

УДК 003.26+004.056

П. П. Урбанович, проф., д-р техн. наук,  
В. О. Берников, магистрант  
(БГТУ, г. Минск)

**СТЕГАНОГРАФИЧЕСКИЕ МЕТОДЫ  
И ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА ПЕРЕДАЧИ  
И ХРАНЕНИЯ ИНФОРМАЦИИ НА ОСНОВЕ  
МНОГОКЛЮЧЕВОЙ МОДЕЛИ ИНФОРМАЦИОННОЙ  
СИСТЕМЫ**

В докладе рассматриваются и анализируются реализации стеганографических методов, основанных на использовании различных характеристик и свойств текстовых документов [1]. Детали, внедряемые (осаждаемые) автором в электронные документы, должны оставаться невидимыми другим пользователям, и при этом позволять однозначно (при их извлечении и расшифровке) подтвердить авторство документа.

Многоключевая модель информационной системы предполагает интегрированное использование различных методов стеганографии, криптографии и помехоустойчивого кодирования для повышения криптостойкости системы [1,2].

Произведено аналитическое исследование современных методов в решении задач обеспечения прав интеллектуальной собственности на текстовые документы. В настоящее время бремя защиты авторских прав лежит на самом авторе или на правообладателе авторских прав. Из этого следует, что автор или правообладатель, прежде чем помещать документ в Интернете, должны предварительно позаботиться о реализации мер по защите своих авторских прав.

Рассматриваемая задача решается использованием нескольких подходов. Один из них разработан специалистами Google для своей поисковой системы и основан на привязке охраняемого контента к профилю Google+ с помощью подтвержденного адреса электронной почты. Однако это могут реализовать лишь те владельцы ресурса, которые имеют собственный сайт с доменом первого уровня и почтовый ящик на нем.

Другой подход, так называемый DRM (Digital Restrictions (Rights) Management – управление цифровыми ограничениями или правами), основан на использовании программных или программно-аппаратных средств, которые ограничивают либо затрудняют различные действия с данными в электронной форме (копирование, модификацию, просмотр и т. п.).

Известны методы стеганографии (на основе цвета и параметра апрова) и программное средство их реализующее, основанные на использовании различных методов предварительного преобразования осаждаемой информации (помехоустойчивое кодирование, шифрование), различных методов осаждения информации в стеганоконтейнер [2, 3].

Для разработки программного средства нами выбран язык программирования C# и технология WPF. Для парсинга электронных документов была выбрана библиотека Aspose.Words, которая поддерживает как старые, так и новые форматы документов Microsoft Word.

Пользователь может ввести любое сообщение, которое он хочет внедрить в электронный документ-контейнер. Данное сообщение преобразуется в нули и единицы, используя кодировку Unicode. Есть возможность дополнительного выбора предварительного криптопреобразования по алгоритму RSA с последующим хешированием зашифрованного сообщения, а также дополнительное кодирование, используя циклический код и классический полином Хемминга соответственно [4].

Произведен анализ целостности файлов с осажденной информацией после конвертирования в иной формат, который поддерживает Microsoft Word. Стоит отметить, что при конвертации в форматы pdf и xps, информация полностью теряется.

## ЛИТЕРАТУРА

- 1 Урбанович, П.П. Защита информации методами криптографии, стеганографии и обfuscации/ П.П. Урбанович. – Минск: БГТУ, 2016. – 220 с.
- 2 Urbanovich, P., Shutko, N. Theoretical Model of a Multi-Key Steganography System/ P. Urbanovich, N. Shutko. – In: Recent Developments in Mathematics and Informatics, Contemporary Mathematics and Computer Science, V. 2, Chapter 11. – Lublin: Wyd. KUL, 2016. – P. 181-202.
- 3 Шутько, Н.П. Математическая модель системы текстовой стеганографии на основе модификации пространственных и цветовых параметров символов текста/ Н.П. Шутько, Д.М. Романенко, П.П. Урбанович// Труды БГТУ. Серия 6: Физ.-мат. науки и информатика. – Минск: БГТУ. – 2015.– №6. – С. 152-156.
- 4 Урбанович, П.П. Защита информации и надежность информационных систем: пособие для студентов / П.П. Урбанович, Д.М. Шиман. – Минск: БГТУ. – 2014. – 90 с.