Презентация на тему:

Защита данных

Подготовили студентки гр.ЭОП-111

Крейдич Анна и Матькова Лилия

Научный руководитель: Ганак О.Б.

СОДЕРЖАНИЕ

Защита информации - комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности (целостности, доступности и, если нужно, конфиденциальности информации и ресурсов, используемых для ввода, хранения, обработки и передачи данных).

Система называется **безопасной**, если она, используя соответствующие аппаратные и программные средства, управляет доступом к информации так, что только должным образом авторизованные лица или же действующие от их имени процессы получают право читать, писать, создавать и удалять информацию.

Не случайно, что защита данных в компьютерных сетях становится одной из самых острых проблем в современной информатике. На сегодняшний день сформулировано три базовых принципа информационной безопасности, которая должна обеспечивать:

1)**целостность данных** - защиту от сбоев, ведущих к потере информации, а также неавторизованного создания или уничтожения данных;

2)**конфиденциальность** информации и, одновременно,

3)ее **доступность** для всех авторизованных пользователей.


2. Потери информации из -за некорректной работы ПО :
- сбои работы серверов, рабочих станций , сетевых карт и т. д.;
- потеря или изменение данных при ошибках ПО;
3. Потери, связанные с несанкционированным доступом :
- потери при заражении системы компьютерными вирусами;
- несанкционированное копирование , уничтожение или подделка информации ;
1. Сбои оборудования:
- сбои кабельной системы;
- перебои электропитания;
- сбои дисковых систем;
- сбои систем архивации данных;
Потенциальные «угрозы» сети
4. Потери информации, связанные с неправильным хранением архивных данных.
5. Ошибки обслуживающего персонала и пользователей.
- ознакомление с конфиденциальной информацией, составляющей тайну, посторонних лиц;
- случайное уничтожение или изменение данных;

В зависимости от возможных видов нарушений работы сети (под нарушением работы мы также понимаем и несанкционированный доступ) многочисленные виды защиты информации объединяются в три основных класса:

- средства физической защиты, включающие средства защиты кабельной системы, систем электропитания, средства архивации, дисковые массивы и т. д.

- программные средства защиты, в том числе: антивирусные программы, системы разграничения полномочий, программные средства контроля доступа.

- административные меры защиты, включающие контроль доступа в помещения, разработку стратегии безопасности фирмы, планов действий в чрезвычайных ситуациях.

Основные критерии оценки надежности

Безопасность	Гарантированность
Безопасность, являясь активным компонентом защиты (включает в себя анализ возможных угроз и выбор соответствующих мер противодействия), отображает тот набор законов, правил и норм поведения, которым пользуется конкретная организация при обработке, защите и распространении информации. Выбор конкретных механизмов обеспечения безопасности системы производится в соответствии со сформулированной политикой безопасности.	*Гарантированность*, являясь пассивным элементом защиты, отображает меру доверия, которое может быть оказано архитектуре и реализации системы (другими словами, показывает, насколько корректно выбраны механизмы, обеспечивающие безопасность системы).

Необходимо поддерживать два фундаментальных принципа: **проверку полномочий** и **проверку подлинности (аутентификацию)**. Проверка полномочий основана на том, что каждому пользователю или процессу информационной системы соответствует набор действий, которые он может выполнять по отношению к определенным объектам. Проверка подлинности означает достоверное подтверждение того, что пользователь или процесс, пытающийся выполнить санкционированное действие, действительно тот, за кого он себя выдает.

Системы архивирования информации в сетях

Организация надежной и эффективной системы архивации данных является одной из важнейших задач по обеспечению сохранности информации в сети. В небольших сетях, где установлены один-два сервера, чаще всего применяется установка системы архивации непосредственно в свободные слоты серверов. В крупных корпоративных сетях наиболее предпочтительно организовать выделенный специализированный архивационный сервер.

Существуют различные архивационные программы. Вот некоторые из них: WinZip, WinRar, 7Zip, WinAse, PowerArchiver, ZiptFast, UltimateZip, PowerZip, TurboZip, FilZip.

Какой архиватор все же лучший? При архивировании информации трудно со стопроцентной уверенностью сказать, какой из архиваторов в данном случае позволит получить максимальную степень сжатия. Наиболее вероятно, что из тройки лидеров Winace, Winrar и 7Zip лучше справится Winrar.

Защита от компьютерных вирусов

Вряд ли найдется хотя бы один пользователь или администратор сети, который бы ни разу не сталкивался с компьютерными вирусами. По данным исследования, проведенного фирмой Creative Strategies Research, 64% из 451 опрошенного специалиста испытали "на себе" действие вирусов. На сегодняшний день дополнительно к тысячам уже известных вирусов появляется 100-150 новых ежемесячно. Наиболее распространенными методами защиты от вирусов по сей день остаются различные антивирусные программы.

Наиболее популярные из них: **Avast! Free Antivirus, Avira AntiVir Personal, Kaspersky Virus Removal Tool, Dr.Web CureIt, Антивирус NOD32.**

Защита персональных данных в Беларуси

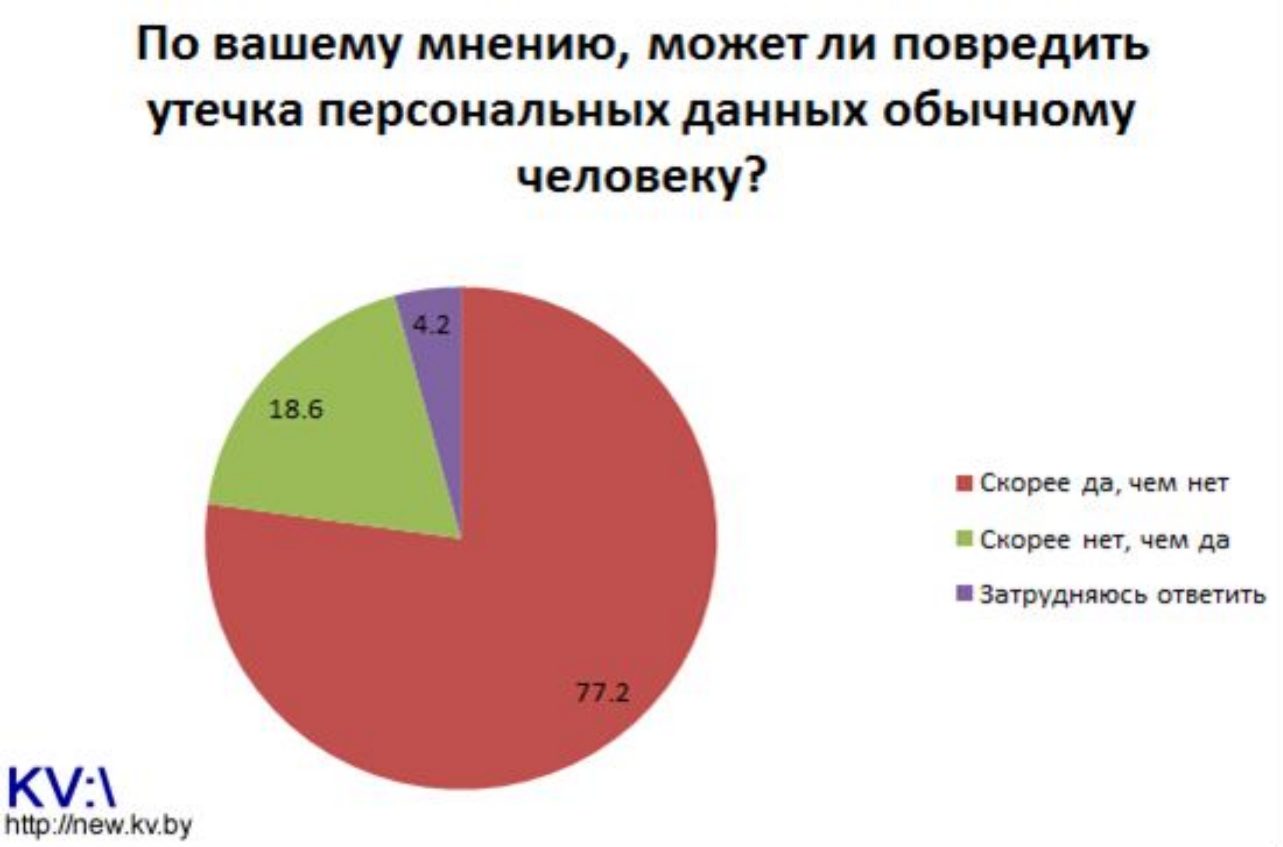
О необходимости защиты персональных данных сегодня не говорит только ленивый. В эпоху всеобщего распространения информационных технологий проблема сохранности подобных данных стала особенно волновать специалистов по безопасности практически всех организаций. К сожалению, приходится констатировать, что белорусские организации пока уделяют недостаточно внимания этому вопросу.

