Root%\System32\Retnotestorage. При восстановлении просто скопируйте данные удаленного хранилища обратно в эту папку.

Резервное копирование делится на несколько типов: обычный тип, разностный, добавочный, копирующий и ежедневный *Обычный.* При выполнении данного типа архивируются все файлы, отмеченные для архивации, при этом у всех за архивированных файлов очищается атрибут «Файл готов для архивирования». Данный вид архивирования необходим для создания еженедельных полных резервных копий каких-либо больших файловых ресурсов. Если в компании или организации имеются достаточные ресурсы, то можно ежедневно осуществлять полное архивирование данных.

Разностный. При выполнении данного архивирования из файлов, отмеченных для архивирования, архивирует только те, у которых установлен атрибут «Файл готов для архивирования», при этом данный атрибут не очищается.

Использование «*Обычного»* и «*Разностного»* архивирования позволяет сэкономить пространство на носителях с резервными копиями и ускорить процесс создания ежедневных копий.

Добавочный. При выполнении данного архивирования из файлов, отмеченных для архивирования, архивирует только те, у которых установлен атрибут «Файл готов для архивирования», при этом данный атрибут очищается.

Копирующий. При таком типе архивируются все отмеченные файлы, при этом атрибут «Файл готов для архивирования» остается без изменений.

Ежедневный. Ежедневный тип архивирования создает резервные копии только тех файлов, которые были модифицирования в день создания резервной копии.

Два последних типа не используются для создания регулярных резервных копий. Их удобно применять в тех случаях, когда с какой-либо целью нужно сделать копию файловых ресурсов, но при этом нельзя нарушать настроенные регулярные процедуры архивирования.

ЗАДАНИЕ

1. Создать архив данных при помощи мастера архивации.
2. Выполнить архивацию u1092 файлов без помощи мастера архивации.
3. Выполнить архивирование Active Directory.
4. Выполнить восстановление данных с помощью мастера.
5. Выполнить восстановление данных без помощи мастера.
6. Выполнить восстановление Active Directory.
7. Просмотреть журналы архивации.

ТРЕБОВАНИЯ К ЗАЧЕТУ

1. К зачету необходимо предоставить результаты выполненной работы.
2. Отчет с подробным описанием выполненных работ.

3. Подготовить ответы на вопросы.

ТЕХНОЛОГИЯ ВЫПОЛНЕНИЯ РАБОТЫ

Создание архива данных при помощи мастера архивации

Для создания архива необходимо запустить утилиту «Архивация данных».

1. Выполнить команду «Пуск» - «Выполнить».

2. В появившемся окне ввести команду «ntbackup» для загрузки мастера архивации или восстановления.

3. В появившемся окне мастера снять флажок «Всегда запускать в режиме мастера», а затем щелкнуть гиперссылку «Расширенный режим» для появления главного интерфейса программы архивации (рис.14.1).

