УДК 003.26+004.56

МЕТОД НА ОСНОВЕ ИЗМЕНЕНИЙ ЯЗЫКА СИМВОЛОВ ДОКУМЕНТОВ WORD В МНОГОКЛЮЧЕВОЙ СТЕГАНОГРАФИЧЕСКОЙ СИСТЕМЕ

Берников В. О.
Белорусский государственный технологический университет, Минск, Беларусь, vladbernikovronaldo@gmail.com

Реферат. В докладе кратко описываются разработанные стеганографический метод на основе изменений языка символов документов Word и программное средство для осаждения и обратного извлечения секретной информации. Этот метод опирается на многоключевую модель стеганографической системы. Данная модель может использовать неограниченное число методов стеганографии, криптографии, помехоустойчивого кодирования или других преобразований для повышения стеганографической стойкости системы. Программное средство может использоваться в научных исследованиях, а также в учебном процессе [1, 2].

В силу стремительного развития информационных технологий защита авторского права на электронные документы приобретает все большую актуальность. Поэтому создание новых методов текстовой стеганографии обеспечивает эффективное решение данной проблемы.

Программное средство написано на языке C# с использованием технологии WPF. Для разбора электронных документов Word использовалась библиотека Aspose.Words. Данная библиотека содержит нужные методы для работы с документами.

Суть разработанного метода состоит в том, чтобы изменять язык символов документов-контейнеров Word на язык символов осаждаемого стегосообщения. Продемонстрируем работу программного средства. Процесс осаждения секретной информации в контейнер показан на рисунке 1.

Сначала выбирается электронный документ, куда помещается секретная информация. Производится автоматических подсчет символов скрываемой информации. Непосредственно вводим сообщение, которое хотим скрыть. Предварительно шифруем секретное сообщение при помощи симметричного алгоритма AES с использованием длины ключа в 256 бит. Далее зашифрованная последовательность

кодируется при помощи кодов Боуза-Чоудхури-Хоквингема с использованием кодовой последовательности в 1023 бита. Для проверки целостности осажденной информации в контейнер используется алгоритм хеширования Keccak с длиной ключа 512 бит. Дополнительно выбирается сокрытие информации псевдослучайным образом, а также подсветка символов, содержащих скрытую информацию. На рисунке 2 представлен фрагмент стегноконтейнера с осажденной информацией.

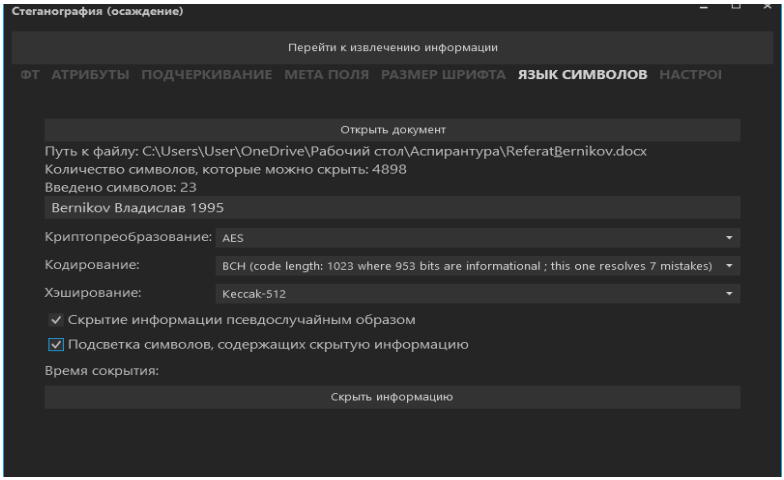

Рисунок 1 – Осаждение секретного сообщения в контейнер

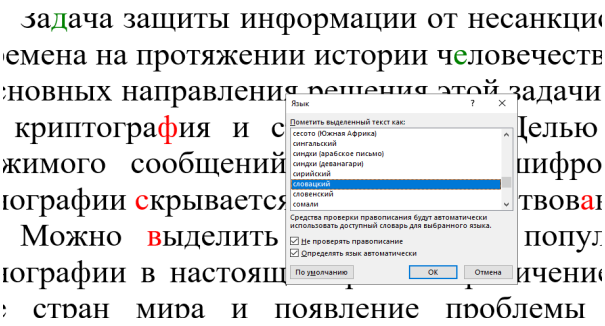

Рисунок 2 – Фрагмент документа после осаждения нулевых бит

Красным цветом помечены нулевые биты секретной информации. Язык этих символов был изменен с русского языка на словацкий. Как видно из рисунка, текстовый процессор Word не подчеркивает слова, в которых использует два языка. Аналогичным образом, происходит осаждение единичных бит стегосообщения (рисунок 3).

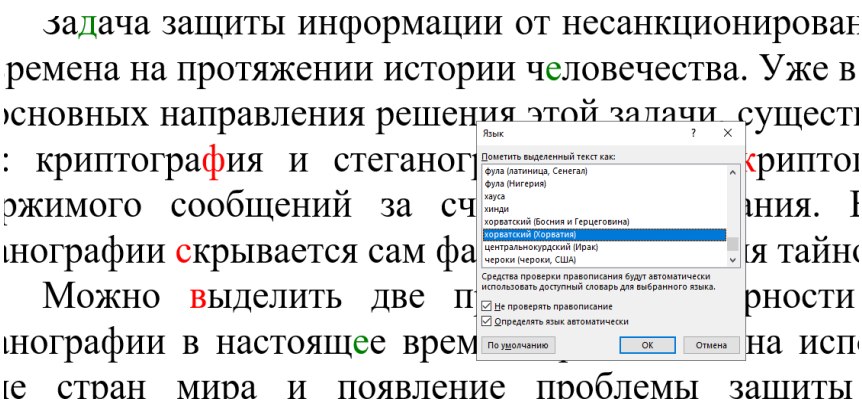

Рисунок 3 – Фрагмент документа после осаждения единичных бит

Соответственно, зеленым цветом помечены единичные биты стегосообщения. Язык данных символов был изменен уже с русского языка на хорватский. При помощи Word-а очень сложно обнаружить биты стегосоообщения, так как необходимо смотреть язык каждого символа документа.

