

А. А. Сушня
(УО «БГТУ», Минск)

СПОСОБ СТЕГАНОГРАФИЧЕСКОГО ОСАЖДЕНИЯ ИНФОРМАЦИИ В ДОКУМЕНТ С РАСШИРЕНИЕМ .DOCX

В отличие от DOC формат DOCX не является расширенным файловым форматом. Он представляет собой файл-архив. Формат файла основан на Open XML и использует сжатие по алгоритму ZIP для уменьшения размера файла.

Исходя из этого, можно использовать формат DOCX для осаждения тайной информации на основе стеганографического преобразования [1]. Как известно XML-формат, из-за своей избыточности, хорошо подходит для внедрения в него дополнительной информации, не изменяющей его непосредственное предназначение.

Для внедрения сообщения в XML можно использовать метод замены кавычек [2]. Известно, что синтаксис XML-документа не чувствителен к типу кавычек. Следовательно, если заменить какую-нибудь пару кавычек в XML-документе (который используется в качестве контейнера, например, с двойной на одинарную), то при визуальном анализе документа со стороны пользователя в браузере никакой разницы видно не будет. Используя эту технику, в XML-документ можно осадить бинарную последовательность.

Для внедрения информации в DOCX, по средствам XML, вначале необходимо изменить расширение файла на ZIP. В полученном архиве разместить XML документы, обработанные методом замены кавычек. Далее изменить расширение на DOCX.

При внедрении информации в DOCX-контейнер важно не нарушать структуру папок и файлов, так как открытие некорректного документа в редакторе MS Word невозможно.

Литература

1 Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие / П. П. Урбанович. – Минск: БГТУ, 2016. – 220 с.

2 Сущень, А. А. Стеганографическое преобразование текстовых контейнеров на основе языков разметки / А. А. Сущень // 68-я научно-техническая конференция учащихся, студентов и магистрантов: сборник научных работ, Минск, 17–22 апреля 2017 г.: в 4 ч. / Белорусский государственный технологический университет. – Мн.: БГТУ, 2017. – Ч. 4. – С. 145 – 149.