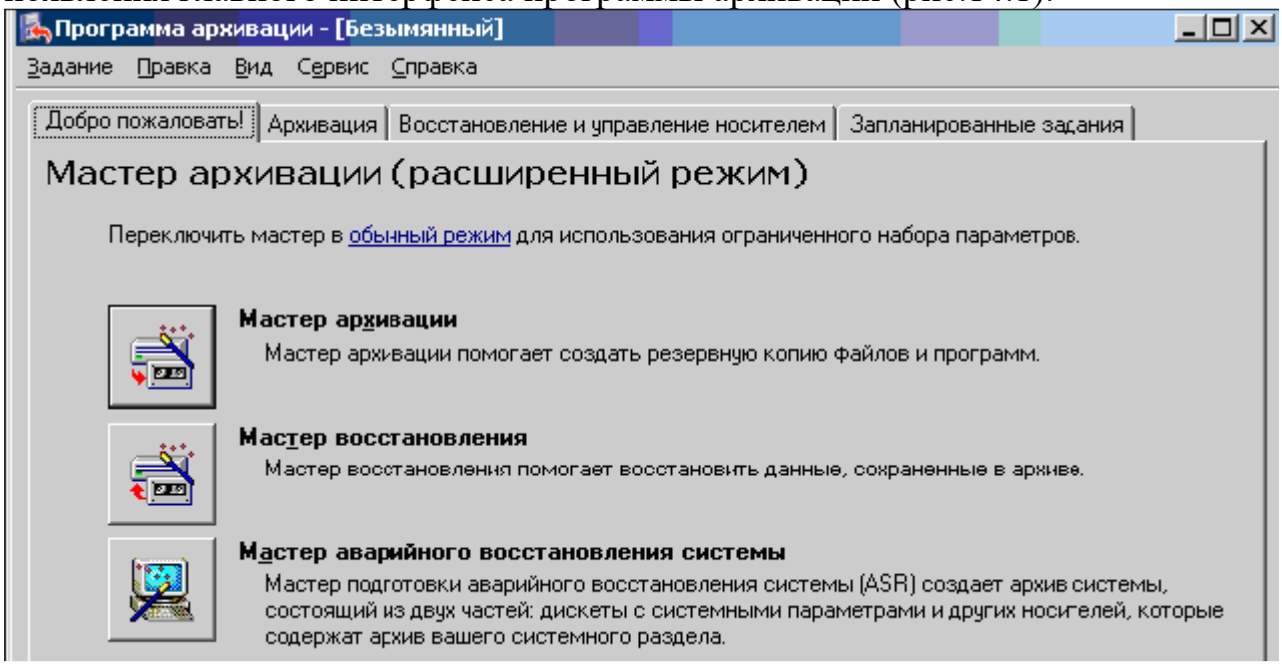

Рис. 14.1 Утилита «Архивация»

4. Запустить «Мастер архивации».

5. В появившемся диалоговом окне отметить пункт «Архивировать Выбранные файлы, диски или сетевые данные» и нажать кнопку «Далее».

6. В диалоговом окне «Элементы для архивации» выбрать папку «C:\Doc» и перейти на следующий пункт.

7. Указать путь расположения архива в папку «Мои документы».

8. В окне «Завершение мастера архивации» нажать кнопку «Дополнительно».

9. Выбрать тип архивации «Копирующий».

10. Отметить пункт «Заменить существующие архивы» и поставить флажок «Разрешить доступ к данным архива и всем добавленным на этот носитель архивам только владельцу и администратору».

11. В окне «Когда архивировать» установить переключатель на пункт «Сейчас».

12. Завершить работу мастера и приступить к архивации. Архив создан и сохранен в указанной папке.

Архивация файлов без помощи мастера архивации:

1. Запустить программу «Архивация данных» и перейти на вкладку

«Архивация».

2. Выделить данные для архивации.

3. В списке «Носитель архива или имя файла» указать путь и имя файла.

4. Щелкнуть кнопку «Архивировать» для появления диалогового окна «Сведения о задании u1072 архивации».

5. Отметить пункт «Дописывать этот архив к данным носителя» и щелкнуть кнопку «Дополнительно» и настроить дополнительные параметры.

Если вы не хотите выполнить архивацию немедленно, щелкните кнопку Расписание. Когда появится предложение записать текущие параметры архивации, щелкните «Да». Затем введите имя сценария выбора и щелкните «Сохранить». В окне «Параметры запланированного задания» введите имя задания, щелкните «Свойства» и составьте расписание. Пропустите остальные пункты.

Сценарии выбора и журналы архивации сохраняются в папке %UserProfile%\Loca\ Settings\Microsoft\ WindowsN~"\ NTBackup\Data. Сценарии выбора сохраняются с расширением .BKS, а журналы архивации — с расширением .LOG. Вы можете просмотреть содержимое этих файлов в любом стандартном текстовом редакторе.

6. Чтобы начать архивацию немедленно, щелкнуть «Архивировать».

7. По завершении архивации щелкнуть «Закрыть» или «Отчет».

Архивирование Active Directory

Для создания резервной копии состояния системы необходимо в утилите резервного копирования «ntbackup» при создании задания на архивирования отметить галочкой пункт «System State».

Выполнить архивирование самостоятельно любым из предложенных способов.

Восстановление данных с помощью мастера

Для восстановления данных используют «Мастер восстановления» или вкладку «Восстановление». Чтобы восстановить данные с помощью мастера, необходимо выполнить следующие действия:

1. Для начала следует убедиться, что необходимый для работы архивный набор загружен в библиотеку.

2. Запустить утилиту «Архивация данных». Щелкнуть кнопку «Мастер восстановления», а затем — «Далее».

3. Выбрать данные для восстановления. В левой части окна отображаются файлы, организованные в тома, в правом — наборы носителей.

4. Щелкнуть «Далее», затем «Дополнительно», чтобы изменить параметры по умолчанию, в частности место для восстановления «Альтернативное размещение» и путь «C:\temp».