* Персональные данные относятся к сведениям конфиденциального характера, и потому должны защищаться от посторонних глаз. Защита их регламентируется в белорусском законодательстве законом «Об информации, информатизации и защите информации». В частности, именно в 32-й статье этого закона оговаривается необходимость защиты персональных данных:

* «Меры по защите персональных данных от разглашения должны быть приняты с момента, когда персональные данные были предоставлены физическим лицом, к которому они относятся, другому лицу либо когда предоставление персональных данных осуществляется в соответствии с законодательными актами Республики Беларусь.

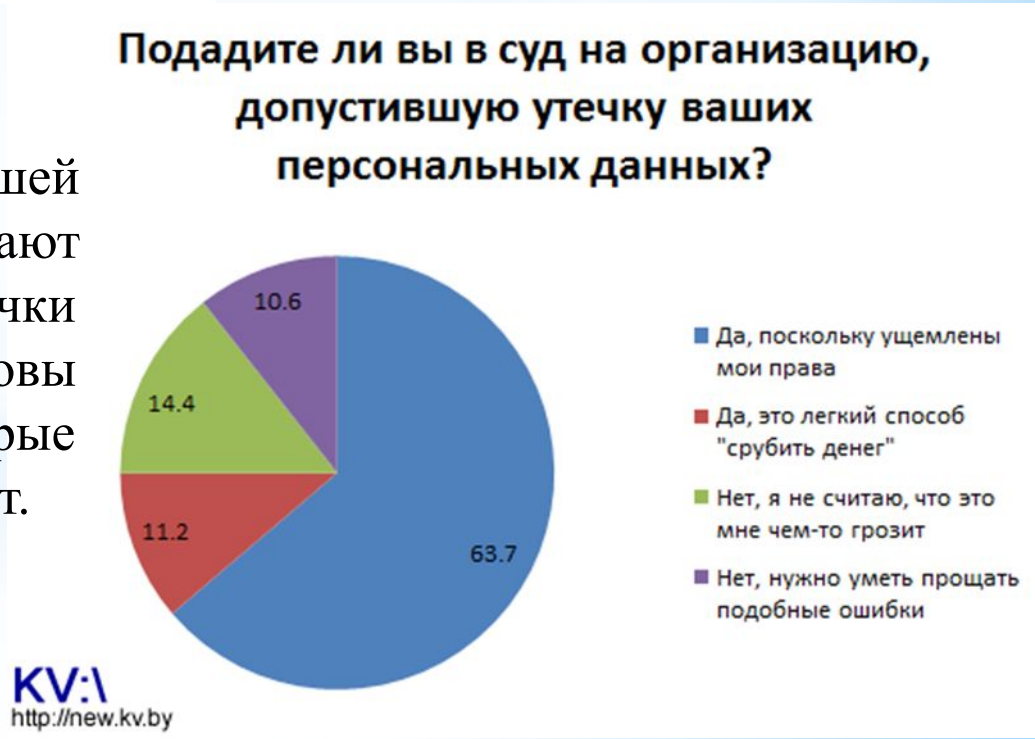
* Последующая передача персональных данных разрешается только с согласия физического лица, к которому они относятся, либо в соответствии с законодательными актами Республики Беларусь. Меры, указанные в части первой настоящей статьи, должны приниматься до уничтожения персональных данных, либо до их обезличивания, либо до получения согласия физического лица, к которому эти данные относятся, на их разглашение».

У большинства белорусов возникает впечатление, что все угрозы, связанные с утечками информации, актуальны только для западных компаний, в то время как государственным и коммерческим организациям, работающим в Беларуси, убытки в результате утечек персональных данных вовсе не грозят. Тем не менее, как показывают исследования, отечественным организациям также не стоит расслабляться и откладывать на потом защиту персональных данных.



Таким образом, не стоит надеяться на то, что утечка персональных данных будет воспринята клиентами и партнерами как что-то само собой разумеющееся.

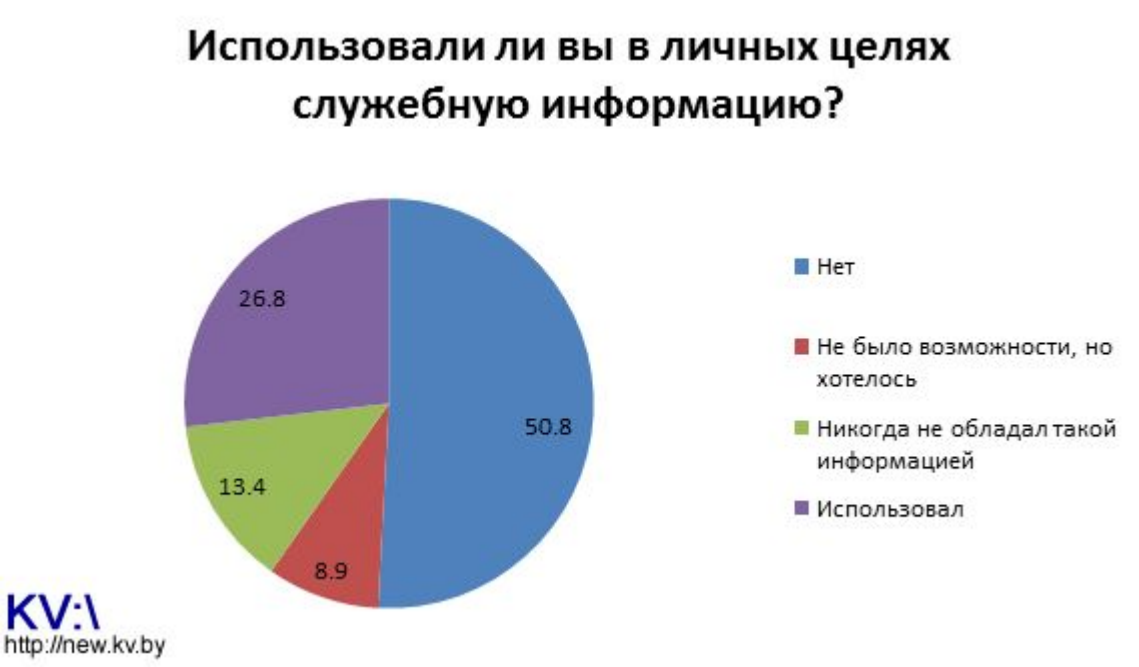
Как показывает опрос, жители нашей страны уже в полной мере осознают угрозы, которые несут в себе утечки персональных данных, а потому готовы бороться за свои права, которые подобного рода инциденты нарушают.



