

Защита информации путем создания архивов с паролем

Теоретическая часть

Программы архивации файлов WinRAR можно использовать двумя способами: в режиме графической оболочки со стандартным интерфейсом Windows и в командной строке.

Чтобы использовать WinRAR в режиме оболочки, дважды щелкните мышью на значке WinRAR — после этого для архивации и извлечения файлов вы сможете пользоваться кнопками и меню.

При открытии архива в окне WinRAR выводится его содержимое. Выделите те файлы и папки, которые вы хотите извлечь. Это можно сделать клавишами управления курсором или левой кнопкой мыши при нажатой клавише <Shift> (как в Проводнике и других программах Windows). Выделять файлы в WinRAR можно также клавишами <Пробел> или <Insert>. Клавиши <+> и <-> на цифровой клавиатуре позволяют выделять и снимать выделение с группы файлов с помощью шаблонов (т.е. задавая маски файлов символами '*' и '?').

Выделив один или несколько файлов, нажмите кнопку Извлечь вверху окна WinRAR, или же нажмите <Alt+E>, введите в появившемся диалоге нужный путь, а после этого нажмите кнопку ОК. Здесь же можно поменять несколько дополнительных параметров. Этот диалог позволяет выбрать папку назначения и параметры для извлечения файлов.

По умолчанию папка получает то же имя, что и архив (без расширения) и размещается в текущей папке. Для того, чтобы поместить в другой папке нужно в диалоге Параметры архивации В поле Путь для извлечения следует ввести нужный путь (если его еще не существует, то он будет создан) или выбрать папку в панели дерева папок.

Оба формата — RAR и ZIP — поддерживают шифрование. Чтобы зашифровать файлы, нужно до начала архивации указать пароль — в командной строке, в меню или непосредственно на вкладке Дополнительно диалога Имя и параметры архива.

Если вы ввели пароль непосредственно в диалоге Имя и параметры архива, то вам не нужно отменять его самостоятельно — пароль будет действовать только в течение одной операции архивирования, по окончании которой сбросится автоматически.

При извлечении зашифрованных файлов можно ввести пароль заранее, хотя это и необязательно. Если пароль не был введен перед началом извлечения, и WinRAR обнаружил зашифрованный файл, он спросит пароль у пользователя. Для обеспечения достаточного уровня безопасности используйте пароли длиной не менее 8 символов. Не следует использовать в качестве пароля слова какого-либо языка, лучшим выбором является случайная комбинация букв и цифр. Обратите внимание, что в паролях учитывается регистр букв. Если вы потеряете свой пароль, восстановить из

Информационная безопасность организации

архива зашифрованные файлы не удастся — в этом вам не поможет даже сам автор WinRAR.

Если включена опция Шифровать имена файлов, WinRAR будет зашифровывать не только находящиеся в файлах данные, но и другие важные области архива как-то: имена файлов, размеры, атрибуты, комментарии и другие блоки, благодаря чему достигается более высокая степень защиты от несанкционированного доступа. Если архив зашифрован с этой опцией, то без указания пароля не удастся даже просмотреть список содержащихся в нём файлов.

В этом диалоге также доступно несколько дополнительных параметров:

В командной строке пароль задается с помощью ключа -p<pwd>

Пример:

WinRAR a -pZaBaToAd -t secret games*.*

Эта команда добавит содержимое папки games в архив secret, используя пароль ZaBaToAd.

Ряд программ обслуживания архивов файлов позволяет использовать криптографическую технику. Наименее широко используются из них программы ZIP и ARJ. Среди традиционных средств поддержки архивов как добавление, удаление, обновление, распечатка и извлечение файлов, в них входят операции «взбивания» файлов с паролем при их помещении в архив и извлечении. Задание пароля осуществляется ключами -sпароль (S - от английского слова scramble, что означает смешивать, взбивать, соединять). В программе ARJ используется ключ G - garble - подготавливать, искажать). Так, например, создание архива всех файлов из каталога может быть выполнено утилитой PKZIP при помощи Trivia так: >PKZIP -sTrivia archive.zip *.*.

К особенностям работы с программами архивации нужно отнести неудовлетворительное задание пароля, который отображается на экране и может быть подсмотрен как визуально, так и техническими средствами перехвата излучения мониторов компьютеров. Кроме того, шифрование захватывает область данных архива, которая легко реконструируется, как длина исходного файла, его название и ряд резервных нулевых байт. Из-за этого, несмотря на вообще-то серьезное взбивание текста с паролем, возникают обоснованные опасения в возможности криптографической атаки на ключ.

Поэтому данные способы засекречивания сообщений устойчивы лишь от любопытных, но не от профессиональных взломщиков и тем более от государственных криптографических служб. Известно множество «ломалок» для зашифрованных архивов, которые подбирают ключ, контролируя контрольную сумму. Эффективность их очень невелика, так как по контрольной сумме файл вскрывается весьма неоднозначно, а примененный способ тотального опробования ключей годится только для сверхбыстродействующих ЭВМ. Однако периодически приходится взламывать архивы, ключи к которым пользователи забыли или ввели с

ошибкой. Простенькая программа модификация этого ключа, учитывающая ошибки при наборе позволяет примерно в половине случаев подобрать ключ за пару часов работы даже слабой персональной ЭВМ.

Использование архиватора RAR.

Данный архиватор пользуется не меньшей популярностью у нас в стране потому, что имеет вполне удобный для работы интерфейс, отчасти напоминающий всем известный NORTON COMMANDER, поддерживает некоторые файловые операции (например, удаление файлов, каталогов) и избавляет пользователя от проблем с указанием всех необходимых ключей в командной строке вызова архиватора (конечно, проще нажать F2 и ввести имя архива, чем набирать «arj a myarch.arj» и т.д. С другой стороны, архивация ZIP и ARJ является уже сформировавшимся стандартом, так что RAR является не более чем просто удобной программой-оболочкой для архивирования. К тому же, работа с ZIP и ARJ у данного архиватора происходит через вызовы всё тех же программ PKZIP и ARJ.

Архивация с паролем с помощью архиватора RAR происходит следующим образом. При нажатии ALT+P архиватор запросит пароль на архивную сессию, т.е. данный пароль будет действовать на всё время, пока пользователь не выйдет из среды архиватора.

После ввода пароля RAR предложит пользователю подтвердить ввод путем повторного введения пароля. При несовпадении пароль запомнен не будет. Далее можно работать с файлами обычным путем, но все пакуемые файлы будут архивироваться с паролем. При открытии архива файлы, защищенные паролем будут иметь значок * перед своим именем, а при попытке разархивирования, если не был введен пароль на архивную сессию, RAR запросит пароль для первого встретившегося файла с паролем и затем спросит, следует ли использовать введенную последовательность для всех остальных архивных файлов.

Задание

1. Создайте архив, используя программу PKZIP, включив в него файлов 5-6. Теперь добавьте к архиву 4 файла, защищенных паролем.
2. Попробуйте разархивировать созданный архив, введя неправильный пароль и проконтролируйте содержимое файлов, архивированных с паролем.
3. Повторите вышеприведенные задания, используя архиватор ARJ.
4. В программе RAR создайте архив, используя несколько различных паролей.
5. Используя программу RAR попытайтесь осуществить разархивирование созданных выше архивов, созданных программами PKZIP и ARJ. Все ли файлы разархивировались?
6. Проверьте, влияет ли регистр вводимых в пароле символов при архивировании на правильность последующего ввода при разархивировании?
7. Используя BAT-файл и архив с паролем из одной цифры, попробуйте осуществить подбор пароля.