счет создания дополнительных переменных и функций работы с данными переменными.

2. Временные затраты на разработку приложений в Unreal Engine несколько больше, нежели в Unity. Это обуславливается более сложным созданием логики приложения.

3. При импорте сложных объектов, созданных посредством Autodesk 3ds max в Unity может повлечь за собой ухудшение производительности приложения, в то время как в Unreal Engine – нет, так как невидимые части объектов не рендерятся на сцене.

4. Разрабатывать на Unreal Engine может даже тот человек, который не знает языков программирования, за счет существования в UE системы Blueprint.

Таким образом, наиболее приемлемой платформой для разработки достаточно сложных в функциональном отношении симуляторов реальных динамических систем по затратам на разработку и возможностям включения элементов логики и интеллекта является платформа Unreal.

ЛИТЕРАТУРА

1. Unity documentation [Электронный ресурс] / Unity Technologies, 2015 Режим доступа: https://docs.unity3d.com/ru/current/Manual/index.html. Дата доступа: 03.04.2018.

2. CRYENGINE V Manual [Электронный ресурс] / CRYTEK GmbH, 2016 Режим доступа: http://docs.cryengine.com/display/CEMANUAL/CRYENGINE +V+Manual. Дата доступа: 04.04.2018.

3. Unreal Engine 4 documentation [Электронный ресурс] / Epic Games Inc., 2004-2018 Режим доступа: https://docs.unrealengine.com/en-us/. Дата доступа: 01.04.2018.

УДК 004.056

М.В. Колмаков, маг.
Науч. рук. ст. преп.Е.А. Блинова
(кафедра информационных систем и технологий, БГТУ)

ОСОБЕННОСТИ ПРИМЕНЕНИЯ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ В АЛЬТЕРНАТИВНЫХ ПОТОКАХ ФАЙЛОВОЙ СИСТЕМЫ NTFS.

Одним из решений проблемы скрытой передачи информации является использование цифровых стеганографических методов. В на-

стоящее 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.

Были разработаны программное средство и адаптация стеганографического метода на основе альтернативных потоков в файловой системе NTFS. В качестве стеганоконтейнера может выступать папка, 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. Из методов можно отметить шифрование с использованием пароля по алгоритму RSA, вставка сообщения в альтернативные потоки с последующим разбиением и извлечение информации в правильной последовательности с объединением в одно сообщение, е если оно зашифровано – расшифровываем при правильном пароле.

При работе с программным средством AltDSS пользователь первоначально выбирает папку с файлами, куда будет выполнено осаждение информации, далее выбирает, на сколько частей разбивать секретное сообщение, но не более чем количество файлов в папке. Так же была добавлена работа только с папками, что помогает скрыть информацию еще лучше.

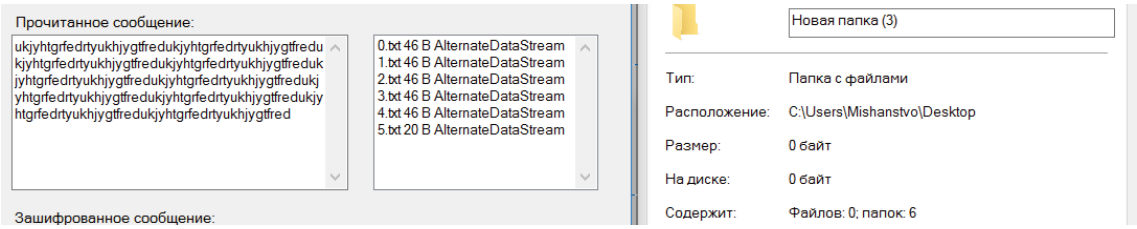

Рисунок 1 − Вставка текста в папки.