5. Пройти через все окна мастера и щелкнуть «Готово».

6. По завершению восстановления щелкнуть «Закрыть» или «Отчет».

Восстановление данных без помощи мастера

Данные можно восстановить вручную, для этого необходимо выполнить следующие действия:

1. Запустить утилиту «Архивация данных» и перейти на вкладку «Восстановление и управление носителем».

2. Указать данные для восстановления. В левом окне отображаются файлы, организованные в тома. В правом окне показаны наборы носителей. Если набор носителей, с которым вы собирались работать, не отображен, следует щелкнуть правой кнопкой файл в левом окне, выбрать «Каталог», затем ввести имя или путь используемого каталога.

3. В списке «Восстановить файлы в» выбрать место для восстановления.

4. Задать способ восстановления файлов, выбрав в меню «Сервис» команду «Параметры». Щелкнуть «ОК».

5. Щелкнуть кнопку «Восстановить». Появится диалоговое окно «Подтверждение восстановления». На этом этапе можно задать дополнительные параметры восстановления, щелкнув кнопку Дополнительно.

6. При необходимости ввести путь или имя архива.

7. По завершению восстановления щелкнуть «Закрыть» или «Отчет».

Восстановление Active Directory:

1. Выключить сервер контроллера домена.

2. Запустить сервер. В процессе загрузки на этапе выбора ОС нажать F8.

3. Выбрать «Восстановление службы каталогов».

4. После запуска системы восстановить данные состояния системы и другие необходимые файлы с помощью утилиты «Архивация данных».

5. После восстановления данных, но перед перезапуском системы, с помощью инструмента «ntdsutil», пометить объекты как полномочные. Проверить данные Active Directory.

6. Перезапустите сервер. После загрузки сервера данные Active Directory должны реплицироваться по домену.

Просмотр журналов архивации

1. Запустить утилиту «Архивация данных».

2. Работая в расширенном режиме, выбрать в меню «Сервис» команду «Отчет». Откроется диалоговое окно «Отчеты архивации».

3. Выделить журнал и щелкнуть кнопку «Просмотр». Журнал откроется в текстовом редакторе по умолчанию.

4. Чтобы напечатать журнал, выделить его и щелкнуть «Печать». Журнал будет напечатан на принтере по умолчанию.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Какие функциональные возможности имеет программа «Архивация (Backup)» ОС Windows Server 2003?

2. Какие пользователи имеют право архивировать и восстанавливать данные?

3. С какими особыми типами данных программа «Архивация (Backup)» предоставляет расширения для работы?

4. На какие типы делится резервное копирование?

5. Какие методы архивирования позволяют сэкономить пространство на носителях с резервными копиями и ускорить процесс создания ежедневных копий?

6. Какие способы архивирования данных можно использовать при создании резервных копий?

7. Как выполняется восстановление данных?

8. Для чего необходим журнал архивации?

Практическая работа № 15

Тема: СОЗДАНИЕ СКРЫТОГО РАЗДЕЛА

ЦЕЛЬ РАБОТЫ: изучение основ создания скрытого раздела системы

ЗАДАЧИ РАБОТЫ

1. Изучить назначение и принципы создания скрытого раздела системы.

2. Освоить методы создания скрытого раздела с помощью «Acronis True Image Echo Enterise Server with Acronis Universal Restore (Safe version)».

ПЕРЕЧЕНЬ ОБЕСПЕЧИВАЮЩИХ СРЕДСТВ

1. ПК.

2. Программное обеспечение: Oracle VirtualBox, ОС Windows Server 2003.

3. Учебно-методическая литература.

ОБЩИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Скрытый раздел – это недоступная для операционной системы логическая секция диска. Несмотря на это, скрытый раздел может содержать файлы и папки, как любой другой раздел. Как правило, скрытые разделы создаются для хранения конфиденциальной информации или резервных копий данных.

Для создания корпоративной системы резервного копирования данных выпущена локализованная линейка программных продуктов Acronis True Image. В ее состав входит четыре продукта: Acronis True Image Echo Workstation, Echo Server для Windows, Echo Server для Linux и Echo Enterprise Server.

