

**ПРОГРАММНОЕ СРЕДСТВО ДЛЯ СКРЫТИЯ ДАННЫХ
В АЛЬТЕРНАТИВНЫХ ПОТОКАХ ФАЙЛОВОЙ СИСТЕМЫ NTFS**

М. В. Колмаков, Е. А. Блинова

Белорусский государственный технологический университет, Минск

Предложен метод скрытия данных в альтернативных потоках файловой системы NTFS, разработано программное средство AltDS, реализующее данный метод, приведены примеры его использования.

Введение

Одним из решений проблемы скрытой передачи информации является использование цифровых стеганографических методов. В настоящее время является актуальной задача поиска новых типов контейнеров, пригодных для стеганографического встраивания информации, и методов их использования. В качестве контейнера скрытых сообщений предлагается использовать альтернативные потоки данных, доступные в файловой системе NTFS.

1. Разработка программного средства AltDS

Авторами разработано программное средство и выполнена адаптация стеганографического метода на основе альтернативных потоков в файловой системе NTFS. В качестве стеганоконтейнера может выступать папка в операционной системе на основе файловой системы NTFS, содержащая любое количество файлов. Данные будут разбиваться на части и записываться в альтернативные потоки к файлам [1]. Для разработки программного средства выбран язык программирования C# с использованием Win-API функций. Для работы с альтернативными потоками была выбрана библиотека Trinet.Core.IO.Ntfs, так как стандартные средства в C# не поддерживают работу с альтернативными потоками. Дополнительно данные могут быть зашифрованы с использованием алгоритма RSA, для расшифрования потребуется правильный пароль. Кроме того, вставка сообщения в альтернативные потоки может осуществляться с разбиением на отдельные блоки, и при последующем извлечении информация будет объединена в одно сообщение в правильной последовательности.

2. Использование программного средства AltDS

При работе с программным средством AltDS пользователь первоначально выбирает папку с файлами, куда будет выполнено осаждение информации (рис. 1).

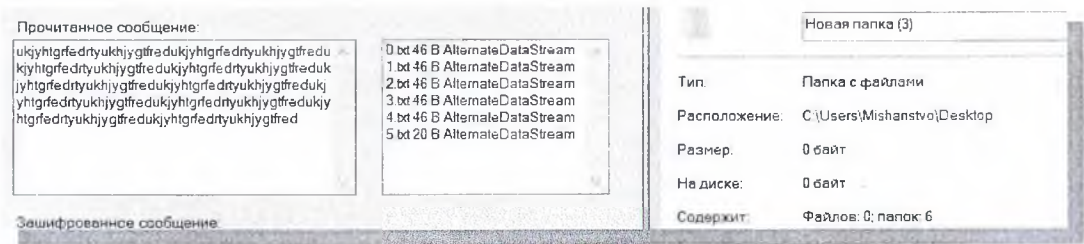


Рис. 1. Вставка текста в папки

Далее пользователь выбирает, на сколько частей разбивать секретное сообщение, но не более чем количество файлов в папке.

Имеется возможность использовать папки как контейнеры. Преимуществом папок является то, что при вставке скрытых данных их размер никак не меняется (рис. 2).

После этого пользователю предлагается сделать выбор, шифровать ли данные. После всех операций программа создает альтернативные потоки к выбранным файлам и записывает в них части сообщения.

