**СТЕГАНОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ**

*Белорусский государственный университет информатики и радиоэлектроники*

*г. Минск, Республика Беларусь*

*Губский М. Д.*

*Стройникова Е. Д. – ассистент кафедры информатики*

Во все времена ценность информации была высока. На протяжении столетий люди использовали всевозможные приемы защиты важных данных от несанкционированного доступа, всякий раз придумывая все более сложные и надежные. Как правило, это были криптографические методы. Но порой лишь зашифровать необходимые сведения являлось недостаточным. Для усиления защиты использовались методы сокрытия информации — стеганографические методы.

На сегодняшний день существует множество способов сокрытия данных. Одним из простых в реализации, но не таким простым в обнаружении, является стеганография.

Стеганография (греч. — тайнопись) — наука, изучающая передачу и хранение информации при сокрытии самого факта ее существования. Уже в IV в. до н. э. использовали стеганографию, чтобы передавать важные сообщения. Так, например, наносилось необходимое сообщение на обритую голову раба. Когда волосы отрастали, он отправлялся к адресату, который, сбрив голову, считывал сообщение.

За время своего существования стеганография претерпела множество изменений и дополнений. На современном этапе сформировалось три направления: классическая, компьютерная, цифровая.

Классическая стеганография — исторически сложившиеся методы сокрытия сведений, которые применяются в повседневной «реальной» жизни, другими словами, некомпьютерные методы. Например, по одной из версий древние шумеры наносили сообщения на глиняные дощечки, после покрывали их слоем глины и вновь наносили надпись, но уже не секретную. Также можно вспомнить запись сообщений на боковой стороне колоды карт, «жаргонные шифры», акростихи и т.д.

Компьютерная стеганография, как видно из названия, включает в себя методы, основанные на особенностях конкретной платформы компьютеров, а также свойствах компьютерных форматов данных. Примерами компьютерных стеганографических методов являются:

* Метод с использованием регистра букв. Его суть заключается в том, что каждый символ секретного сообщения переводится в байт-код. Затем, у каждого символа скрывающего текста, которому соответствует единица сообщения, следует поменять регистр. Таким образом, можно зашифровать максимум N/8 символов, где N— количество символов в скрывающем тексте.
* Метод, использующий специфику файловых систем. Как известно, операционные системы для хранения файлов выделяют целое число блоков (для удобства адресации). Соответственно, для хранения маленьких файлов выделяется лишняя память, в которой как раз можно хранить необ-ходимую информацию.
* Использование зарезервированных полей форматов данных, также является отличным методом сокрытия сведений. Метод полагается на то, что большинство мультимедийных форматов имеют поля расширения, не использующиеся программой, как правило, они заполнены нулевой инфор-мацией.

На сегодняшний день самым важным и наиболее используемым направлением является цифровая стеганография. Это направление известно тем, что внедряет и скрывает необходимую информацию в цифро-вые объекты. К сожалению, это направление накладывает некоторые обязательства, такие как сохранение целостности и аутентичности файла, поэтому обычно в качестве контейнеров (хранилищ данных) используют медиафайлы. Существуют следующие алгоритмы встраивания скрываемой информации:

* работающие с цифровым сигналом напрямую (метод LSB);
* внедрение скрытой информации (наложение секретного изображение, аудиофайла, текста поверх оригинала; часто используется для внедрения цифровых водяных знаков);
* использование форматов файлов (к примеру, запись в метаданные).

Одним из самых известных алгоритмов встраивания является метод LSB (Least Significant Bit — англ. наименьший значащий бит). Он основан на замене последних, незначащих бит в контейнере (графическом, аудио, видеофайле) на биты секретного сообщения. Метод опирается на низкий порог чувствительности че-ловеческих органов. Например, изменение в 8-битном изображении двух последних бит приводит к измене-нию в цвете максимум на 3 бита, такие градации не отображают многие программы (считая не существен-ным), не говоря уже о человеческом глазе.