Недостаточная защищенность организаций

Стоит отметить, что это же исследование показало не только заинтересованность участников опроса в защите своих персональных данных от утечек, но также и недостаточную защищенность организаций от утечек информации и, в частности, персональных данных. При этом сотрудники демонстрируют практически единодушную готовность делиться закрытой корпоративной информацией со всеми желающими за вознаграждение, что еще больше усугубляет проблему.

Проблема защиты персональных данных пока что не стоит в Беларуси так остро, как, например, в соседней России, хотя в данном случае это скорее плохо, чем хорошо. Российские организации уже сейчас задумываются о том, как защитить своих клиентов от утечек информации, а себя – от штрафов. Не за горами то время, когда за небрежное отношение с персональными данными клиентов организации будут нести реальную ответственность и в Беларуси. Тогда гораздо дешевле будет предотвратить утечку персональных данных, чем выплачивать штрафы и нести судебные издержки из-за неё.



Нужно сказать, что сами компании, работающие с большим количеством персональных данных – это, в первую очередь, финансово-кредитные учреждения, туристические операторы, операторы мобильной связи и прочие компании – сегодня уже в большинстве своем серьезно занимаются проблемами защиты информации о своих клиентах, поэтому хочется рассказать о некоторых угрозах внутренней информационной безопасности организаций, которые существуют на рынке.

Защита информации от утечек становится все более актуальной по нескольким причинам:

Бизнес становится более мобильным

- Ноутбуки быстро заменяют настольные компьютеры
- В настоящее время они составляют более 68% всех компьютеров

Больше мобильных данных – больше утечек

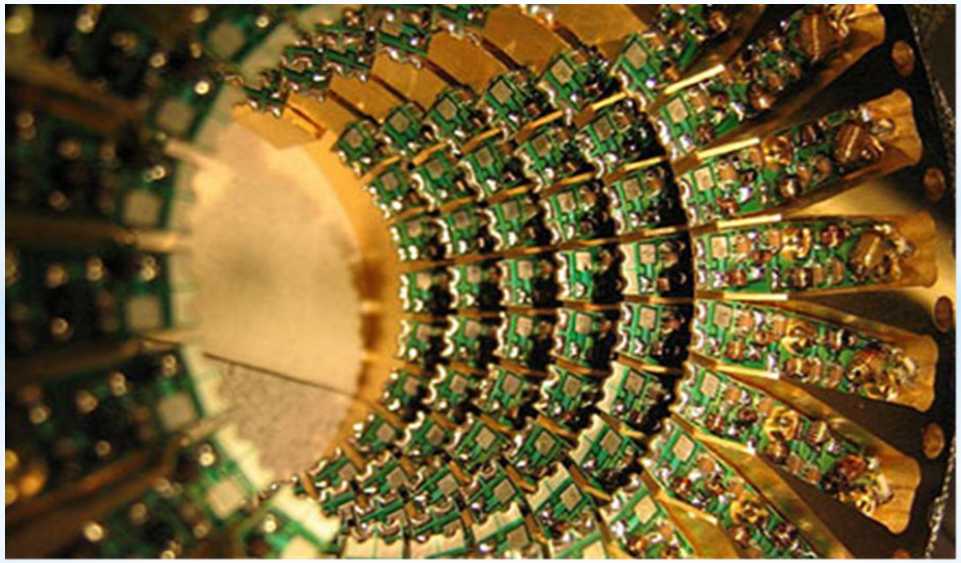
- Пользователи склонны сохранять всё подряд
- Мобильность повышает риск утечки данных

Но, безусловно, в таких случаях существуют и методы защиты. Например, шифрование данных или защита паролем.

Создана «абсолютная» защита данных

В марте 2012 года в Европе впервые была продемонстрирована коммерческая сеть, в которой использовалась квантовая технология шифрования данных. По словам ученых, данную систему невозможно взломать.

Технология квантовой криптографии обеспечивает беспрецедентный на сегодняшний день уровень шифрования данных. На разработку сети ушло 4 года, и в проекте приняли участие 12 европейских стран.



«В основе любого квантового шифрования лежит принцип неопределенности Гейзенберга – то есть вы не сможете взломать систему, не разрушив передаваемые в ней данные, - рассказывают ученые. – Ключевой момент технологии заключается в том, что никто не может взломать систему, не оставшись незамеченным».

Если в основе современных систем безопасности лежат сложные математические вычисления, которые трудно, хотя и можно рассчитать, потратив на это различный период времени, то в квантовой системе взлом осуществить невозможно. В основе этой технологии лежат базовые принципы квантовой механики.

ЗАКЛЮЧЕНИЕ

В заключение хотелось бы подчеркнуть, что никакие аппаратные, программные и любые другие решения не смогут гарантировать абсолютную надежность и безопасность ваших данных. В то же время свести риск потерь к минимуму возможно лишь при комплексном подходе к вопросам безопасности.

Конечно, пока что в нашей стране не было громких утечек персональных данных, приведших к большим неприятностям крупные государственные или коммерческие организации. Но глядя на частоту утечек информации в той же России, сложно предполагать, что так будет продолжаться до бесконечности – рано или поздно гром грянет, и тогда тем, кто окажется в эпицентре бури, придется нелегко. Так что белорусским организациям вряд ли имеет смысл откладывать внедрение системы защиты от утечек информации до лучших времен – вполне может случиться так, что времена из-за этого как раз настанут не самые лучшие.

ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Использование архиватора WinRAR

1. Для запуска архиватора WinRAR выберите в Главном меню Windows команду **Программы ► WinRAR ► WinRAR**. После этого на экране будет раскрыто окно *WinRAR*, как показано на рис. 1.

Рис. 1. Окно *WinRAR* в режиме операций с файлами

Содержание

Вперёд

2. Для получения справочной информации выберите команду ► **Содержание**. В окне *Справка WinRAR:Help* выберите на вкладке **Содержание** раздел **WinRAR Interface**, подраздел **WinRAR menus**, как показано на рис. 2.

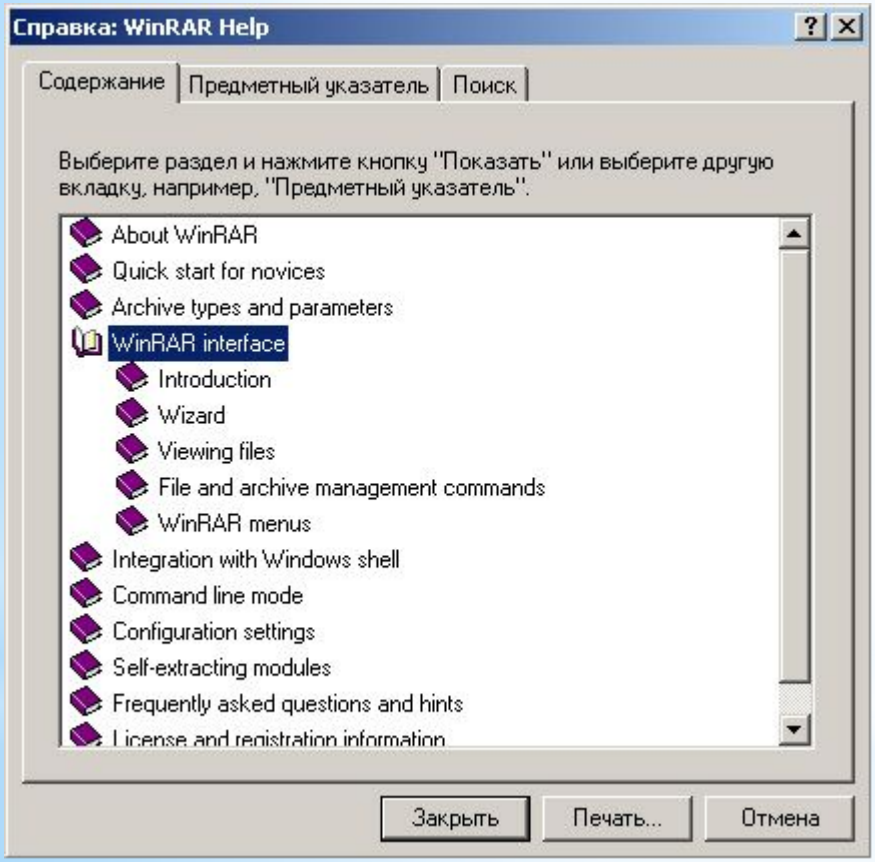


Рис.2 Окно справки WinRAR

3. Создайте архив из нескольких файлов в папке **H:\Home** Для этого выберите в поле списка дисков и папок **H:\Home**, выделите нужные файлы и щелкните кнопку «Добавить» на панели инструментов (рис. 3).

