# СТЕГАНОГРАФИЧЕСКАЯ СИСТЕМА, ОСНОВАННАЯ НА ИСПОЛЬЗОВАНИИ МЕРЫ СЛОЖНОСТИ ГРАФИЧЕСКОГО ОБРАЗА

*Мельник М.А.*

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Ярмолик В.Н. – д.т.н.,профессор*

Информация – это один из самых ценных товаров в современном мире, а потому очевидно, что ее защита является весьма актуальной для настоящего времени проблемой. С развитием современных информационных технологий число компьютерных преступлений, в том числе хищений конфиденциальной информации, только растет. В таких условиях применение стеганографии является отличным способом защиты от несанкционированного доступа.

Стеганография, как и криптография, представляет собой набор методов, посвященных проблеме скрытой передачи информации. Но в отличие от криптографии, она также скрывает сам факт секретной передачи информации [1].

Общей особенностью всех стеганографических методов является то, что скрываемое сообщение внедряется в некоторый нейтральный объект, который не привлекает внимания. При применении криптографии наличие зашифрованного сообщения само по себе привлекает внимание, а вот в случае стеганографии наличие скрытой информации остается незаметным.

Основной принцип работы стеганографии приведен на рисунке 1. Сообщение – это любая информация, подлежащая скрытой передаче. Контейнер – любой непримечательный объект. Стего-ключ – криптографический ключ, который используют при встраивании сообщения в контейнер.

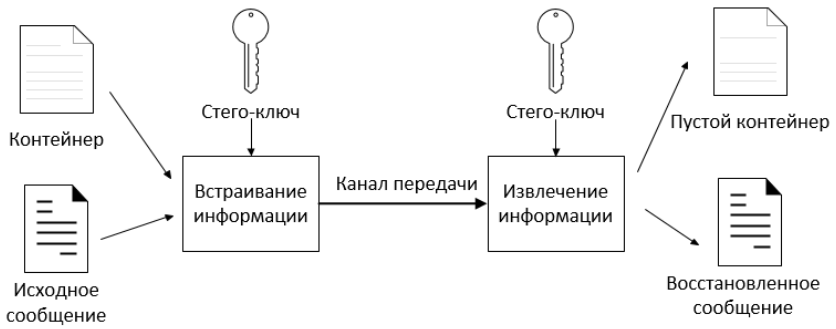


Рисунок 1 – Основной принцип сокрытия данных в стеганографии

Среди всего многообразия стеганографических методов особый интерес представляют алгоритмы встраивания информации в графические контейнеры с целью их последующей передачи. Такой интерес можно объяснить тем, что внесение искажений, которые трудно различимы для среднестатистического человека, не приводит к существенным изменениям этих контейнеров [2].

Среди методов сокрытия информации в графических изображениях наиболее простым и доступным для понимания является **метод LSB**. Суть данного метода заключается в изменении наименьшего из значащих бит в каждом блоке изображения, что не влияет на картину в целом. У данного метода есть один существенный недостаток: он довольно прост в реализации и также прост в обнаружении.

Большим отличием нового **алгоритма BPCS** от уже устоявшегося LSB являлось то, что пока LSB использовал младшие биты картинок и мог поместить данных на 10% от исходного размера контейнера, BPCS пытался вставить данные и в более старшие биты картинки там, где это по-прежнему не будет ухудшать сам контейнер. А объем данных, который можно было внедрять в картинку с использованием BPCS, вырос до 44%. Для определения зашумленных областей данный алгоритм использует *меры сложности* α и β. Но представленные меры не всегда позволяют точно определить зашумленную область, а потому часто при применении данного метода вставка информации может сильно исказить контейнер.

Развитием BPCS стеганографии стал **метод ABCDE**, который использует сразу три меры сложности графического образа для определения шумоподобных блоков. Он отличается большей сложностью, а также и большим количеством внедренной информации: объем данных достигает 50% от объема исходного графического образа.

***Список использованных источников:***

1. Ярмолик, В.Н. Криптография, стеганография и охрана авторского права/ В.Н. Ярмолик, С.В. Ярмолик, С.С. Портянко – 2007. – № 10. – С. 149–167.
2. Википедия [Электронный ресурс]. - Электронные данные. - Режим доступа: https://en.wikipedia.org/wiki/Steganography.