А.В. Лопушко, А.А. Пашковская
Научный руководитель — кандидат технических наук А.А.Гордич
БГЭУ (Минск)

ИССЛЕДОВАНИЕ ПРОГРАММ СТЕГАНОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

В настоящее время вопросам обеспечения информационной безопасности в Республике Беларусь уделяется большое внимание. На законодательном уровне принят ряд документов, определяющих концептуальные и практические мероприятия для обеспечения информационной безопасности. Достаточно отметить, что постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 была утверждена Концепция информационной безопасности Республики Беларусь. Поэтому исследование и изучение методов и средств обеспечения информационной безопасности — весьма важная научная и практическая задача. Одним из эффективных методов защиты информации является стеганография.

Стеганография — технология защиты на основе сохранения в тайне самого факта наличия или передачи защищаемой информации. При стеганографии защищаемая информация помещается в контейнер, называемый также стегоконтейнером. В настоящей работе были исследованы пять программ: QuickStego, OpenPuff, Silenteye, Deepsound и Xiao Steganography.

Результаты исследования программы Silenteye следующие. При использовании в качестве пустого контейнера изображения размером 270 Кб, максимальный размер скрываемого файла составляет 512 Кб. Если размер изображения-контейнера составляет 400 Кб, то максимальный размер скрываемого файла также составляет 512 Кб. При этом качество исходного изображения меняется в худшую сторону. В аудиоконтейнерах размером 48 и 460 Кб можно разместить защищаемую информацию размером до 1 Кб. Качество воспроизведения аудиофайлов ухудшается значительно. Во всех случаях возможными типами скрываемых файлов являются: документ Microsoft Word (.doc, .docs), текстовый документ (.txt), файл PDF (.pdf), электронная таблица Microsoft Excel (.xlsx).

Программа Openpuff также позволяет использовать в качестве пустого контейнера изображение. В контейнер размером 270 Кб можно разместить файл (без потери качества изображения), который имеет размер 1 Кб, — доля максимально скрываемого файла информации (от пустого контейнера) составляет 0,37 %. При использовании изображения-контейнера размером 400 Кб максимальный размер скрываемого файла составляет 1 Кб — доля максимально скрываемого файла информации (от пустого контейнера) 0,25 %. Максимальный размер скрываемого файла в аудиоконтейнерах 48 и 460 Кб составляет 1 Кб — доля максимально скрываемого файла информации (от пустого контейнера) соответственно

2,08 и 0,22 %. Качество аудиофайлов ухудшается значительно. Возможные типы скрываемого файла во всех случаях — документ Microsoft Word (.doc, .docs), текстовый документ (.txt), файл PDF (.pdf).

Наряду с этим были проведены исследования программ Deepsound, Xiao Stenography и QuickStego. Данные программы имеют простой пользовательский интерфейс, но не выделяются среди других программ максимальным объемом скрываемой информации или иными характеристиками.

Результаты исследования определили программу, которая является лидером по объему защищаемой информации, вмещаемой файлом-контейнером. Этой программой является Silenteye. Для сокрытия защищаемой информации следует использовать в качестве стегоконтейнера изображение. При этом можно скрывать текстовую информацию размером до 512 Кб. Кроме очевидных преимуществ в объеме скрываемой информации Silenteye обладает наиболее понятным пользователю интерфейсом, и информация может быть защищена паролем. Однако следует отметить, что по уровню защиты информации Silenteye все же уступает приложению OpenPuff, которое, в свою очередь, использует не один, а три уровня защиты данных паролем. Также Silenteye предоставляет возможность извлекать из стегоконтейнера не только свои стеганографические файлы, но и файлы, полученные в сторонних приложениях.