

# ЗАЩИТА АУДИОДАНЫХ С ПОМОЩЬЮ ВСТРАИВАНИЯ В НИХ ДОПОЛНИТЕЛЬНОЙ СПЕЦИАЛЬНОЙ ИНФОРМАЦИИ

Мирончик В.В., Зельманский О.Б.

Научный руководитель: канд. техн. наук Зельманский О.Б.

Белорусский государственный университет информатики и радиоэлектроники, Беларусь

E-mail: Violet-88@tut.by

*Аннотация* — Рассмотрены методы применения компьютерной стеганографии для защиты авторских прав и интеллектуальной собственности. Приведен пример применения стеганографии для защиты аудиоданных.

## 1. Введение

Современный прогресс в области глобальных компьютерных сетей и средств мультимедиа привел к разработке новых методов, предназначенных для обеспечения безопасности передачи данных по каналам телекоммуникаций и использования их в необъявленных целях. Эти методы, учитывая естественные неточности устройств оцифровки и избыточность аналогового видео или аудио сигнала, позволяют скрывать сообщения в компьютерных файлах (контейнерах). В настоящее время существует достаточно много различных компьютерных методов встраивания сообщений в аудиоданные. Причем, в отличие от криптографии, данные методы скрывают сам факт передачи информации [1].

## 2. Основная часть

В основе применения компьютерной стеганографии лежит неспособность органов чувств человека различать незначительные изменения в цвете изображения или качестве звука, что особенно легко использовать применительно к объекту, несущему избыточную информацию. При обработке звука учитывается так называемое окно слышимости человека. Органы слуха человека звуковые частоты воспринимают по-разному. Верхняя граница окна слышимости соответствует оглушительному звуку, соседствующему с болевым ощущением. Нижняя граница определяется порогом слышимости. Кроме того, человек не может однозначно регистрировать на слух незначительные изменения интенсивности звука. Стеганографические алгоритмы обработки звука строятся с таким расчетом, чтобы максимально использовать окно слышимости и другие свойства речевых сигналов (тембр, скорость и т.д.), незначительные изменения которых человек различить не может [2].

В настоящее время методы компьютерной стеганографии развиваются по двум основным направлениям:

— методы, основанные на использовании специальных свойств компьютерных форматов;

— методы, основанные на избыточности аудио и визуальной информации.

Недостатками первой группы методов являются низкая степень скрытности и возможность передачи небольших ограниченных объемов информации. Вторая группа методов лишена этих недостатков и может применяться для скрытой передачи изображения товарной марки, регистрационных номеров и т.п. Благодаря этому, системы стеганографии активно используются для решения задачи защиты авторского права на интеллектуальную собственность. На компьютерные графические изображения наносится специальная метка, которая остается невидимой для

глаз, но распознается специальным программным обеспечением. Такое программное обеспечение уже используется в компьютерных версиях некоторых журналов. Данное направление стеганографии предназначено не только для обработки изображений, но и для обработки файлов с аудио- и видеoinформацией и призвано обеспечить защиту интеллектуальной собственности. Однако, за счет введения дополнительной информации искажаются статистические характеристики цифровых потоков. Это требует снижения компрометирующих признаков применения стеганографии за счет коррекции статистических характеристик.

Компьютерное пиратство — это несанкционированное правообладателем копирование, распространение или использование данных в личных целях. Применение компьютерной стеганографии позволяет установить метку, содержащую информацию о реальном правообладателе на данный информационный продукт, но не защищает от несанкционированного копирования или использования.

Предлагается наряду с метками применить компьютерную программу, которая позволяет защитить объект от копирования. Суть данной программы заключается в том, что при несанкционированном копировании без использования специального программного обеспечения, доступного только правообладателю, она удаляет защищаемый объект с предполагаемого места копирования, но оставляет на исходном носителе. Тем самым будет обеспечена защита от несанкционированного копирования без ущерба для защищаемого объекта.

## 3. Заключение

Таким образом, для обеспечения защиты авторских прав на мультимедийные объекты звукозаписывающим компаниям целесообразно использовать совместно со специальными метками дополнительную программу, которая обеспечит защиту от несанкционированного копирования аудиоинформации, без вреда для нее.

## 4. Список литературы

- [1] Коначович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Коначович, А.Ю. Пузыренко. — К.: МК-Пресс, 2006. — 288 с.
- [2] Соколов А.В. Защита от компьютерного терроризма / А.В. Соколов, О.М. Степанюк. — СПб.: БХВ-Петербург Арлит, 2002. — 496 с.

## AUDIODATA PROTECTION BY EMBEDDING ADDITIONAL SPECIAL INFORMATION

Mironchik V.V., Zelmanski O.B.

Scientific adviser: Zelmanski O.B.

Belarusian State University of Informatics and Radioelectronics, Belarus

*Abstract* — Methods of a computer steganography, to protect a copyright and an intellectual property, were considered. A steganography application for protection of audiodata was given.