Файл Zip с паролем. Насколько это безопасно?

Анастасия Рыкова

https://te-st.org/2023/06/23/zip/

Статья опубликована 23 июня 2023

Когда речь идет о защите важных файлов, мы вспоминаем о шифровании. Veracrypt, Cryptomator, Picocrypt, hat.sh, Mailvelope — примеры замечательных шифровальных инструментов, о которых мы уже рассказывали читателям. А как же обычные файловые архивы, спрашивают люди на вебинарах и консультациях. Надежно ли шифрование в zip-файле?

Как устроено шифрование в архивах

Шифрование в zip-архивах было впервые предложено и реализовано в далеком 1993 году. Алгоритм назывался ZipCrypto. По нынешним представлениям, стандарт Zip 2.0, основанный на ZipCrypto, — слабенькая защита. Пожалуй, единственное его преимущество, да и то сомнительное, это совместимость практически со всеми утилитами архивирования/шифрования, даже устаревшими. В 2003 году в архивах стал использоваться популярный протокол AES (Advanced Encryption Standard, расширенный стандарт шифрования). Сегодня в ходу 128-битный и 256-битный AES — числа означают длину ключа. AES-128 быстрее, но AES-256 обеспечивает гораздо более стойкое шифрование.

Для шифрования пользователю нужно придумать пароль. (Когда про zip-файлы говорят «защитить паролем», речь фактически идет о шифровании.) Качество защиты ваших файлов зависит не только от протокола шифрования и его реализации в конкретной программе, но и

от пароля. Самый крутой шифровальный метод становится бессмысленным, если пароль простой, легко угадываемый и записан на рабочем столе в файле passwords.txt.

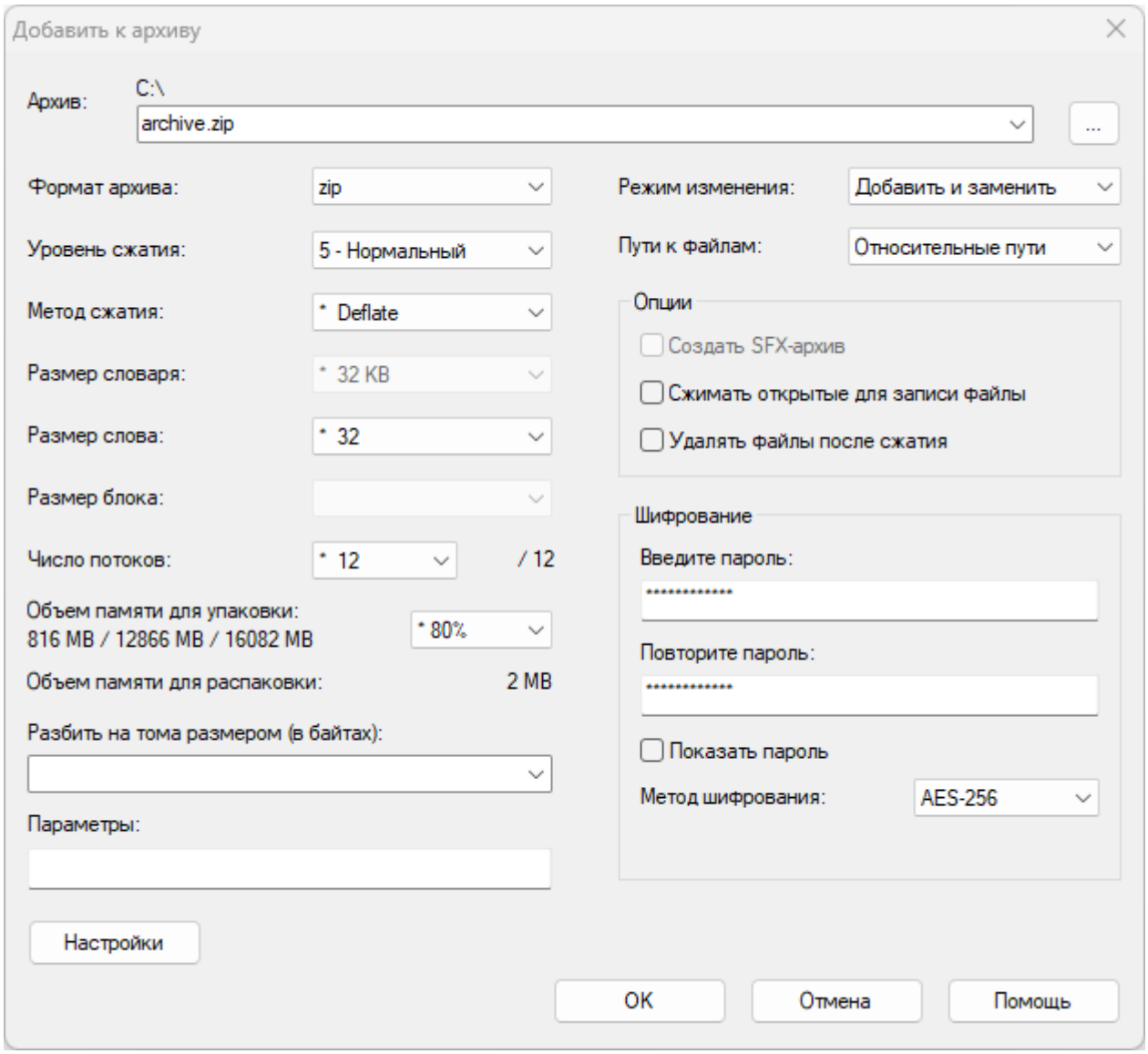
Есть и еще одна особенность. Шифрование в архивах защищает только собственно файлы, их содержимое. Метаданные (названия файлов, даты создания, размер и др.) под защиту не попадают и могут быть просмотрены тем, кто не знает пароль.