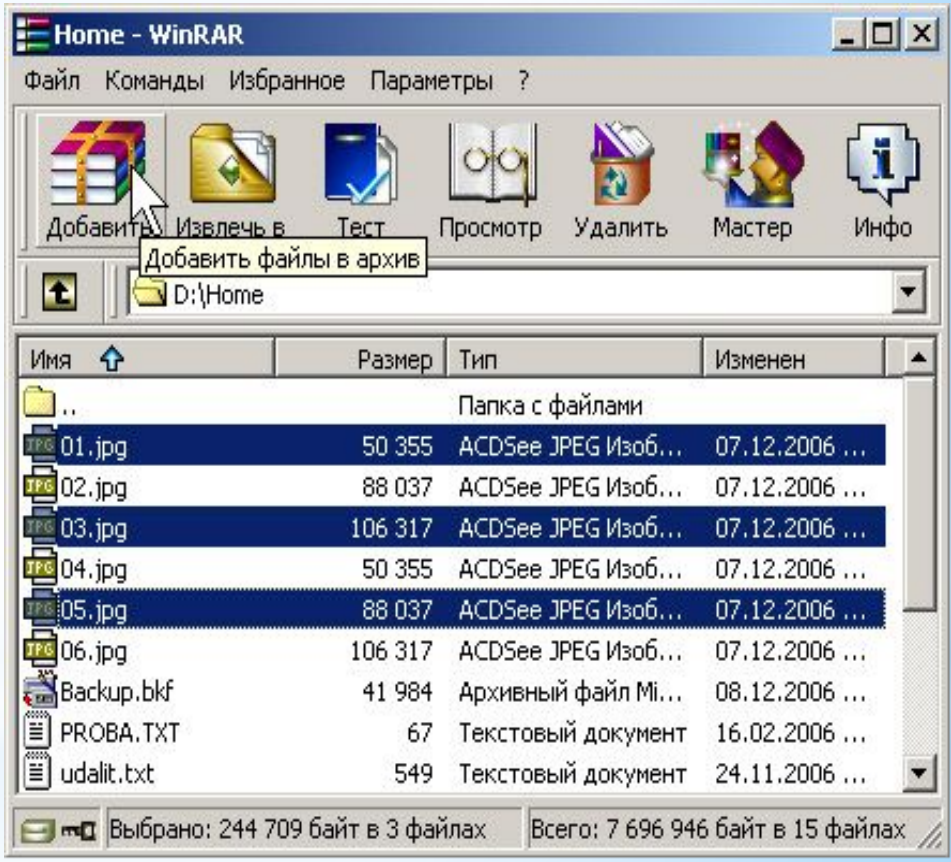


Рис. 3. Добавление выбранных файлов в архив

Содержание

Вперёд

В окне *Имя и параметры архива* выберите вкладку **Общие**, в поле *Имя архива* задайте имя архива (по умолчанию оно задается по имени папки), выберите вариант формата архива RAR, в поле *Параметры архивации* включите флажок **Создать SFX-архив** (создать самораспаковывающийся архив). Обратите внимание, что после этого расширение создаваемого архивного файла в поле *Имя архива* изменяется с rar на exe, как показано на рис. 4.

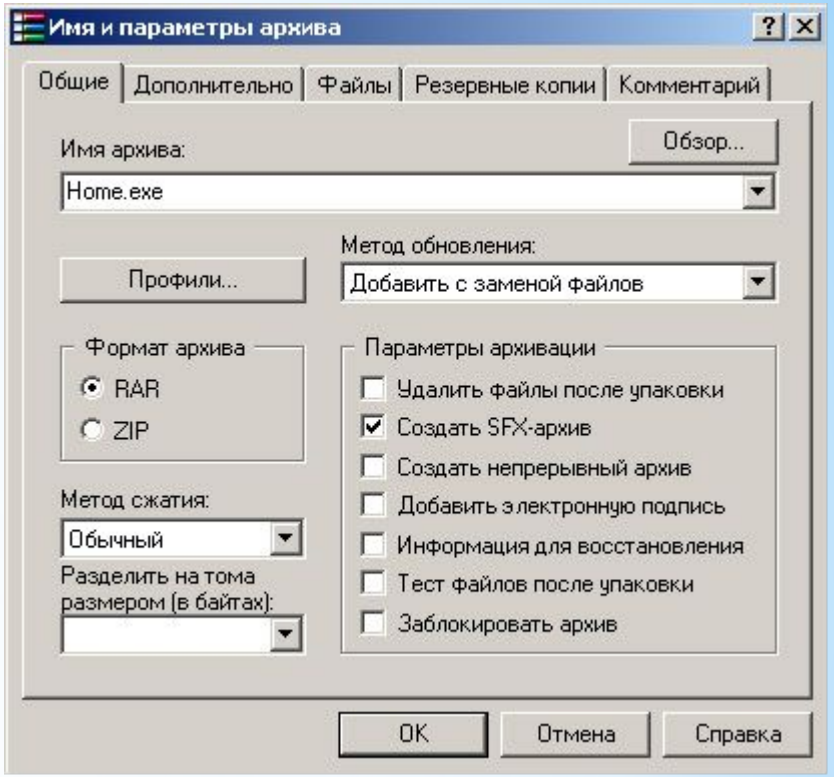


Рис. 4. Определение параметров архива

Выбрав вкладку **Комментарий**, введите в поле **Ввод** комментария вручную текст комментария к создаваемому архиву.

Щелкнув кнопку «ОК», запустите операцию упаковки файлов в архив. После этого выполняется архивация, а на экране выводится окно, отображающее процесс архивации. По окончании архивации в текущем каталоге появится файл самораспаковывающегося архива, в нашем примере, home.exe.

Содержание

Вперёд

4. Удалите из архива home.exe любой файл, для чего откройте архив в окне архиватора WinRAR, укажите удаляемый файл и щелкните кнопку «Удалить» на панели инструментов или выберите команду **Команды ► Удалить файлы**. Подтвердите удаление, щелкнув на кнопке «Да» на запрос в окне подтверждения *Удаление* (рис. 5).

Рис. 5. Окно WinRAR в режиме операций с архивами: удаление файла из архива

Содержание

Вперёд

5. Извлеките из архива home.exe, расположенного в папке H:\Home, файлы, имеющие в имени первый символ «**0**».

Для извлечения файлов из архива выберите каталог H:\Home, в котором содержится архив. Установите курсор на строку с именем архивного файла home.exe и нажмите клавишу **Enter** или щелкните на этом файле левой кнопкой мыши. WinRAR переключится в режим работы с архивами, в окне появится список файлов архива, а в правой части окна будет выведен комментарий к данному архиву. Для выделения группы файлов выберите в меню **File** команду **Select group** или щелкните **Серый +** и задайте в окне выбора маску «**0*.***», как показано на рис. 6. Щелкнув кнопку «ОК», завершите создание маски для выбора группы файлов.

