

**В. О. Берников**  
(УО «БГТУ», Минск)

**РАЗРАБОТКА СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ  
НА ОСНОВЕ МНОГОКЛЮЧЕВОЙ МОДЕЛИ  
ИНФОРМАЦИОННОЙ СИСТЕМЫ**

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

Были разработаны программное средство и новые методы текстовой стеганографии на основе внедрения цвета и изменения межбуквенного интервала на основе параметра апроша в стеганоконтейнер Microsoft Word. Данное программное обеспечение основано на использовании различных методов предварительного преобразования осаждаемой информации (кодирование, шифрование), а также различных методов внедрения информации в стеганоконтейнер.

Для разработки программного средства 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 и дополнительное кодирование, используя циклический код и классический полином Хемминга соответственно.

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 обфускации / П. П. Урбанович. – Минск: БГТУ, 2016. – 220 с.