7-Zip

В Windows 10 и 11 так просто файл с паролем не зашифруешь. Нужно устанавливать дополнительную программу для работы с архивами. 7-Zip — возможно, самый популярный архиватор для Windows. Это бесплатная программа с открытым кодом. Для macOS и Linux доступны консольные версии.

После установки 7-Zip в «Проводнике» (или другом файловом менеджере) щелкните правой кнопкой мыши по файлу. В Windows 11 вам может понадобиться выбрать в контекстном меню пункт «Показать дополнительные параметры»: так вы увидите меню полностью. Выберите «7-Zip» — «Add to archive». Откроется окно с параметрами архивирования. Укажите формат архива zip. Теперь нас интересует раздел «Шифрование». Выберите «AES-256» и дважды введите пароль.

Теперь при попытке открыть зашифрованный zip-файл с помощью 7-Zip программа покажет внутренности архива, но не позволит вытащить из него файл без знания пароля.

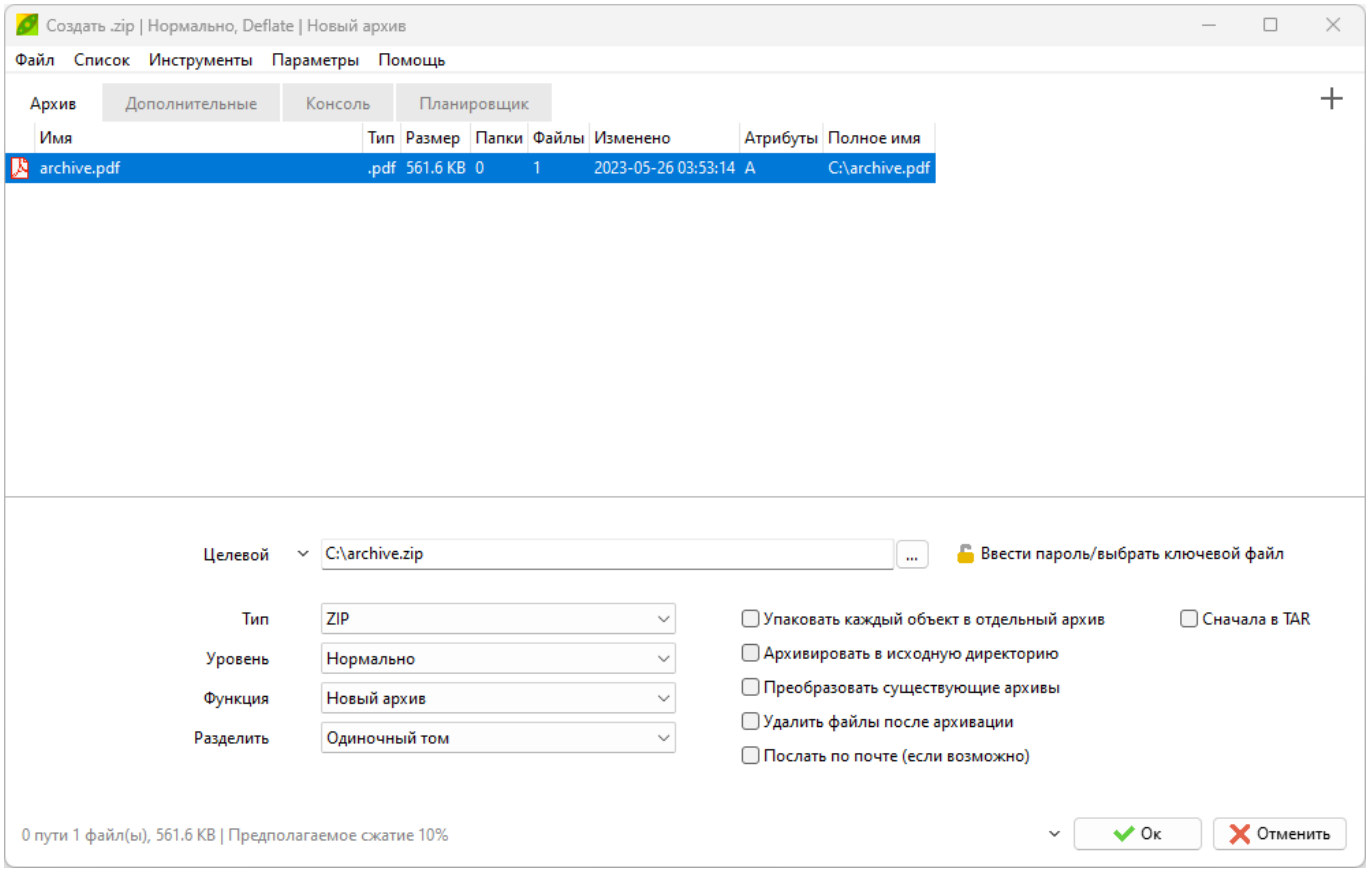


PeaZip

PeaZip — не столь знаменитый, но сильный и симпатичный конкурент 7-Zip. Тоже бесплатный и с открытым кодом. Есть версии для macOS и Linux.

После установки PeaZip в «Проводнике» (или другом файловом менеджере) щелкните правой кнопкой мыши по файлу. В Windows 11 вам может понадобиться выбрать в контекстном меню пункт «Показать дополнительные параметры»: так вы увидите меню полностью. Выберите «PeaZip» — «Добавить в архив». Откроется окно с параметрами архивирования. Убедитесь, что в поле «Тип» выбран формат архива zip (по умолчанию). Теперь чуть правее нажмите ссылку «Ввести пароль / выбрать ключевой файл». Введите пароль дважды. Вы также можете дополнительно выбрать ключевой файл (и таким образом задействуете двухфакторную аутентификацию). PeaZip поддерживает только шифровальный протокол AES-256, так что выбирать в настройках нечего.