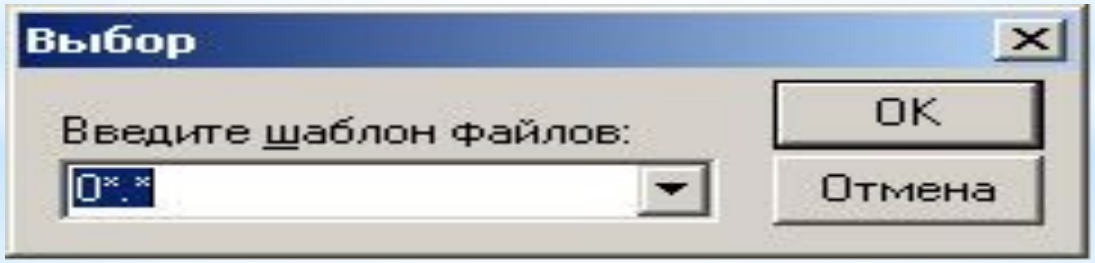


Рис. 6. Выделение группы файлов в архиве

Затем щелкните кнопку «Извлечь в» на панели инструментов или выберите из меню **Команды** команду **Извлечь в указанную папку** (можно щелкнуть комбинацию клавиш Alt+E). В окне *Путь и параметры извлечения* задайте параметры извлечения файлов из архива, щелкните на кнопке «ОК» и наблюдайте процесс извлечения файлов из архива.

Примечание. Если в каталоге уже есть извлекаемый из архива файл, то на экран выводится окно сообщения о том, что такой файл уже существует. В ответ на запрос «Вы хотите заменить существующий файл?» вы должны принять решение и в зависимости от этого щелкнуть кнопку на окне сообщения, показанного на рис. 7.

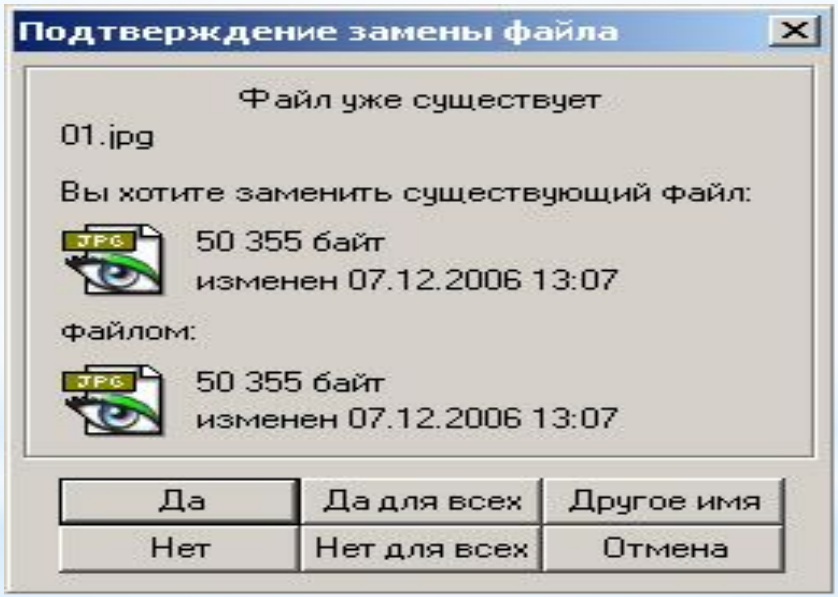


Рис. 7. Окно подтверждения замены файла при извлечении из архива

6. Распакуйте все файлы в папку H:\Home из самораспаковывающегося архива home.exe, созданного при выполнении п. 3. Для этого в **Проводнике Windows** выберите каталог, в котором содержится SFX-архив home.exe, и запустите этот файл на исполнение. Если вы хотите извлечь файлы из архива в другую папку, то, щелкнув кнопку «Обзор», вы откроете диалоговое окно, в котором выберете диск и папку. Если вы хотите отказаться от выполнения операции извлечения файлов из архива, щелкните кнопку «Отмена». После появления на экране диалогового окна выбора папки выберите папку, в которую будут извлекаться упакованные в архив файлы, как показано на рис. 8.

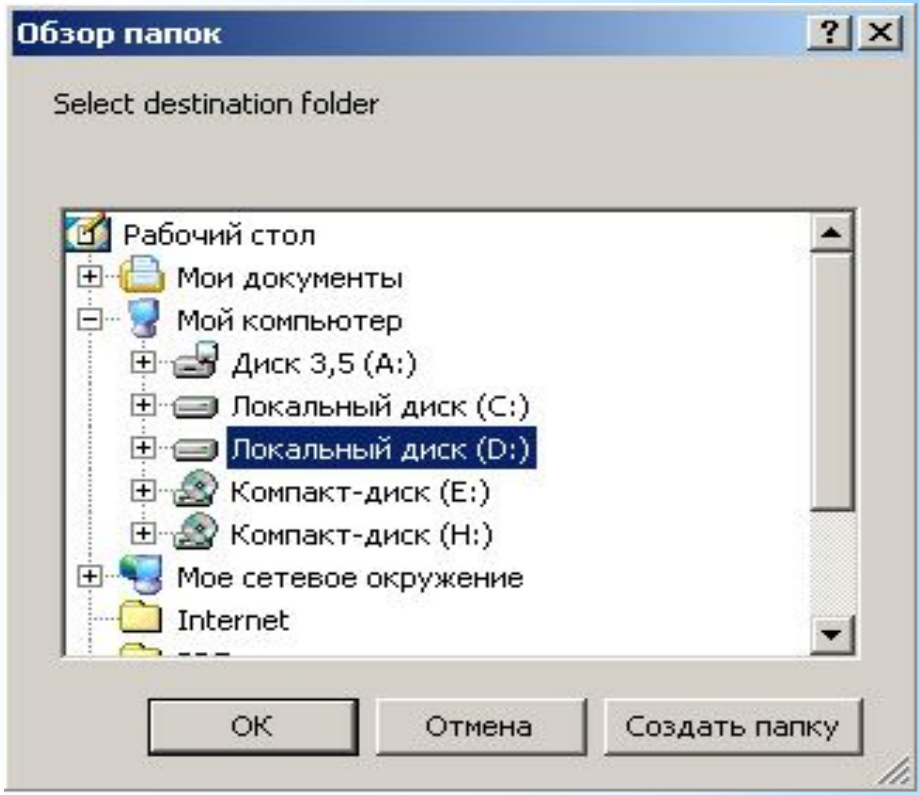


Рис. 8. Диалоговое окно выбора папки

Для начала извлечения файлов щелкните кнопку «Извлечь» для извлечения архива в предложенную папку.

Просмотрите содержимое папки H:\Home и убедитесь, что все файлы извлечены из SFX-архива home.exe в данный каталог.

Содержание

Вперёд

7. Создайте многотомный архив файлов из папки H:\Home, для чего откройте окно архиватора, выберите в поле списка дисков и папок H:\Home, выделите все файлы и щелкните кнопку «Добавить» на панели инструментов.

В окне *Имя и параметры архива* выберите вкладку **Общие**, в поле *Имя архива* задайте имя архива (например, Archive2.rar), выберите вариант формата архива RAR, в поле *Volume size* (Размер тома) задайте размер тома архива (например, 60 000).

Примечание. Выбор размера тома определите в 4-5 раз меньше суммарного объема файлов, включаемых в архив, чтобы в процессе архивации было создано нескольких томов.

Щелкнув кнопку «ОК», запустите операцию упаковки файлов в архив. По окончании архивации в текущем каталоге появится несколько файлов с именем созданного архива, с расширениями, отличающимися нумерацией, например: Archive2.rar, Archive2.r00, Archive2.r01, Archive2.r02, и т.п., где файл с расширением .rar - первый том архива, файлы с расширением .r00,.r01,.r02 и т.п. - файлы следующих томов архива.