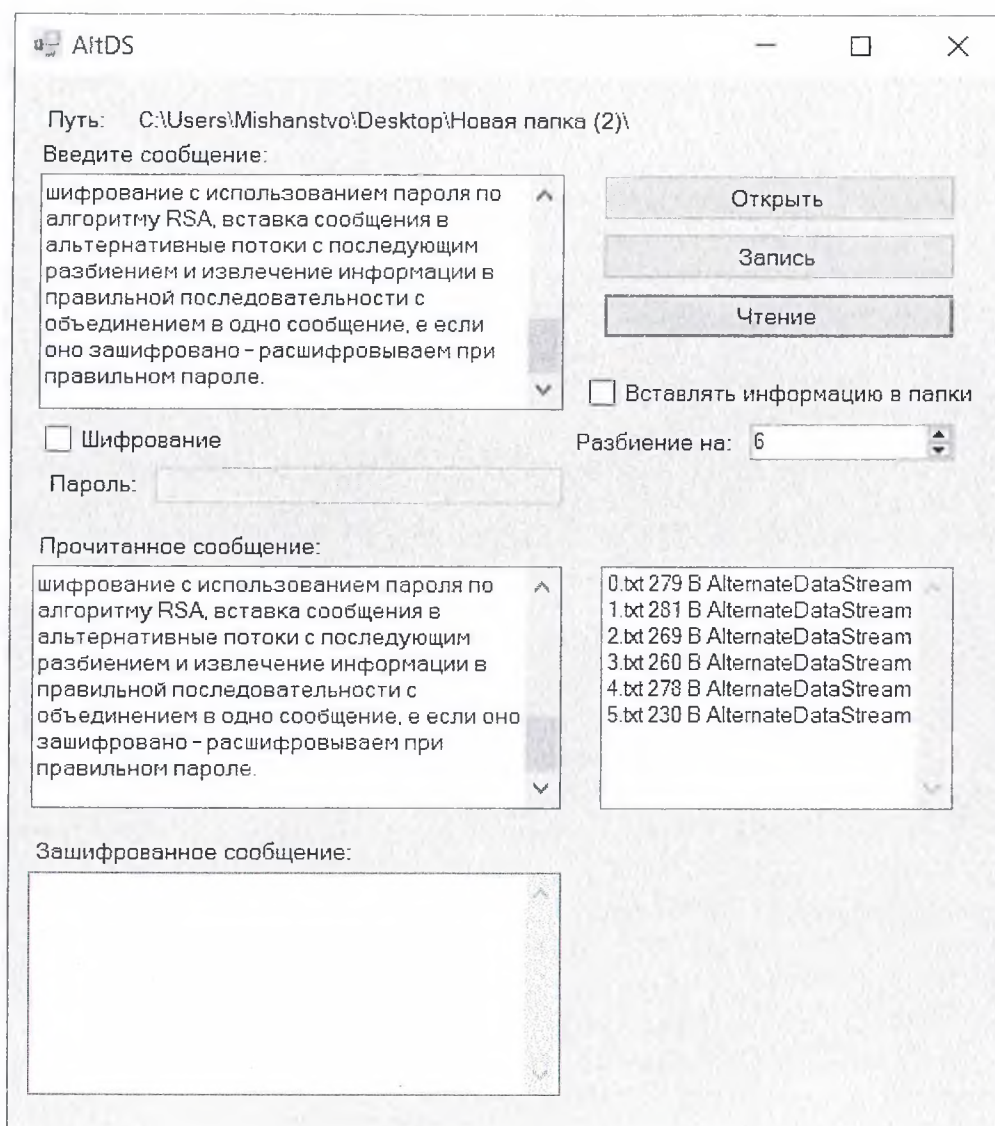


Рис. 2. Вставка текста и его чтение из альтернативных потоков

При выборе директории, в которую мы хотим вставить скрытую информацию, она проверяется на наличие файлов и папок (рис. 3). Если окажется, что директория пуста, то будет ошибка, так как нечего вставлять. В программе отображается размер каждого потока и указывается, сколько было использовано потоков.

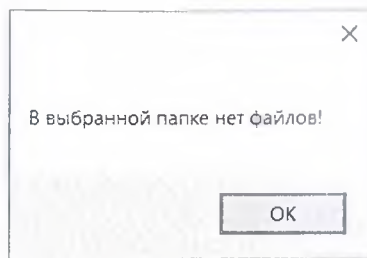


Рис. 3. Проверка на пустую папку

Пользователь может ввести любое сообщение, которое он хочет внедрить в электронный файл-контейнер, длина сообщения не ограничена. Есть возможность дополнительного выбора предварительного криптопреобразования сообщения алгоритмом RSA с последующим хешированием зашифрованного сообщения. При считывании сообщения идет проверка на наличие альтернативных потоков, и при наличии в них данных секретная информация может быть извлечена (рис. 4).

