Введение

В настоящее время большой объем данных передается в сетях связи между пользователями. В ряде случаев требуется спрятать факт передачи конфиденциальных данных от третьих лиц. Например, известные каналы связи могут подвергнуться DDoS-атаке, но тайный канал останется незамеченным для злоумышленника. В другой ситуации злоумышленник под видом обычных электронных писем может скрытно переслать охраняемую базу данных клиентов, которая предназначена только для внутреннего пользования сотрудниками кампании. То есть, имитируя безобидную переписку, возможно создание потайного канала связи, что может нанести существенный экономический или репутационный ущерб.

Соответственно, возникают задачи создания новых, контроля существующих и противодействия использованию методов скрытой передачи данных. Подобные задачи решаются в рамках науки *стеганографии*. В общем случае стеганография — это наука, изучающая методы сокрытия факта передачи секретного сообщения. Одним из примеров применения является встраивание паспортных данных покупателя в платный контент (файл). Если покупатель начнет самостоятельное распространение такого файла без разрешения правообладателя, то при обнаружении «пиратской копии» можно извлечь встроенные паспортные данные и выявить нарушителя.

Обратной к внедрению задачей является обнаружение. Такая задача решается в рамках *стегоанализа*. Стегоанализ, например, применяется службами безопасности банков для контроля и пресечения распространения конфиденциальной информации (например, базы данных клиентов). Очевидно, что количество данных, передаваемых по Сети, велико и требуются методы автоматизированного анализа сетевого трафика, выявляющих подобные утечки.

Известны исторические случаи применения стеганографии. Например, в Древней Греции для передачи секретного сообщения через границу использовали раба. Его голову брили и наносили татуировку с тайным посланием. Когда волосы отрастали, то его отправляли к месту назначения. На границе между государствами проводился обыск, но никто из пограничников не догадывался проверить голову. Далее раб приходил на место назначения, где еще раз брили голову и читали секретное сообщение.

В современной истории известно использование микрофотографий. Так изображение может быть отмасштабировано в типографскую точку, которая после вклеивалась в обычное письмо или книгу. При внешнем осмотре эта точка ничем не выдавала себя. Однако при многократном увеличении получалось воспроизвести изображение размером с лист формата А4.

Другой пример использования стеганографии — отправка тайных писем В.И. Лениным, который писал Н.Н. Крупской молоком на белой бумаге. Такое письмо выглядит как обычный белый и чистый лист бумаги. Тем не менее при нагревании, например, над пламенем свечи молоко сворачивалось (коагулировало), меняло цвет и текст письма становился видимым.

Вопросами стеганографии занимается множество отечественных и зарубежных ученых. Среди них известны отечественные (С.В. Беззатеев, С.В. Белим, В.Г. Грибунин, В.М. Довгаль, Г.А. Кабатянский, Г.Ф. Конахович, В.И. Коржик, Р.В. Мещеряков, И.Н. Оков, А.Ю. Пузыренко, Б.Я. Рябко, И.В. Туринцев) и зарубежные ученые (C. Cachin, X. Chen, C. Collberg, J. Fridrich, A. Ker, G. Simmons, C. Thomborson, X. Wang, L. Xiang, C. Yang). Проводятся международные конференции и семинары, посвященные данной проблеме, а также публикуются статьи в высокорейтинговых журналах. Министерство цифрового развития, связи и массовых коммуникаций ежегодно выделяет финансирование в виде грантов (гос. заданий) на исследования, направленные на анализ существующих и разработку новых методов стеганографии.

Настоящая монография посвящена цифровой стеганографии, где в качестве носителя скрытой информации выступает цифровой объект данных — файл. Рассмотрены вопросы обеспечения контроля за распространением данных по Интернету. Собраны последние достижения и нерешенные проблемы в области защиты данных.

Материал ориентирован на начинающих исследователей, магистрантов и аспирантов, которые погружаются в данную тему. Одна из глав содержит рекомендации по проведению эксперимента и обработке его результатов.