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

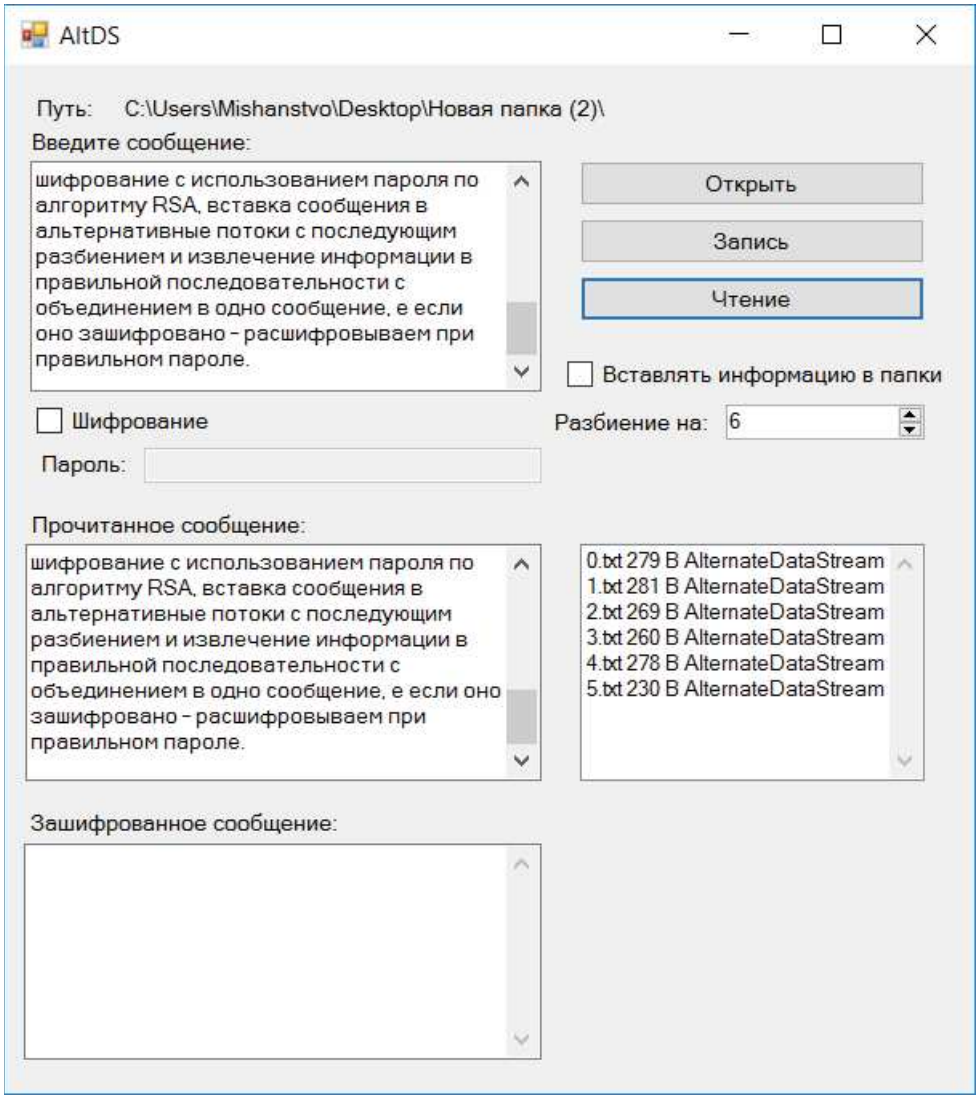

Рисунок 2 – Вставка текста, и чтение его из альтернативных потоков

Так же существуют различные проверки на неправильный пароль, если выбрать папку без файлов. В программе отображается размер каждого потока и указывается сколько было использовано потоков.

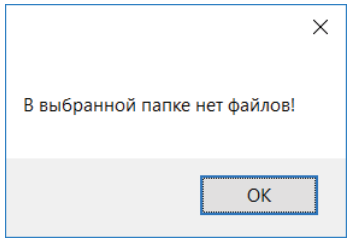

Рисунок 3 – Проверка на пустую папку

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.

