Глава I.

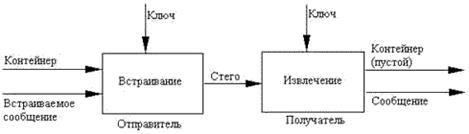
Основы стеганографии

Стеганография – это искусство и наука о способах передачи (хранения) скрытой информации, при которых скрытый канал организуется на базе и внутри открытого канала с использованием особенностей восприятия информации (Аграновский А.В. Стеганография, цифровые водяные знаки и стеганоанализ. М., 2009. С.26). Для этой цели используются различные приёмы. Это может быть:

* маскировки скрытой информации в протоколе
* полное сокрытие факта существования скрытого канала связи
* создание трудностей для обнаружения, извлечения или модификации передаваемых скрытых сообщений внутри открытых сообщений-контейнеров

В стеганографии можно выделить несколько основных понятий. Это контейнер, сообщение и ключ.

Контейнер – это несекретные данные, уже в которых сокрыта определенная информация (там же, с.27). Имеет место быть замена этого термина на название “стего”. Контейнер может быть пустым или заполненным. Пустой контейнер – контейнер, в котором пока отсутствует скрытые данные. Заполненным называют контейнер, который содержит скрытые данные. Пространством сокрытия называются участки контейнера, в которых стеганосистема может скрыть информацию. Это могут биты, поля и так далее. Используемое пространство сокрытия представляет собой совокупность областей пространства сокрытия, в которых действительно произошло сокрытие в процессе работы стеганосистемы.

Сообщение – как раз та информацию, которую нам необходимо скрыть (там же). Всевозможные сообщения объединяются в пространство сообщений. Сообщения содержатся в контейнерах. С сообщениями возможны две операции: внедрение и извлечение. Внедрение (сокрытие) – использование прямого преобразования к определенным сообщению, контейнеру и ключу (смотри ниже). Под извлечением понимают действие, обратное тому, что производилось при внедрении.  
 И последнее определение – ключ. Он известен только законному пользователю, и определяет конкретный вид алгоритма сокрытия.

Стеганографическая система – это совокупность контейнеров, сообщений, ключей и связывающих их преобразований (там же, с.28).

Сторону стеганографии, пытающуюся раскрыть стеганографическую систему называют стеганоаналитиком. Задача стеганоаналитика состоит в раскрытии стеганографической системы и определения самого сообщения. Под раскрытием (взломом принято понимать нахождения её уязвимости, с помощью которой можно определить факт сокрытия информации в контейнере и возможность доказать это с высокой степенью достоверности.

Процесс стеганоанализа можно разделить на два действия:

1. Определение наличия сообщения в контейнере
2. Извлечение содержания скрытого сообщения

Попытка определить наличие сообщения и его смысла называют атакой на стеганографическую систему. Данные атаки делятся на несколько классов (там же, с.29):

* Атаки со знанием модифицированного контейнера, в данном случае стеганоаналитик обладает только модифицированным контейнером. С его помощью он пытается определить наличие скрытого сообщения. Этот вид атак – базовый из всех, по которым оцениваются стеганосистемы.
* Атаки со знанием немодифицированнного контейнера возможны в случае, когда стеганоаналитик также обладает способностью узнавать, какой именно немодифицированный контейнер был использован для сокрытия сообщения. Данная атака определяет возможность определения факта скрытия сообщения в дальнейшем в зависимости от наличия однажды перехваченного контейнера и раскрытого сообщения.
* Атаки с выбором сообщения, в этом случае стеганоаналитик имеет возможность указывать, какие именно сообщения будут сокрыты, но при этом не имеет возможности указать контейнер, который будет для этого использоваться. Устойчивость к этому классу атак характеризует устойчивость самой системы к перехвату и отслеживанию сообщений, посланных с использованием одного и того же контейнера. Данный вид атак иногда также позволяет определить тип применённой стеганографической системы.
* Атаки с выбором контейнера, так же как и предыдущие позволяют определить стойкость стеганосистемы к раскрытию в случае повторного использования одного и того же сообщения с различными контейнерами.
* Атаки по подмене и имитации не призваны определить факт наличия сообщения или извлечь его. Их используют для модификации скрытой информации, либо имитации такой передачи.
* Атаки по противодействию передаче информации используют для уничтожения скрытой информации и снижения пропускной способности каналов скрытой передачи данных.

Стеганоаналитик, не модифицирующий доступные ему для анализа данные, носит название пассивного нарушителя(там же, с.30). Стеганоаналитик, который может вносить изменения в передаваемые по каналу данные, называется активный нарушитель(там же). Атаки по подмене, имитации и противодействию характерны только для активного нарушителя. Остальные виды атак присущи только пассивным нарушителям.

Человечеству были известны способы скрывать информацию и до изобретения компьютеров.

Уже в V веке до н.э. люди умели оправлять скрытые сообщения. Так как в то время было распространено рабовладение, то для пересылки использовались рабы. Им брили голову, писали на ней послание, ждали когда волосы отрастут обратно, а затем отправляли его к адресату.

В Китае военные сообщения писались на кусках тончайшего шелка и закатывались в маленький шар, который глотал посыльный. В Риме и Греции сообщения вырезались на кусочках древесины, которые потом опускались в воск, чтобы закрыть запись.

За свою историю человечество изобрело множество различных способов скрывать сообщения. Наиболее известный и давно использующийся – симпатические чернила. Их особенность в том, что после написания они исчезают. Сделать их обратно видимыми можно только путем специальной обработки. Данный метод применялся в Древнем Риме, на Древнем Востоке, России и так далее.

Широкое распространение и применение в стеганографии получил метод микроточки. Под микроточкой понимают уменьшенное более чем в сто раз фотоизображение обычного документа. Существует две разновидности микроточки: обычная (0,8 мм в диаметре) и ультра-микроточка (менее 0,2 мм в диаметре).

Но не будем путать стеганографию и криптографию. Хоть между ними существует только одно отличие, но оно весьма важное.

Перед тем, как обозначать его, разберемся, что такое криптография. Это наука о математических методах обеспечения конфиденциальности и аутентичности информации[[1]](#footnote-1). Чаще всего результатом данных методов является зашифрованное послание.

В это и состоит отличие криптографии от стеганографии. Информацию, которую скрывают первой наукой, может увидеть любой человек в виде шифра, однако лишь тот, кто знает ключ, сможет извлечь её. Стеганография, в отличие от криптографии, скрывает сам факт передачи данных как таковой. Ведь чаще всего их переносчиками являются самые обыкновенные и ничем не примечательные изображения, документы и так далее.

1. Научное вики сообщество [Электронный ресурс] /Криптография: http://ru.science.wikia.com/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F [↑](#footnote-ref-1)