Для резервного копирования информации с персональных или портативных компьютеров, которые входят в состав корпоративной сети, служит продукт Acronis True Image Echo Workstation. С его помощью можно создавать резервные копии отдельных папок и файлов, а также посекторные образы целых разделов жестких дисков. Для корпоративных пользователей второй вариант предпочтительнее, поскольку позволяет восстановить работоспособность компьютера в случае сбоя ОС буквально за несколько минут. Конечно, образы занимают больше места, нежели простые копии, u1086 однако в Acronis True Image Echo Workstation реализовано несколько способов уменьшения требований к свободному пространству. Это сжатие информации, создание инкрементных (каждый образ содержит только те данные, которые изменились с момента последнего копирования) и дифференцированных образов (каждый образ содержит только изменившиеся по сравнению с базовой копией данные).

Создаваемые программой резервные копии надежно защищаются от повреждения или уничтожения. Для этого используется так называемая зона безопасности (Acronis Secure Zone). Она представляет собой скрытый служебный раздел, который можно разместить на локальном жестком диске. Зона безопасности имеет особую файловую систему и потому доступна

только программам компании Acronis. Все остальное ПО, использующее стандартные возможности ОС, считает этот раздел просто неразмеченным пространством и не может работать с сохраненными в нем резервными копиями и образами. Это защищает последние от повреждения вирусами, удаления легитимными пользователями и т. д. Помимо этого резервные копии можно создавать просто в существующих разделах локального жесткого диска, на сетевых дисках, удаленных FTP-серверах, сменных (в том числе и ленточных) носителях.

Для построения серверной системы резервного копирования в линейке продуктов Acronis True Image предназначены сразу три программы. Первые две, Echo Server для Windows и Echo Server для Linux, очень схожи: обе используются для организации резервного копирования корпоративных серверов, только работающих под управлением разных ОС. По функциональности эти продукты практически не различаются, разве что в версии, предназначенной для Linux, отсутствует часть возможностей, которые связаны с реализованными в Windows технологиями: поддержка службы теневого копирования томов, работа с журналом событий и т. п.

ПО Acronis True Image Echo Server напоминает несколько урезанную версию Acronis True Image Echo Workstation, только предназначенную для серверов. С его помощью можно создавать резервные копии отдельных файлов или папок и образы целых разделов локального жесткого диска. Размещаться они могут непосредственно на жестком диске сервера, на сетевых дисках, FTP/SFTP-серверах, на всевозможных сменных накопителях (USB и FireWire, CD и DVD) или накопителях на магнитных лентах. Восстановление информации выполняется как путем запуска программы из под Windows, так и с применением автономной версии (со специально созданного загрузочного диска) или функции «Восстановление при загрузке».

Таким образом, единственное, чем Acronis True Image Echo Server отличается от продукта для рабочих станций, — это поддержка серверных ОС и специальные технологии, которые позволяют резервировать информацию без остановки приложений сервера, например, системы управления базами данных.

Это очень важно, поскольку во многих информационных системах простои серверных служб недопустимы.

Последний продукт рассматриваемой серии, Acronis True Image Echo Enterprise Server, — универсальная система. В комплект его поставки входят компоненты для серверных ОС как семейства Windows, так и Linux. Это позволяет применять его для всех серверов, функционирующих в организации.

По своим основным функциям Acronis True Image Echo Enterprise Server аналогичен Acronis True Image Echo Server, однако в нем реализованы средства централизованного администрирования. В первую очередь это консоль управления и агенты, которые могут устанавливаться на серверах и обеспечивать удаленное администрирование системы резервного

копирования. При этом ответственным сотрудникам доступны все возможности, имеющиеся в Acronis True Image Echo Workstation: групповое управление заданиями, возможность удаленного восстановления информации и т. п.

Таким образом, можно сделать следующий вывод: продукты Acronis True Image Echo Server для Windows и для Linux отвечают потребностям компаний с небольшой ИТ-инфраструктурой, в состав которой входит от одного до трех серверов, установленных в комнате со свободным доступом администратора. В более же серьезных информационных системах предпочтительнее использовать Acronis True Image Echo Enterprise Server.

ЗАДАНИЕ

1. Изучить теоретический материал по данной теме.
2. Создать скрытый раздел.

ТРЕБОВАНИЯ К ЗАЧЕТУ

1. К зачету необходимо предоставить результаты выполненной работы.
2. Отчет с подробным описанием выполненных работ.
3. Подготовить ответы на вопросы.

