В. А. Бондаренко
Научный руководитель — кандидат технических наук А. А. Гордич
БГЭУ (Минск)

СТЕГАНОГРАФИЧЕСКАЯ ЗАЩИТА ЭКОНОМИЧЕСКОЙ ИНФОРМАЦИИ

Тема исследования является актуальной в настоящее время. Экономика — важнейшая сфера жизни общества. Информация, связанная с производственно-хозяйственной, коммерческой и финансовой деятельностью, является основным регулятором экономических отношений. А так как любая информация может быть найдена, удалена, изменена, то появляется необходимость ее защиты.

Целью настоящей работы является выявление сути стеганографической защиты информации и анализ программ, позволяющих защищать информацию данным способом.

Главная особенность стеганографического способа защиты информации — это маскировка самого факта наличия защищаемой информации. Стегосистема включает методы и средства, используемые для создания скрытого канала передачи информации (стегосообщения). Защищаемая информация помещается в стегоконтейнер. В качестве стегоконтейнера может использоваться информация различного формата. А стегоключи помогают внедрять и извлекать секретную информацию из данного контейнера.

В работе приведены исследования сравнительных характеристик программ ImageSpyer G2, RedJPEG XT, DarkCryptTC и MSU StegoVideo.

ImageSpyer G2 позволяет не только скрыть сам факт наличия секретной информации, но и защитить ее от возможных атак одним из 40 криптоалгоритмов: Cast128, Blowfish, IDEA, Mars, Misty 1, RC2, SAFER, TEAN, 3Way и др. В данной программе используется метод LSB (Least Significant Bit), который заключается в замене последних значащих бит в контейнере изображения на биты скрываемого сообщения. В качестве исходных графических файлов могут использоваться форматы *.bmp, *.jpeg, *.wmf, *.emf, *.tiff [1].

RedJPEG XT позволяет скрывать данные в изображения формата *.jpeg. В программе RedJPEG XT применен механизм внедрения различной информации в графическое изображение. В этой программе используются открытые криптографические алгоритмы AMPRNG rev.1.1, Cartman Cipher 2.DDP.4, а также LZMA-компрессия. Само изображение при этом изменяется незначительно. При извлечении проверяется корректность и целостность архива, правильность ввода пароля [1].

DarkCryptTC поддерживает более сотни различных криптоалгоритмов, включает в себя поддержку собственной системы плагинов, предназначенной

для блочных шифров. Программа содержит генератор паролей и систему уничтожения информации и ключей. Отличительной особенностью является большой список поддерживаемых форматов: *.txt, *.html, *.xml, *.docx, *.odt, *.bmp, *.jpg, *.tiff, *.png, *.jp2, *.psd, *.tga, *.mng, *.wav, *.exe, *.dll.

MSU StegoVideo позволяет встраивать любой файл в видеопоследовательность. Программа слабо искажает видео при встраивании файла, делает возможным извлечение информации даже после сжатия с относительно низким битрейтом. При этом информация защищается паролем [2].

В настоящее время стеганография активно используется для защиты авторских прав, документов от копирования и обработки. Поэтому так важно уметь пользоваться данными программами. При выборе программы следует учитывать формат исходного файла и саму цель сокрытия информации. В результате исследований было установлено, что самой оптимальной программой является DarkCryptTC из-за большого количества поддерживаемых форматов защищаемой информации.

И с т о ч н и к и

1. Стеганография [Электронный ресурс] // PixelLIFE. — Режим доступа: https://pixellife.3dn.ru/publ/mindhack/equipment/steganografija/59-1-0-14. — Дата доступа: 28.03.2020.

2. *Ватолин, Д.* MSU StegoVideo [Электронный ресурс] / Д. Ватолин, О. Петров // Все о сжатии данных, изображений и видео. — Режим доступа: https://www.compression.ru/video/stego_video/. — Дата доступа: 28.03.2020.