Содержание

Вперёд

8. Для создания архивов, доступ к которым защищен паролем, выберите в меню **Файл** команду **Пароль**, в окне *Ввод пароля* по умолчанию в поле *Введите пароль* введите значение пароля и повторите ввод пароля в поле *Повторите пароль для проверки.* Щелкнув кнопку «ОК», завершите определение пароля. После этого в данном сеансе работы архиватора доступ ко всем создающимся архивам будет закрываться заданным паролем (рис. 9).

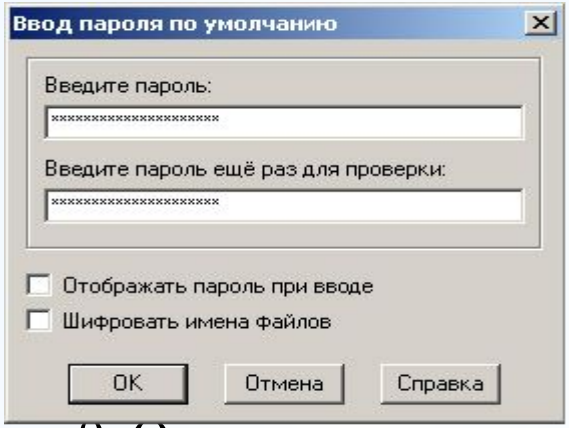


Рис. 9. Определение пароля архива

Примечание. При вводе пароля обратите внимание на включенный регистр символов (лучше выключить Caps Lock) и включить раскладку клавиатуры, принятую по умолчанию (Ru или En).

9. Создайте архив из нескольких файлов в каталоге H:\Home.

10. Чтобы очистить пароль, заданный вами при архивировании, закройте окно архиватора. Запустите повторно архиватор WinRAR и, открыв в окне архиватора архив, доступ к которому защищен паролем, выделите любой файл и щелкните кнопку «Извлечь в» на панели инструментов. Так как архив защищен паролем, то на экране откроется окно *Ввод пароля.*

11. Введите в поле *Введите пароль для зашифрованного файла* любое сочетание символов - неправильный пароль и щелкните кнопку «ОК». Если пароль неправильный, то раскроется окно сообщений, в котором будет выведено сообщение: Ошибка CRC в зашифрованном файле (неправильный пароль). Щелкнув кнопку «Закрыть», закройте окно сообщения. Повторно щелкнув кнопку «Извлечь в» на панели инструментов, в окне *Ввод пароля* введите правильный пароль и щелкните кнопку «ОК». Если пароль был введен правильно, то файл будет распакован из архива.

Содержание

Вперёд

12. Измените настройки программы WinRAR. Для изменения настроек выберите команду **Параметры ► Установки**, после чего на экране развернется окно настройки параметров WinRAR. Выбирая различные вкладки окна *Параметры* для получения подсказки по параметрам настройки, используйте всплывающую подсказку. Задайте следующие параметры настройки WinRAR: На вкладке **Архивация** щелкните кнопку «Создать по умолчанию» для создания опций архивирования по умолчанию, в открывшемся после этого окне *Установить параметры* сжатия по умолчанию включите опции Создать SFX-архив, в списке Размер тома выберите 1 457 664 (стандартный размер тома на диске 3.5»). Щелкнув кнопку «ОК», закройте окно *Установить параметры сжатия* по умолчанию.

Примечание. Можно отредактировать значение размера тома в списке Размер тома, задав его величину вручную.

На вкладке Интеграция включите все флажки в поле *Связать WinRAR* с и щелкните кнопку «ОК» для применения внесенных изменений.

13. Проверьте действие измененных параметров, выделив несколько файлов и щелкнув кнопку «Добавить» на панели инструментов. После этого откроется окно *Имя и параметры архива,* в поле *Имя архива* которого выводится имя с расширением .exe (как было установлено, по умолчанию создается SFX-архив), в поле *Размер тома* отображается значение 1457664 (заданный по умолчанию размер тома). Щелкнув клавишу **Esc**, отмените архивацию. Закройте окно архиватора WinRAR.

Вопросы к защите практической работы

1. Какие факторы влияют на степень избыточности данных?
2. Что такое архив?
3. Какие программные средства называются архиваторами?
4. Применение архиваторов.
5. Понятие процесса архивации, разархивации файлов.
6. Сжатие информации.
7. Архивный файл.
8. Основные характеристики процессов сжатия.
9. Какая зависимость существует между коэффициентом сжатия и эффективностью метода сжатия?
10. Преимущества и недостатки обратимых и необратимых методов сжатия.
11. Форматы архивных файлов. Приведите примеры форматов обратимых и необратимых методов сжатия.

Содержание

Вперёд

12. В чем состоит основная идея необратимых методов сжатия?

13. Особенности сжатия графической информации.

14. Создание и применение самораспаковывающихся архивных файлов.

15. Особенности создания многотомных архивов в программах архиваторах ARJ, PKZIP, WINZIP, WINRAR.

16. Основные виды программ-архиваторов.

17. Работа с программами-архиваторами ARJ, PKZIP, PKUNZIP, WinZip, WinRar.

18. Дополнительные возможности архиваторов. Блокировка, шифрование, создание меток тома.

19. Как осуществить архивацию файлов с паролем?

20. Как осуществить проверку целостности архива?

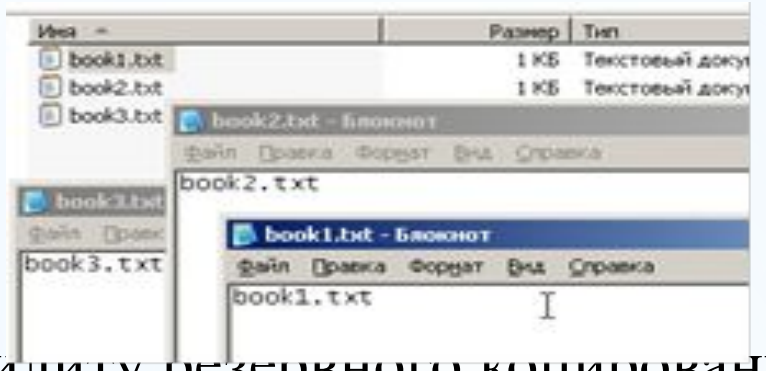
Содержание

Вперёд

Резервирование данных

1. Создать на диске «Н» Вашего сервера каталог *backup* и *restore*;

2. В папке Резерв создать 3 текстовых файла с наименованиями *book1.txt*, *book2.txt* и *book3.txt*. Файлы должны содержать свое наименование.



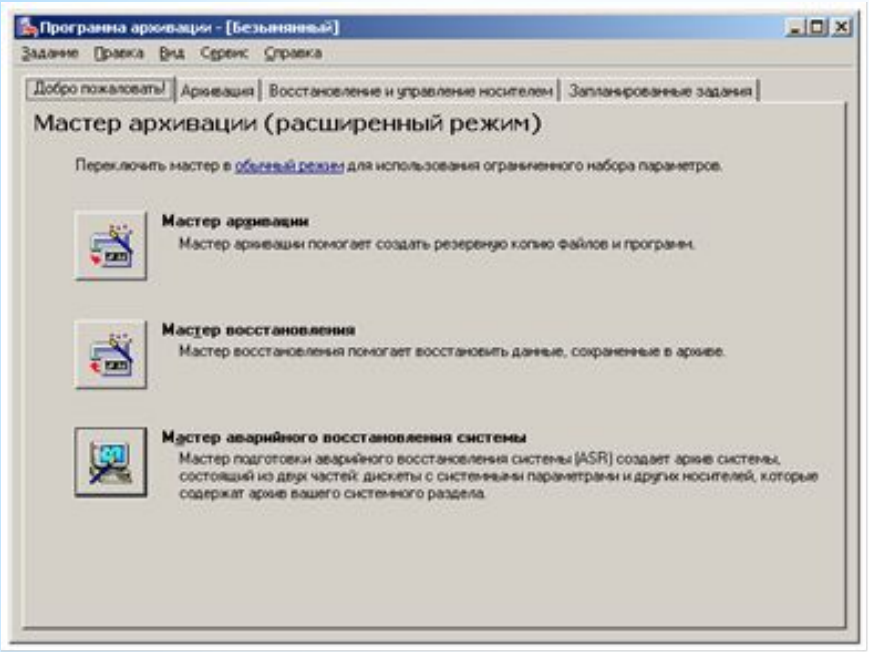
3. Запустить утилиту резервного копирования *ntbackup*.