ТЕХНОЛОГИЯ ВЫПОЛНЕНИЯ РАБОТЫ

Создание скрытого раздела:

1. Подключить образ загрузочного диска «acron.iso».
2. Запустить виртуальную машину.
3. В появившемся диалоговом окне «Выбор варианта загрузки» выбрать пункт «ATIES Echo 9.5.8018 EN with UR».
4. Загрузить «Acronis True Image Echo Enterprise Server with Acronis Universal Restore (Safe version)».
5. В появившемся окне выбрать «Manage Acronis Secure Zone».
6. Следуя требованиям мастера установки нажать «Next» в окне приветствия.
7. В окне «Create Acronis Secure Zone» выбрать диск «C:» и перейти на следующий этап.
8. В окне «Size» оставить все по умолчанию.
9. В окне «Acronis Secure Zone Protection» установить переключатель « Do not use password protection » (не использовать защиту паролем).
10. В окне «Activating Acronis Startup Recovery Manager» установить переключатель « Do not activate Acronis Startup Recovery Manager » (не активировать менеджер восстановления запуска).
11. Завершить создание скрытого раздела, запустив команду «Proceed».
12. Отключить CD/DVD-ROM на виртуальной машине и выполнить перезагрузку.
13. Зарегистрироваться на сервере с правами администратора и проверить наличие скрытого раздела (рис.15.1).

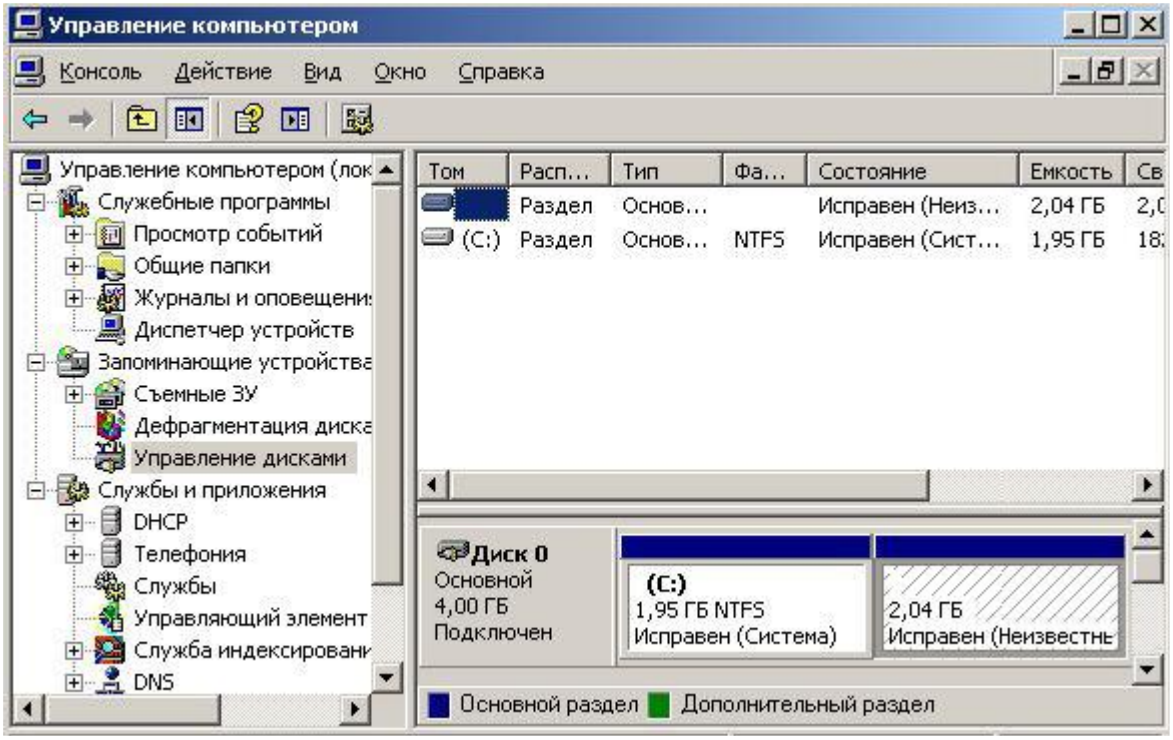

Рис. 15.1 Консоль «Управление компьютером»

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что представляет собой скрытый раздел системы? И для чего он создается?
2. Для чего предназначены программные продукты Acronis True Image?
3. Что такое Acronis Secure Zone?
4. Как создать скрытый раздел?