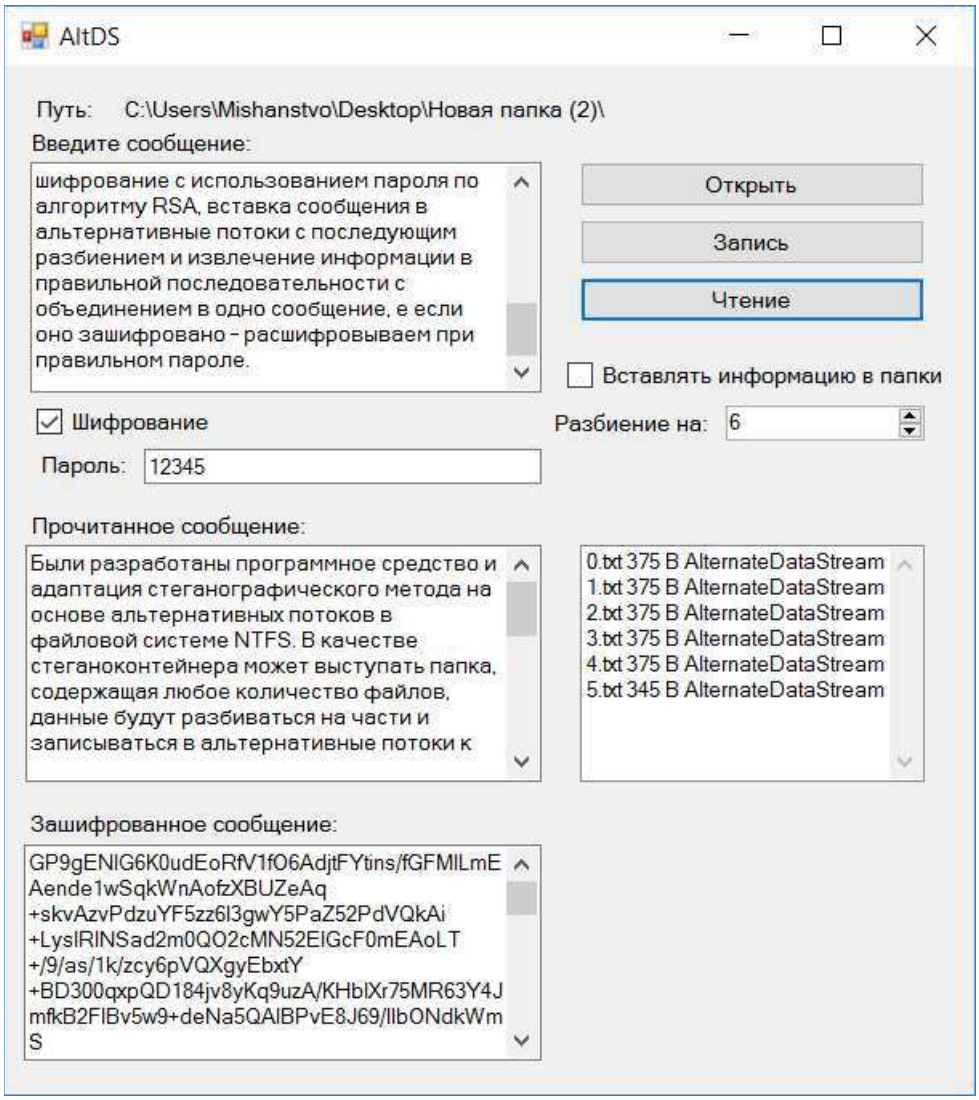

Рисунок 4 – Вставка текста с шифрованием по паролю

Если она была предварительно зашифрована – при извлечении из контейнера нужно ввести пароль.