Эту утилиту можно запустить из Главного меню системы (кнопка «Пуск» — «Все программы» — «Стандартные» — «Служебные» — «Архивация данных»), а можно запустить более быстро из командной строки (кнопка «Пуск» — «Выполнить» — «ntbackup» — кнопка «ОК»). При первом запуске утилиты рекомендуем убрать галочку у поля «Всегда запускать в режиме мастера».

Содержание

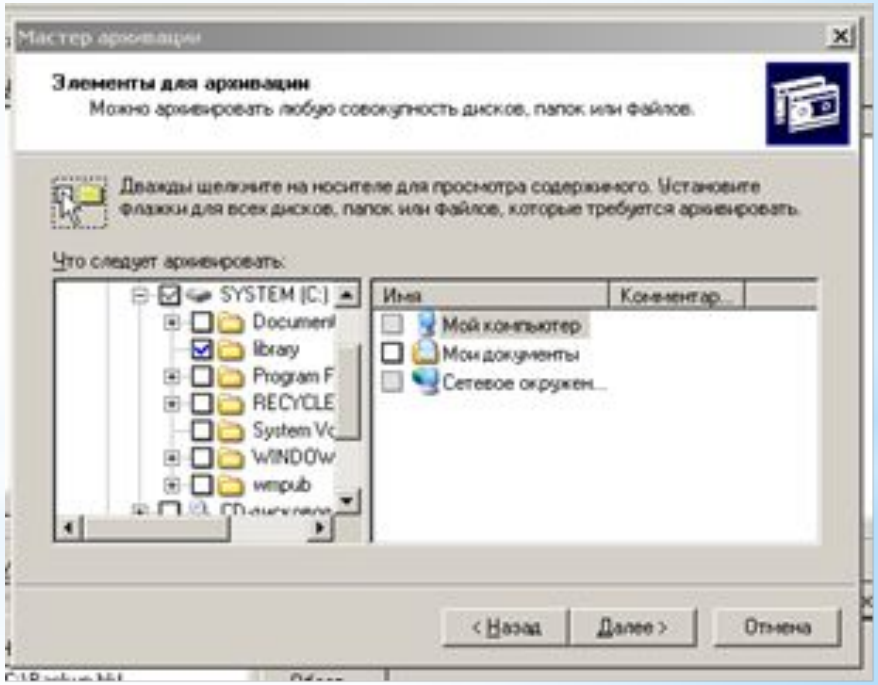
Вперёд

4. Запустить «Мастер архивации» (на закладке «Добро пожаловать» нажать кнопку «Мастер архивации».



5. После запуска мастера нажмем кнопку «Далее» и выберем, что нам нужно архивировать, в данном примере — «Архивировать выбранные файлы, диски или сетевые данные»

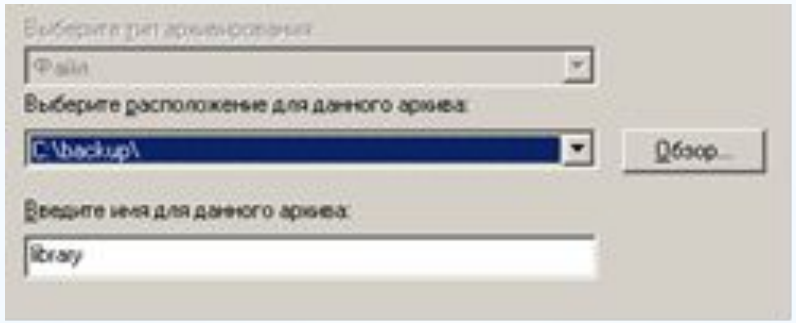
6. Выберем для архивирования папку *Резерв*.



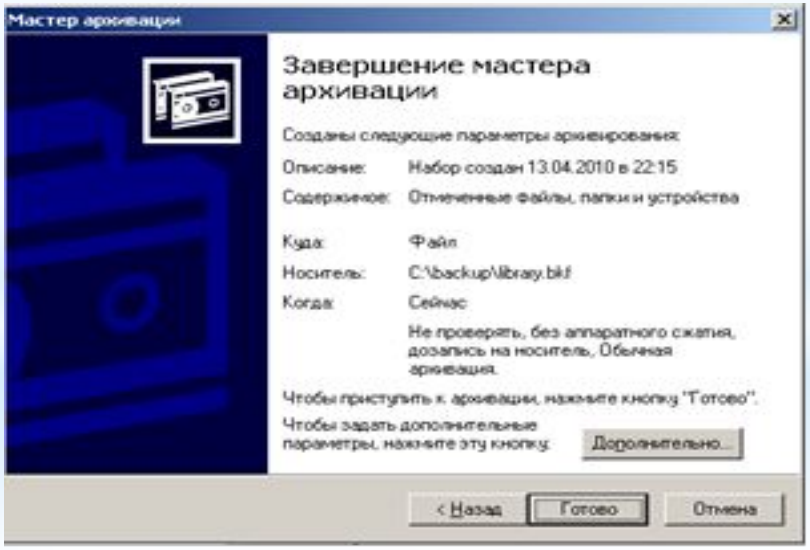
Содержание

Вперёд

7. Выберем место для создания резервной копии, создадим файл с именем *Резерв*, этому файлу автоматически будет назначено расширение «*.bkf*»



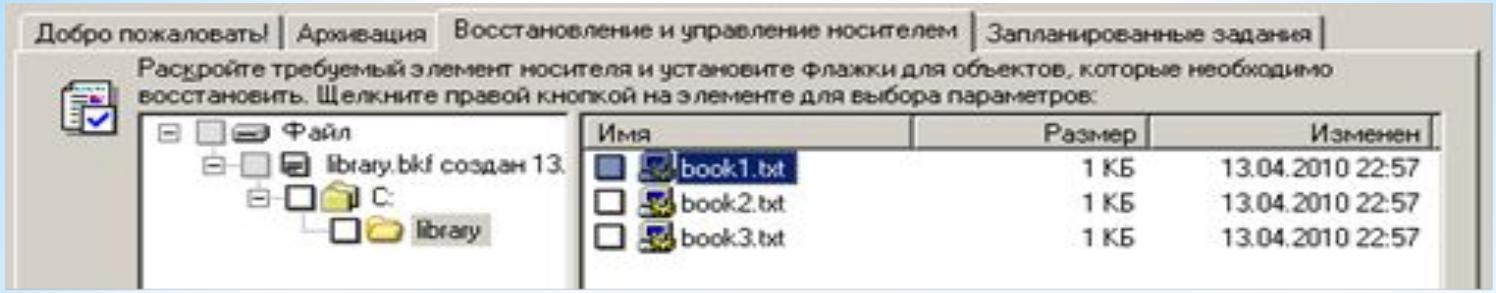
8. На данном этапе нажмем кнопку «Готово».



