**Исследовательская работа на тему**

**«Стеганография»**

Выполнил: Шульгин Александр

Студент группы ПО-23

Ливенский филиал ОГУ им. И.С.Тургенева

Ливны
2019

**Введение**

Задача защиты информации от несанкционированного доступа решалась во все времена на протяжении истории человечества. Уже в древнем мире выделилось два основных направления решения этой задачи, существующие и по сегодняшний день: криптография и стеганография. Целью криптографии является скрытие содержимого сообщений за счет их шифрования. В отличие от этого, при стеганографии скрывается сам факт существования тайного сообщения.

Слово «стеганография» имеет греческие корни и буквально означает «тайнопись». Исторически это направление появилось первым, но затем во многом было вытеснено криптографией. Тайнопись осуществляется самыми различными способами. Общей чертой этих способов является то, что скрываемое сообщение встраивается в некоторый безобидный, не привлекающий внимание объект. Затем этот объект открыто транспортируется адресату. При криптографии наличие шифрованного сообщения само по себе привлекает внимание противников, при стеганографии же наличие скрытой связи остается незаметным.

Какие только стеганографические методы не использовали люди для защиты своих секретов. В прошлом веке широко использовались так называемые симпатические чернила, невидимые при обычных условиях. Скрытое сообщение размещали в определенные буквы невинных словосочетаний, передавали при помощи внесения в текст незначительных стилистических, орфографических или пунктуационных погрешностей. С изобретением фотографии появилась технология микрофотоснимков, успешно применяемая Германией во время мировых войн. Крапление карт шулерами – это тоже пример стеганографии.

Развитие средств вычислительной техники в последнее десятилетие дало новый толчок для развития компьютерной стеганографии. Появилось много новых областей применения. Сообщения встраивают теперь в цифровые данные, как правило, имеющие аналоговую природу. Это – речь, аудиозаписи, изображения, видео. Известны также предложения по встраивании информации в текстовые файлы и в исполняемые файлы программ.

Существуют два основных направления в компьютерной стеганографии: связанные с цифровой обработкой сигналов и не связанные. В последнем случае сообщения могут быть встроены в заголовки файлов, заголовки пакетов данных. Это направление имеет ограниченное применение в связи с относительной легкостью вскрытия и/или уничтожения скрытой информации. Большинство текущих исследований в области стеганографии, так или иначе, связаны с цифровой обработкой сигналов. Это позволяет говорить о цифровой стеганографии.

Стеганография – быстро и динамично развивающаяся наука, использующая методы и достижения криптографии, цифровой обработки сигналов, теории связи и информации.

**ОБЩИЕ СВЕДЕНИЯ О СТЕГАНОГРАФИИ**

**Основные понятия и определения стеганографии**

Несмотря на то, что стеганография как способ сокрытия секретных данных известна уже на протяжении тысячелетий, компьютерная стеганография - молодое и развивающееся направление.

Как и любое новое направление, компьютерная стеганография, несмотря на большое количество открытых публикаций и ежегодные конференции, долгое время не имела единой терминологии.

**Стеганографическая система или стегосистема** - совокупность средств и методов, которые используются для формирования скрытого канала передачи информации.

**Положения и требования стегосистемы:**

1. Аутентичность и целостность файла;
2. Предположения, что противник знает все стегометоды;
3. Необходимое сохранение всех свойств открыто передаваемого файла при внесении в него секретного сообщения и ключа;
4. Сложная вычислительная техника при извлечении сообщения противником.

В качестве данных может использоваться любая информация: текст, сообщение, изображение и т. п.

В общем же случае целесообразно использовать слово "**сообщение**", так как сообщением может быть как текст или изображение, так и, например, аудиоданные. Далее для обозначения скрываемой информации, будем использовать именно термин сообщение.

**Содержимое стегосистемы:**

**Контейнер** - любая информация, предназначенная для сокрытия тайных сообщений.

**Пустой контейнер** - контейнер без встроенного сообщения; **заполненный контейнер** или **стего - контейнер**, содержащий встроенную информацию.

**Встроенное (скрытое) сообщение** - сообщение, встраиваемое в контейнер.

**Стеганографический канал** или просто **стегоканал** - канал передачи стего.

**Стегоключ** или **просто ключ** - секретный ключ, необходимый для сокрытия информации. В зависимости от количества уровней защиты (например, встраивание предварительно зашифрованного сообщения) в стегосистеме может быть один или несколько стегоключей.

**Методы стеганографии:**

Большинство методов компьютерной стеганографии базируется на двух принципах.

Первый состоит в том, что файлы, которые не требуют абсолютной точности (например, файлы с изображением, звуковой информацией и пр.), могут быть до определенной степени видоизменены без потери функциональности.

Второй принцип основан на отсутствии специального инструментария или неспособности органов чувств человека надежно различать незначительные изменения в таких исходных файлах.

**Основные задачи стеганографии**

1. Защита конфиденциальной информации от несанкционированного доступа;

2. Преодоление систем мониторинга и управления сетевыми ресурсами;

3. Камуфлирования программного обеспечения;

4. Защита авторского права на некоторые виды интеллектуальной собственности.

**Дестеганография**

Дестеганография – метод выявления секретной информации

Простые методы дестеганографии заключаются в следующем:

для начала нужно найти все места возможных закладок инородной информации, которые допускает формат файла-контейнера.

Далее требуется извлечь данные из этих мест и проанализировать их свойства на соответствие стандартным значениям.

**Стеганография**

Один из самых увлекательных и эффективных методов сокрытия данных, которые использовались за всю историю человечества. В настоящее время компьютерная стеганография продолжает развиваться. Главной причиной этого процесса является лавинообразное развитие компьютерной сети общего пользования Internet, в том числе такие нерешенные противоречивые проблемы Internet, как защита авторского права, защита прав на личную тайну, организация электронной торговли, противоправная деятельность хакеров, террористов, принятые в ряде стран ограничения на использование сильной криптографии.

Чем больше человек знает о методах стеганографии, тем больше у него шансов не попасть впросак.

**ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА:**

1. Автор, автор 2, автор 3. Наименование статьи. Minnesota Technolog, Fall 2004.

2. Marvel L. Image Steganography for hidden communication. PhD Thesis. Univ.of Delaware, 1999. 115p.

3. <http://www.citforum.ru/internet/securities/stegano>

4. Цифровая стеганография / Сост. Грибунин В.Г., Оков И.Н., Туринцев И.В.

Безопасность, криминалистика, промышленный шпионаж - <http://www.phreaking.ru/showpage>

5. Скрытая утечка информации –

6. <http://www.cio-world.ru/bitrix/php_interface>

7. Конахович Г. Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. К.: «МК-Пресс», 2006. – 280 стр., ил.