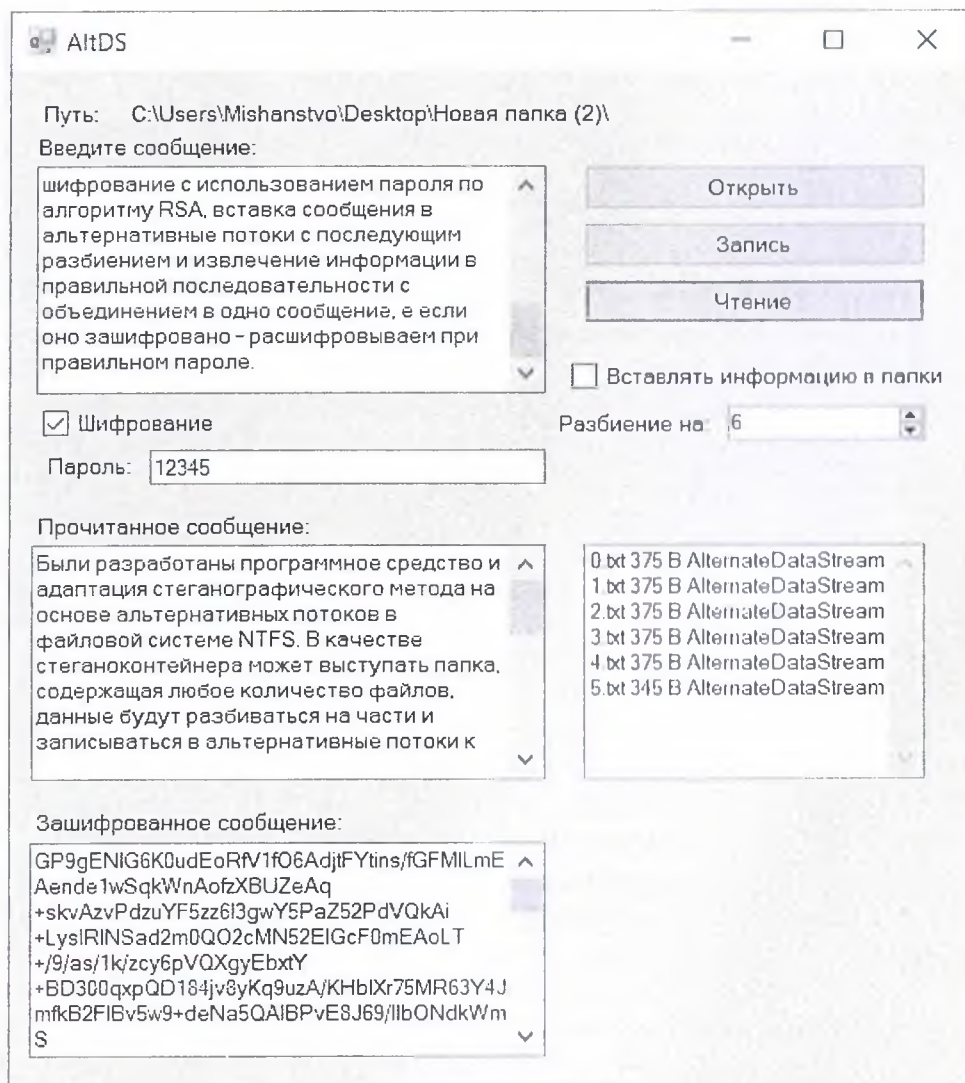


Рис. 4. Вставка текста с шифрованием по паролю

Если информация была предварительно зашифрована, то при извлечении из контейнера нужно ввести пароль (рис. 5).