Практическая работа № 16

Тема: ОБЕСПЕЧЕНИЕ НАДЕЖНОСТИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛОКАЛЬНО-ВЫЧИСЛИТЕЛЬНОЙ СЕТИ (4 часа)

ЦЕЛЬ РАБОТЫ: изучение вопросов обеспечения надежности и информационной безопасности компьютерных сетей.

ЗАДАЧИ РАБОТЫ

1. Изучить требования к надежности и информационной безопасности компьютерной сети предприятия.
2. Изучить принципы организации комплексной защиты информации корпоративной сети.

ПЕРЕЧЕНЬ ОБЕСПЕЧИВАЮЩИХ СРЕДСТВ

1. ПК.
2. Программное обеспечение: Oracle VirtualBox, ОС Windows Server 2003.
3. Учебно-методическая литература.

ОБЩИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Наиболее важными задачами сетевого администрирования являются обеспечение надежности и безопасности.

Надежность – это свойство информационной сети сохранять полную или частичную работоспособность вне зависимости от выхода из строя некоторых её компонентов.

Безопасность – это защищенность информационной среды предприятия от внешних и внутренних угроз её формированию, использованию и развитию.

Для обеспечения надежности и безопасности применяются специальные методы и средства, распределяющиеся по трем основным уровням:

- *на физическом уровне* осуществляется повышение надежности элементов сети, резервирование оборудования, резервное копирование и архивирование данных;
- *на системном уровне* используются программно-аппаратные средства контроля и восстановления работоспособности сети;
- *на административном уровне* производится распределение полномочий пользователей, разрабатываются и реализуются планы действий в чрезвычайных ситуациях и т. п.

Рассмотрим некоторые простые правила обеспечения надежности и защиты информации в локальной сети предприятия.

Самая важная информация, как правило, хранится на серверах, поэтому эти устройства имеют повышенные требования к надежности и безопасности.

В связи с этим, серверные устройства необходимо размещать в отдельном помещении, доступ к которому ограничен. Лучше установить в данном помещении кондиционер для дополнительного охлаждения.

Наилучшим вариантом будет организация отдельного помещения для мини-АТС, серверов и других сетевых устройств. Сервер нужно обязательно опечатать, чтобы быть уверенным в том, что его в ваше отсутствие не разбирали. По возможности отключите дисководы и приводы компакт-дисков в BIOS или путем отсоединения кабелей (это нужно для того, чтобы никто не смог получить доступ к файловой системе с помощью этих носителей данных). Если сервер даст сбой и нужно будет загрузиться с дискеты или компакт диска, их всегда можно будет вернуть в систему.

Точно так же, как и сервер, вам следует опечатать и компьютеры пользователей. Если у клиентов отсутствует необходимость использования съемных носителей, то отключите их приводы от материнской платы, оставив работающими приводы на нескольких компьютерах для того, чтобы там можно было произвести запись, если возникнет потребность. Отключите все неиспользуемые USB, COM и LPT-порты. Установите пароль на BIOS и запретите возможность загрузки компьютера с дискет и компакт-дисков.

Установите антивирусное программное обеспечение.

Если ваша сеть имеет подключение к интернету, следует установить брандмауэр. Брандмауэр— это программа или специальное устройство, которое пропускает через себя весь трафик. Эта программа входит в сеть и выходит из нее с целью фильтрации трафика. В процессе анализа и фильтрации потоков данных, брандмауэр опирается на специально установленные системным администратором правила, блокируя пакеты с данными или же пропуская их.

Чтобы убедиться в том, что брандмауэр работает правильно, нужно использовать сканер безопасности. Сканер анализирует сеть и находит в ней все уязвимые места, обрабатывает полученные результаты и генерирует отчет на их основе. Достаточно часто найденное слабое место может быть устранено без вмешательства администратора.

В систему защиты сети и данных от несанкционированного доступа входят следующие технологии:

– система управления доступом;
– система аудита;
– система аутентификации пользователей;
– аутентификация с использованием смарт-карт;
– политика на ограничение использования программ;
– служба управления правами;
– центр сертификации;
– встроенные средства шифрования;
– шифрующая файловая система EFS;
– поддержка протокола IPSec;
– безопасность беспроводных соединений;
– организация виртуальных частных сетей.
- защита от вирусов, спама и внешних атак.

Использование межсетевых экранов (например, ISA Server 2000) позволяет обеспечивать защиту локальной сети на трех уровнях: сетевом,

транспортном и уровне приложений.

Усиленные политики безопасности рабочих станций Windows XP Professional позволяют предотвратить исполнение нежелательных приложений, в том числе вирусов и «троянских коней».

