УДК 00.004

Алексеев П.А., студент 1 курса,
факультет информационных технологий,
Брянский государственный технический университет,
г. Брянск, Россия

ЗАШИФРОВАННЫЕ АРХИВЫ – ЛУЧШЕЕ РЕШЕНИЕ ДЛЯ ОБЫВАТЕЛЯ

Аннотация. *В статье рассказывается о архивах с шифрованием и их особенностях*

Ключевые слова: *шифрование, архивы, RAR, ZIP, AES-128.*

Abstract: *The article describes encrypted archives and their features.*

Keywords: *encryption, archives, RAR, ZIP, AES-128.*

Зашифрованные архивы - лучшее решение для обывателя

Благодаря скоротечному развитию IT-сектора и Всемирной сети сегодня все большее количество информации, которая может иметь конфиденциальный характер, передается по Интернету. Такую информацию при приложении определенных усилии могут получить в своих целях злоумышленники или просто заинтересованные лица. Чтобы избежать этого, необходимо шифровать данные. Существуют разные методы обеспечения высокого уровня конфиденциальности при помощи шифровки, которые отличаются значительной степенью надежности сохраняемых сведений. Это может быть архивирование с паролем, применение специальных шифрующих приложений или криптографических файловых систем. Архивирование отдельно взятых запароленных файлов и каталогов через использование обычных архиваторов – это наиболее простой способ шифровки данных. Широко известно, что представляет собой «архив» в отношении файлов. Это

некий контейнер, потенциально содержащий огромное количество файлов, но выступающий для операционной системы в качестве единственного файла.

Использование архива дает владельцу способность сократить занимаемый файлами объем памяти на персональном компьютере благодаря их сжатию. Кроме того, пересылать их по электронной почте или выкладывать в сети Интернет несколько файлов зачастую более удобно не по отдельности, а в форме архива. Не всем известно, что архиваторы также способны ограничить доступ к содержимому архивного файла через установление парольного доступа. Тем самым, помимо экономии объема памяти на диске, пользователю ПК обеспечивается защищенность файлов благодаря процедуре шифрования.

Во многих архивирующих системах внедрена функция шифровки, и данные программные средства находятся в свободном доступе для пользователя. Неудобной стороной их использования можно считать потребность в проведении операций вручную при создании архивов. Однако современные архиваторы не имеют этой проблемы, и с их использованием возможно запросто учредить пароль для архива непосредственно из программного меню. Опцией шифровки, заложенной в архивирующих программах, можно пользоваться для не очень значимой информации, поскольку применяемая там методика шифровки не особо надежна. Эта особенность не дает возможность серьезно полагаться на качественную защиту. Говоря о методах шифрования, которые реализуются в программах-архиваторах, нужно отметить ограниченный выбор. В большинстве наиболее популярных архиваторов в основе заложен какой-либо один метод. Помимо этого, стандартная ZIP-кодировка наряду с шифрованием по алгоритму DES не относится в настоящий момент к категории надежных.

Архивирование данных в некоторых случаях может применяться с целью распространения вирусов. Они могут изменять поток архивных данных, что может вызвать повреждение содержимого. Это приведет к невозможности распаковать данный архив даже при наличии верного пароля. В документах к

архивирующим программам с функцией шифровки часто сообщается о невозможности расшифровки архивов с паролями. Сегодня эта информация не всегда соответствует реальности. При работе с конфиденциальными данными этот факт обязательно стоит учитывать. Свои особенности защиты архива имеются в программах WinRAR и 7-Zip.

В чем различия между шифрованием информации в архивах форматов ZIP и RAR? Если кратко, то при шифровании первого типа архива проводится лишь шифровка данных, а при шифровке архива RAR возможно зашифровать также сведения о файлах. В частности, к таким данным относятся их размер, атрибуция, комментарии, наименование. Если совершать просмотр подобного архива и выбрать шифрование данных и наименование файлов, то возникнет пустая папка. Файлы будут видны при просмотре, если шифровка файловых наименований не задействуется.

Для шифрования файлов необходимо до старта архивации ввести пароль в меню, командной строке, или самой вкладке. В отличие от ZIP формата, RAR дает возможность зашифровать не только сами файловые данные, но также другие значимые архивные области: имена файлов, атрибуты, размеры, комментарии и иные блоки. Непрерывные RAR-архивы и архивы, содержащие зашифрованные имена файлов, могут иметь лишь один пароль, одинаковый для всех файлов. Файлы в обычных архивах этого формата без шифровки файловых имен и в ZIP архивах могут быть зашифрованы с различными паролями. Необходимо удалять введенный пароль после того, как он станет ненужным, в противном случае можно непреднамеренно запаковать файлы с паролем. Для удаления пароля введите в соответствующем диалоге пустую строку или закройте WinRAR и вновь запустите его.

В формате ZIP 2.0 используется свой алгоритм шифрования. Архивы RAR шифруются на основе значительно более надежного и сложного алгоритма AES-128. В случае необходимости зашифровать секретную или приватную информацию более предпочтительным будет выбор формата RAR, при этом наибольшая длина пароля для таких архивов составляет 127

символов. Важно учесть, что при утрате пароля извлечение из архива зашифрованных файлов станет невозможно. Установленный на RAR пароль, как правило, не хранится внутри архива. RAR шифрует данные после сжатия с помощью алгоритма AES, получая в итоге зашифрованный текст. При разархивации RAR пытается расшифровать его с введенным паролем независимо от правильности пароля. То есть понять, является ли пароль верным, можно лишь после процедуры распаковки архива. Ввиду того, что формат RAR использует симметричный алгоритм, криптографический ключ (ключ шифрования) для него один.

Архиваторы ZIP применяют свой собственный алгоритм шифровки, который относится к неустойчивым, и является причиной двух практических уязвимостей. Злоумышленник всегда способен провести атаку по имеющемуся открытому тексту, для чего нужен лишь один архивный файл без шифровки. В случае если архив был создан в формате WinZip или Infozip и содержит в составе пять или больше файлов, то тогда можно провести гарантированное расшифрование архива вне зависимости от того, насколько длинным и сложным является пароль.

Устойчивость зашифрованного архивного файла зависит лишь от самого пользователя. В современный период действуют программы, позволяющие осуществить подбор паролей при использовании различных словарей. Исходя из этого, предполагаемый к использованию пароль должен содержать значительное количество символов (не менее 8, а лучшим решением будет задать размер от 15 символов). Кроме того, пароль не рекомендуется делать словом, которое содержится в словарях, и он должен состоять из букв и цифр. Следует помнить, что пароль зависит и от регистра. При соблюдении данных требований есть очень большая уверенность в том, что никто не окажется способен подобрать необходимый пароль к архиву.

Таким образом, использование для шифровки программ-архиваторов будет неплохим решением для обычного пользователя с целью защиты личных данных ввиду простоты и значительной надежности. При этом нужно

учесть специфику данного типа шифрования и соблюдать правила составления паролей.

Используемые источники:

1. Ватолин Д., Ратушняк А., Смирнов М., Юкин В. Методы сжатия данных.

2. Устройство архиваторов, сжатие изображений и видео - 2002.- стр 57-63.

3. Экслер А.Б. Архиваторы. Программы для хранения и обработки информации в сжатом виде.- 1992 – стр 23-29.