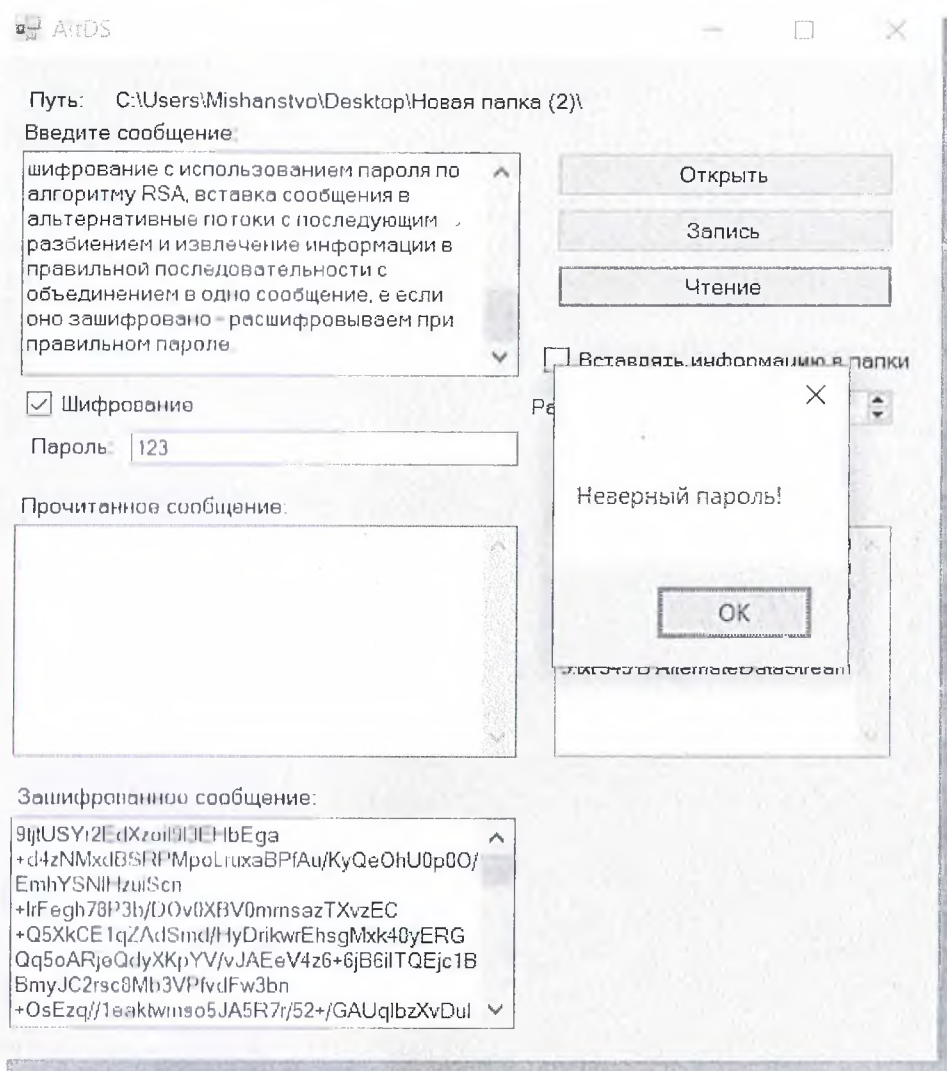


Рис. 5. Результат попытки ввести неверный пароль

Заключение

Проведен анализ целостности файлов с осажденной информацией после переноса их между различными файловыми системами. Разработано программное средство и выполнена адаптация стеганографического метода на основе альтернативных потоков в файловой системе NTFS. В качестве стеганоконтейнера может выступать папка в операционной системе на основе файловой системы NTFS, содержащая любое количество файлов и папок.

Стоит отметить, что при переносе файлов в другие файловые системы, отличные от NTFS, скрытая информация полностью теряется.

Список литературы

1. Github [Electronic resource]. – 2018. – Mode of access: https://github.com/mishanstvo/AltDS_Steganography. – Date of access: 01.04.2018.