7-Zip прекрасно открывает архивы, созданные PeaZip, и наоборот. Правда, если с помощью PeaZip вы добавили при шифровании ключевой файл, такой прием 7-Zip понять не сможет и не откроет содержимое архивированных файлов. Встроенный архиватор Windows с расшифровкой защищенных архивов 7-Zip и PeaZip не справляется вовсе.



Другие программы и форматы архивов

Zip, вероятно, самый распространенный формат для архивирования в мире Windows. Но у 7-Zip есть и собственный формат — 7z. PeaZip его понимает. В этом формате вы можете зашифровать не только содержимое архивированных файлов, но и метаданные. Тогда чрезмерно любопытный человек, заглянув в архив, не увидит, как называются файлы внутри и когда они созданы. Для этого:

- 7-Zip: поставьте галочку в поле «Шифровать имена файлов»;
- PeaZip: поставьте галочку в поле «Также шифровать имена файлов (если позволяет формат».

Мы не рассматриваем в качестве примеров такие известные программы, как WinZip и WinRAR, потому что стараемся по возможности предлагать читателям бесплатный софт с открытым кодом. Однако обычные архивы .rar прекрасно открываются и 7-Zip, и PeaZip. Кроме того, rar допускает шифрование с паролем и поддерживает AES-256, а также шифрование метаданных архивируемых файлов. Если перед вами стоит выбор «zip или rar», мы советуем первое. Формат zip более распространен и активно поддерживается свободным программным обеспечением. Рекламируемое преимущество rar в степени сжатия не выглядит существенным при нынешних объемах носителей данных. Архивы rar большого объема лучше поддаются восстановлению в случае повреждения. Это может сыграть важную роль, если вы имеете дело с крупными архивами на не очень надежных носителях.

Шифрование в архиваторах вряд ли может похвастать использованием каких-то новомодных технологий. Но оно есть и работает. Существует немало других утилит и сервисов для защиты файлов, помимо упомянутых в начале этой статьи. Например, шифрование существует как встроенная функция Windows. Можно защитить паролями файлы документов Microsoft Office и Adobe (PDF). Теплица вернется к этой теме.