Управление доступом в Интернет из корпоративной сети позволяет защитить компьютеры от исполнения вредоносного u1082 кода и объектов ActiveX.

Высокая безопасность веб-сервера Internet Information Services (IIS)6.0 , являющегося частью Windows Server 2003, обеспечивает его надежную работу и защиту сервера от атак.

Если данные хранятся в СУБД, то добавляется дополнительный уровень защиты - аутентификация пользователя на уровне самой СУБД. Для управления доступа пользователей к различным объектам баз данных используются полномочия. Они указывают, какие пользователи могут выполнять определенные операции с базой данных. Вы можете задавать полномочия на уровне сервера и на уровне базы данных. Полномочия на уровне сервера используются для того, чтобы администраторы баз данных (DBA) могли выполнять административные задачи для баз данных. Полномочия на уровне базы данных используются для того, чтобы разрешать или запрещать доступ к объектам и операторам базы данных. Полномочия на уровне объектов базы данных – это класс полномочий, которые предоставляются для доступа к объектам базы данных и на использование операторов. Вы можете упростить задачу управления многими полномочиями для многих пользователей путем использования ролей для баз данных. Роли баз данных используются, чтобы предоставлять группам пользователей одни и те же полномочия доступа к базам данных без необходимости присваивания этих полномочий по отдельности.

Вместо присваивания отдельных полномочий отдельным пользователям вы можете создать роль, представляющую полномочия, используемые группой пользователей, и затем присвоить их этой группе.

Обычно роли создаются для определенных рабочих групп, классов работ или задач. При этом подходе новые пользователи могут становиться членами одной или нескольких ролей баз данных, исходя из заданий, которые они будут выполнять.

Необходимо отметить, что наибольшую опасность для информационной безопасности организаций представляют вовсе не внешние угрозы - вирусы, трояны, хакеры и т.п., а внутренние. Внутренние угрозы вызваны тем, что пользователи имеют неконтролируемый доступ к важной информации изнутри - со своих компьютеров, объединенных в локальную сеть. Последствием может быть как несанкционированное копирование или удаление конфиденциальной информации, так и появление на рабочих компьютерах вредоносных программ и просто бесполезных файлов (например, видеофильмов и музыки). Как правило, в таких случаях используются внешние накопители информации (USB-диски, CD и DVD приводы, флоппи-дисководы, устройства Bluetooth и др.)

Существуют программы (например FileControl) для контроля доступа к различным устройствам хранения информации (USB дискам и другим USB устройствам, CD/DVD приводам, флоппи-дисководам, различным портам) и мониторинга операций с файлами внутри локальной сети. Такие программы дистанционно устанавливаются на компьютеры локальной сети, невидимы для пользователей, предельно просты в использовании. Помимо управления доступом, осуществляется мониторинг действий пользователей с внешними накопителям информации (информация о времени подключения/отключения устройств и о том, какие файлы и когда были прочитаны или записаны, сохраняется в лог-файлы).

Возможность осуществлять контроль действий с внешними устройствами и мониторинг операций с файлами по локальной сети - необходимый элемент обеспечения информационной безопасности любой организации, на компьютерах которой хранится ценная информация.

ЗАДАНИЕ

1. Изучить теоретический материал по данной теме.

2. Подготовить проект (план) мероприятий по обеспечению информационной безопасности локально-вычислительной сети предприятия.

ТРЕБОВАНИЯ К ЗАЧЕТУ

4. К зачету необходимо предоставить результаты выполненной работы.

5. Отчет с подробным описанием выполненных работ.

6. Подготовить ответы на вопросы.

ТЕХНОЛОГИЯ ВЫПОЛНЕНИЯ РАБОТЫ

Самостоятельно исследовать возможные угрозы информационной безопасности корпоративной сети. Провести анализ современных программно-аппаратных средств защиты информационной сети предприятия. На основании проведенного исследования разработать интегрированный комплекс программно-технических средств и административных мер по обеспечению u1085 надежной работы сети и безопасности информационных ресурсов организации.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое надежность и безопасность ИС?

2. По каким трем основным уровням распределяются специальные методы и средства обеспечения надежности и информационной безопасности?

3. Какие средства обеспечения защиты информации вы знаете?

4. Что должен включать комплекс программно-технических средств и административных мер по обеспечению надежности и информационной безопасности компьютерной сети предприятия?