Содержание

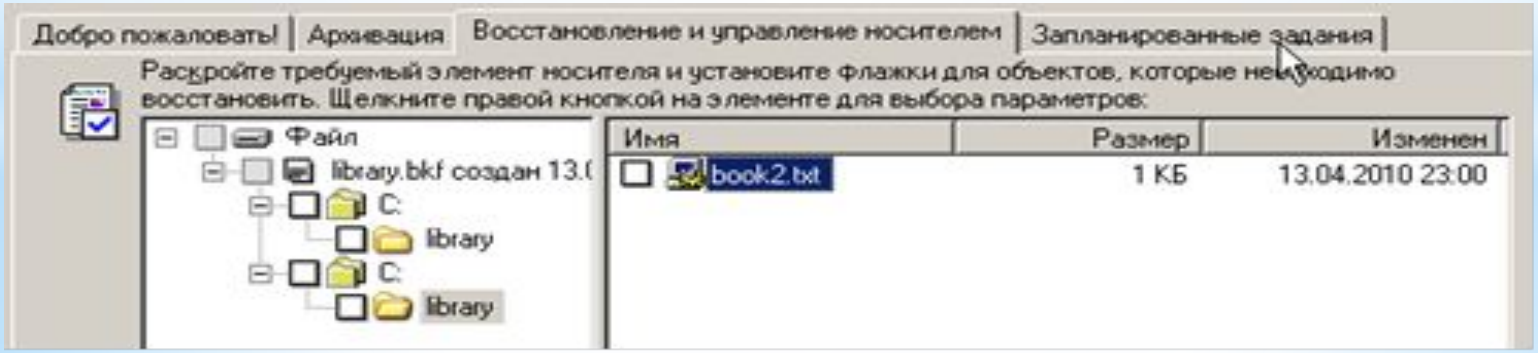
Вперёд

9. Проверяем полученный результат.



10. Вносим изменение в файл *book1.txt* и *book2.txt*, у файла *book1.txt* убираем атрибут «Файл готов для архивирования», а *book3.txt* - удаляем.

11. Запускаем снова процесс архивации, но на 8 этапе нажмем кнопку «Дополнительно», чтобы задать дополнительные параметры и выбираем тип архивации «Добавочный». Далее все пункты по умолчанию, но при этом не забывайте запоминать, что Вы делаете. Проверяем полученный результат. Почему он такой?



Содержание

Вперёд

12. Восстановите файл *book3.txt*. Для этого выполните следующие действия:

1) Запустим утилиту резервного копирования *ntbackup*.

2) Перейдем на закладку "Восстановление и управление носителем".

3) После появления в списке архивных файлов нужного архива раскроем этот архив и выберем файлы для восстановления из резервной копии. При этом мы можем восстановить файлы в то место, где они были ранее ("Исходное размещение") или выбрать иной путь для их сохранения ("Альтернативное размещение"). Выберите папку *restore*.

4) После определения всех параметров восстановления нажмем кнопку "Восстановить", утерянные данные будут восстановлены.

13.Создайте задания на выполнения архивации данных для папки *profiles*, используя выбор дополнительных возможностей:

1) Выбираем тип архивирования (выберем «Обычный»).

2) Ничего не меняем на странице «Способы архивации».

3) На странице «Параметры архивации» можно выбрать замену существующих архивов или добавление архива (если файл с архивной копией уже существует).

Содержание

Вперёд

14. На странице «Когда архивировать» задайте расписание для автоматического создания резервной копии — выберите вариант «Позднее» и задайте расписание архивирования, чтобы архивирование происходило по всем рабочим дням недели. Время начала установите, исходя из текущего времени системы + пять минут.

15. Нажмите далее. Система запросит имя и пароль пользователя, с чьими полномочиями будет выполняться задание архивирования. Рекомендуем для выполнения заданий резервного копирования создать специальные учетные записи, обладающие достаточными правами (как минимум члены группы «Операторы архива»).

16. Нажмем кнопку «Готово», задание будет создано, и оно появится в списке «Назначенных заданий». Теперь оно будет выполняться регулярно в соответствии с расписанием.

17. Завершите сеанс администратора, ожидайте до завершения задания. После проверьте результат.

Содержание

Вперёд

Вопросы к защите практической работы

1. Что такое резервирование файлов?
2. Как выполняется резервирование файлов?
3. Как выполняется восстановление зарезервированных файлов?
4. Что подразумевается под резервированием файлов?
5. Причины и цели резервирования информации?
6. Какие существуют способы резервирования?
7. Какие существуют встроенные в MS Windows программные средства резервирования?
8. Как создать ASR-копию?
9. Как восстановить систему с помощью ASR-копии?
10. Какие данные необходимо резервировать?
11. Какие причины резервирования данных?

Содержание

Вперёд

Работа с антивирусами

Порядок выполнения

1. Сканирование папок на наличие вирусов:

- Двойным щелчком на значке антивируса на панели индикации открыть главное окно программы;
- Изучить содержимое окна: обратить внимание на дату последнего обновления антивирусной базы и дату последней полной проверки компьютера;
- В своей личной папке создать папку **Подозрительные файлы** и создать там 2 файла: ***Текстовый файл*** и ***Документ Microsoft Word***. Имена файлов ввести самим;
- Выбрав пункт в главном окне программы пункт **Поиск вирусов** и добавить в окно заданий папку **Подозрительные файлы**.
- Выполнить проверку папки. По завершению сканирования, используя кнопку **«Сохранить как…»**, сохранить отчет с результатами проверки в папке **Подозрительные файлы**. Имя файла-отчета – **Scan_Log**.
- Закройте окно **Поиск вирусов**.

2. Обновление антивирусной базы:

- В главном меню программы выберете пункт **Сервис.**
- Нажмите на пункт **Обновление** и, используя кнопку **Обновить**, осуществите обновление базы известных вирусов.
- По завершению обновления, используя кнопку **«Сохранить как…»**, сохранить отчет об обновлении в папке **Подозрительные файлы**. Имя файла-отчета – **Upd_Log.**
- Закройте окно Обновление, и обратите внимание на пункт **Дата выпуска сигнатур**.
- Закройте окно **антивируса**.

Содержание

Вперёд

Вопросы к защите практической работы

1. Что называется компьютерным вирусом?
2. Какая программа называется "зараженной"?
3. Что происходит, когда зараженная программа начинает работу?
4. Как может маскироваться вирус?
5. Каковы признаки заражения вирусом?
6. Каковы последствия заражения компьютерным вирусом?
7. По каким признакам классифицируются компьютерные вирусы?
8. Как классифицируются вирусы по среде обитания?
9. Какие типы компьютерных вирусов выделяются по способу воздействия?
0. Что могут заразить вирусы?
1. Как маскируются "невидимые" вирусы?
2. Каковы особенности самомодифицирующихся вирусов?
3. Какие методы защиты от компьютерных вирусов можно использовать?
4. В ка[illegible]яют специализированные програм[illegible] компьютерных вирусов?

Содержание

Вперёд

15. На какие виды можно подразделить программы защиты от компьютерных вирусов?
16. Как действуют программы-детекторы?
17. Что называется сигнатурой?
18. Всегда ли детектор распознает зараженную программу?
19. Каков принцип действия программ-ревизоров, программ-фильтров, программ-вакцин?
20. Как выглядит многоуровневая защита от компьютерных вирусов с помощью антивирусных программ?
21. Перечислите меры защиты информации от компьютерных вирусов.
22. Каковы современные технологии антивирусной защиты?
23. Каковы возможности антивируса Касперского для защиты файловых серверов? почтовых серверов?
24. Какие модули входят в состав антивируса Касперского для защиты файловых систем?
25. Каково назначение этих модулей?
26. Какие элементы электронного письма подвергаются проверке на наличие вирусов?
27. Как обезвреживаются антивирусом Касперского обнаруженные подозрительные или инфицированные объекты?
28. Ка[illegible]русных сигнатур?

Содержание