В общем случае система маскирования имеет следующий вид (рис 1):

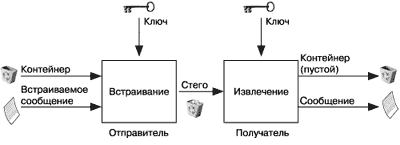


Рис. 1 — Процесс сокрытия данных с помощью цифровой стеганографии

Где

* Контейнер — любая побочная информация (аудио, видео, изображение), служащая для сокрытия секретных сообщений.
* Встраиваемое сообщение — секретные данные, нуждающееся в сокрытии.
* Встраивание — внедрение сообщения в контейнер, происходит на компьютере с использованием одного из методов стеганографии и ключа.
* Стего — стеганографический канал, канал передачи внедренного сообщения.
* Извлечение – получение секретного сообщения с использованием ключа.
* Ключ — сведения, необходимые для сокрытия/получения информации. Ключи бывают секретные и открытые. Системы с секретным ключом использует его как для встраивания, так и для извлечения. С открытым ключом — только для встраивания, для извлечения используется независимый ключ.

В ходе исследования была произведена оценка устойчивости метода LSB с использованием изображе-ний на языке Python. Процесс внедрения производился приведенным выше способом (рис. 1). В качестве кон-тейнера пользовалось изображение формата PNG. Для примера секретным сообщением было выбрано «success\_1». Вмонтирование сведений производилось посредством резервирования 2 последних бит каждого цвета, из которых состоит пиксель изображения в системе RGB. Для работы с изображениями и их трансфор-мацией использовался модуль PIL языка Python. Анализ производился по двум параметрам: незаметность из-менений контейнера при добавлении данных и валидность извлеченного сообщения. Примеры работы про-граммы в зависимости от вида трансформации приведены в таблице 1.

Таблица 1. Оценка устойчивости LSB в зависимости от метода трансформации контейнера.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Вид трансформации | | Без трансформации | EXTENT | AFFINE | PERSPECTIVE |
| Ввод | | success\_1 | | | |
| Вывод | 1 | success\_1 | ÿÿÿÿÿÿÿÿÿ | ÿÿÿÿÿÿÿÿÿ | ÿÿÿÿÿÿÿÿÿ |
| 2 | ÿÿÿü8Àõý@ | ÝXØÙ\Ü×Ìÿÿ | ÝÇqÇqÇ |
| 3 | qV6Ï\_?ÿÿÿ | ß}÷ ß}÷ ß}÷ | ÿÿÿýÇqÇ |
| Видимость | | — | — | — | — |

Где

* EXTENT — извлекает область и помещает в новое изображение с данным размером (использовался как resize).
* AFFINE — аффинное преобразование.
* PERSPECTIVE — перспективное преобразование.

Полученные данные показали, что невооруженным глазом определить наличие скрытого сообщения невозможно. Однако, быть уверенным, что сообщение будет доставлено в целости и сохранности, нельзя. Та-ким образом метод LSB является не устойчивым ко всякого рода трансформациям контейнера, т.е. метод хо-рош лишь при использовании статических контейнеров (не подверженных изменениям).

В заключение хотелось бы отметить, что стеганография не является должной заменой криптографии и полагаться только на нее не стоит. Но в сочетании с криптографическими методами она становится еще од-ним рубежом защиты вашей бесценной информации.

Список использованных источников:

1. Грибунин, В.Г. Цифровая стеганография / Оков И.Н., Туринцев И.В. – М.:СОЛОН-Прессб 2002., — 272 стр.
2. Рябко, Б. Я. Основы современной криптографии и стеганографии / Фионов А. Н. — 2-е изд. — М.: Горячая линия — Телеком, 2013. — 232 с.
3. CitForum [Электронный ресурс]. — Электронные     данные.  — Режим доступа: http://citforum.ru