Для корректного извлечения секретной информации из документа необходимо использовать такие же ключи многоключевой модели системы, которые использовались при осаждении этой информации. Процесс извлечения стегосообщения представлен на рисунке 4.

Предварительно выбирается электронный документ с осажденным стегосообщением. После этого выбираются файлы с тайным ключом и хешем. Секретная информация сначала декодируется, затем расшифровывается и извлекается из контейнера согласно разработанному стеганографическому методу на основе изменений языка символов.

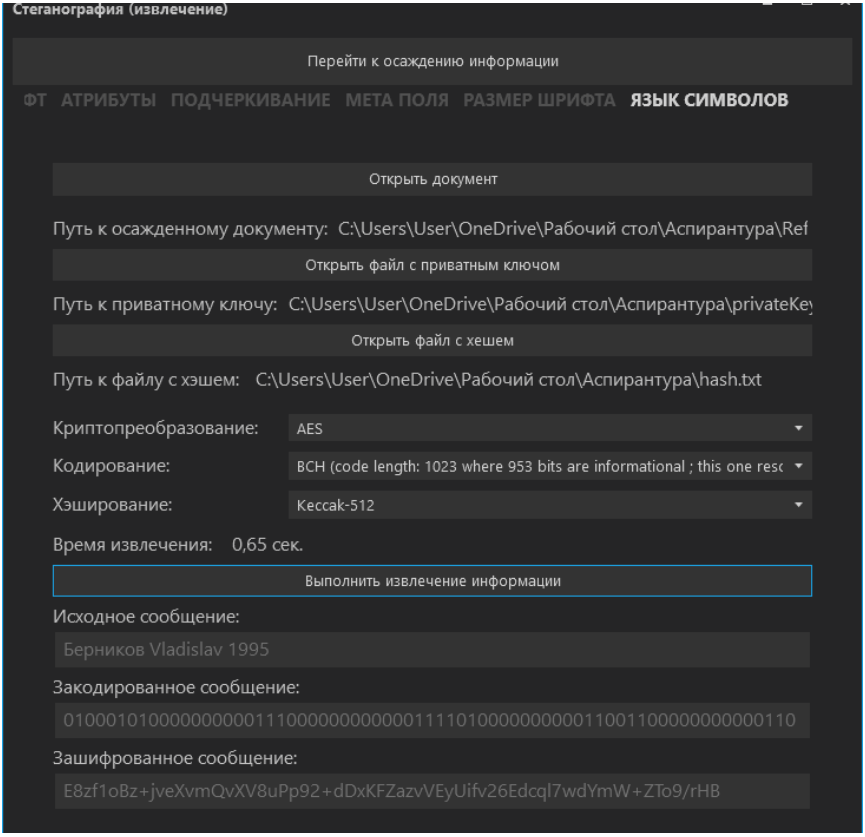

Рисунок 4 – Извлечение секретного сообщения из контейнера

Данный метод можно считать эффективным, так как процесс поиска секретной информации в документе очень трудоемкий. Для того, чтобы обнаружить факт сокрытия информации в контейнере, необходимо проанализировать язык каждого символа этого документа [3, 4].

Описанное программное средство реализовано на основе модели информационной системы, которая подразумевает применение практически неограниченного числа ключей. Представлен процесс внедрения и извлечения стегосообщений на основе разработанного стеганографического метода. Разработанное средство можно использовать в учебном процессе при изучении студентами дисциплин

«Защита информации и надежность информационных систем» и «Криптографические методы защиты информации».

СПИСОК ЛИТЕРАТУРЫ

1. Pavel Urbanovich, Nadzeya Shutko. Theoretical Model of a Multi-Key Steganogra- phy System, in: Recent Developments in Mathematics and Informatics, Contemporary Mathematics and Computer Science Vol. 2, Ed. A. Zapała. – Wydawnictwo KUL, Lublin, 2016, Part II, Chapter 11. – P. 181–202.

2. Берников В. О. Разработка стеганографических методов на основе многоключевой модели информационной системы / В.О. Берников // Новые математические методы и ком- пьютерные технологии в проектировании, производстве и научных исследованиях. – Гомель: ГГУ им. Ф. Скорины. – 2018. – С. 192–193.

3. Берников В. О. Анализ стеганографической стойкости текстового документа- контейнера в многоключевой стеганосистеме // 69-я НТК студентов и магистрантов: сб. науч. работ: в 4-х ч. 17–22 апреля 2018 г. – Минск: БГТУ, 2018. – Ч. 4. – С. 14–17.

4. Берников В. О. Математическое моделирование стеганографической стойкости многоключевой системы / В. О. Берников, П. П. Урбанович // Информационные технологии: материалы 83-й научно-технической конференции профессорско-преподавательского состава, научных сотрудников и аспирантов (с международным участием), Минск, 4–15 февраля 2019 г. / отв. за изд. И. В. Войтов; УО БГТУ. – Минск : БГТУ, 2019. – С. 31–33.