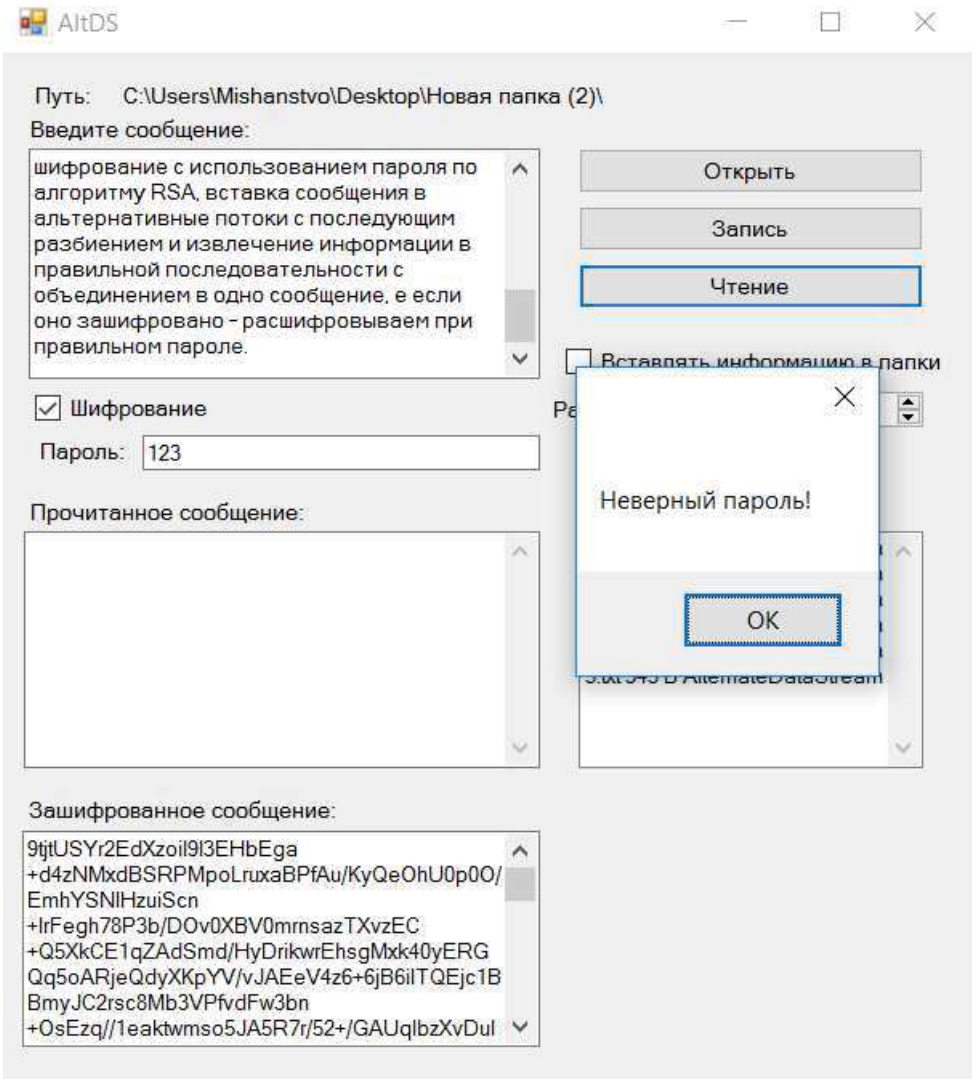

Рисунок 5 − Попытка ввести не верный пароль

Произведен анализ целостности файлов с осажденной информацией после переноса их между различными файловыми системами. Стоит отметить, что при переносе файлов в другие файловые системы отличные от NTFS, скрытая информация полностью теряется.

ЛИТЕРАТУРА

1. Github [Электронный ресурс] / github.com/mishanstvo. – 2018 GitHub, Inc. – Режим доступа: https://github.com/Mishanstvo/AltDS_Steganography. – Дата доступа: 01.04.2018.