

УПРАВЛЕНИЕ ЗАЩИТОЙ ИНФОРМАЦИИ НА ОСНОВЕ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ

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.

Можно выделить две причины популярности исследований в области стеганографии в настоящее время: ограничение на использование криптографических средств в ряде стран мира и появление проблемы защиты прав собственности на информацию, представленную в цифровом виде. Первая причина повлекла за собой большое количество исследований в духе классической стеганографии (то есть скрытия факта передачи информации), вторая — еще более многочисленные работы в области так называемых водяных знаков.

Цифровой водяной знак (ЦВЗ) — специальная метка, незаметно внедряемая в изображение или другой сигнал с целью тем или иным образом защищать информацию от несанкционированного копирования, отслеживать распространение информации по сетям связи, обеспечивать поиск информации в мультимедийных базах данных.

Слово стеганография в переводе с греческого буквально означает тайнопись (steganos - тайна, секрет; graphy - запись) [1].

Стеганография - это наука о способах передачи (хранения) скрытой информации, при которых скрытый канал организуется на базе и внутри открытого канала с использованием особенностей восприятия информации, причем для этой цели могут использоваться такие приемы, как [2]:

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

Наблюдаемый в настоящее время интерес к стеганографии, как совокупности методов сокрытия информации, возник в большой мере благодаря интенсивному внедрению и широкому распространению средств вычислительной техники во все сферы деятельности человека. В рамках вычислительных сетей возникли достаточно широкие возможности по оперативному обмену различной информацией в виде текстов, программ, звука, изображений между любыми участниками сетевых сеансов независимо от их территориального размещения. Это

позволяет активно использовать все преимущества, которые дают стеганографические методы защиты.

Стеганография тайно передает одну информацию в другой. При этом сам факт передачи секрета скрывается. Поскольку объем чисто текстовой информации в каналах связи и интернете постоянно растет (текущие новости, электронная почта, реклама, спам и пр.), есть надежда передавать секретные сообщения прямым их внедрением в несущие тексты, пусть с невысокой скоростью, но незаметно. Этим и занимается текстовая стеганография. Ей важно сохранить текст-носитель безобидным и осмысленным.

В настоящее время существует множество методов компьютерной стеганографии. В научной работе отмечалось многообразие методов текстовой стеганографии, а также раскрывалась сущность других методов данного вида стеганографии, таких как:

- метод невидимых символов;
- метод изменения межстрочных интервалов;
- метод изменения интервала табуляции;
- метод изменения регистра символа.

Синтаксические методы текстовой стеганографии производят сокрытие информации в таких элементах текста, изменение или модификация которых, как правило, незначительно преобразует исходный текст (исключением является метод изменения регистра букв) и не вызывает подозрений у стороннего читателя.

Алгоритмы текстовой стеганографии не являются единственно возможными, т.к. они проводят встраивания не во всех элементах текстового документа, изменение или модификация которых не приводит к значительному преобразованию исходного текста. Такими ранее неиспользуемыми параметрами документа могут выступать цвет символов, масштаб символов, апрош, кернинг.

Таким образом, можно предложить к использованию следующие новые синтаксические методы:

- метод изменения цвета символов;
- метод изменения масштаба символов;
- метод изменения апроша [2];
- метод изменения цветовых координат символов.

На основе одного из этих методов, была разработана авторская программа "Sword", реализующая сокрытие данных за счет изменения цвета символов в заданном документе [3]. Целью программы стала автоматизация процесса скрытия, которое является крайне трудоемким при реализации вручную. Разработанная программа позволяет свести весь процесс скрытия данных к выбору необходимого документа и вводу скрываемого текста. В тоже время предусмотрена возможность тонкой настройки различных параметров: задание используемых цве-

тов, режима скрытия, выбор кодировки символов, использования шаблонов для скрытия, подсветка используемых для скрытия символов и др.). Помимо скрытия в программе реализована возможность извлечения скрытых данных на основе заданных параметров, а также их удаление из документа.

Представленная программа внедрена в учебный процесс на кафедре ИСиТ, а также зарегистрирована в Национальном Центре интеллектуальной собственности [4].

ЛИТЕРАТУРА

- 1 Хорошко, В. А. Методы и средства защиты информации / В. А. Хорошко, А. А. Чекатков. — Киев: Юниор, 2006. — 504 с.
- 2 Применение текстовой стеганографии для защиты и передачи информации / П. П. Урбанович [и др.] // Автоматический контроль и автоматизация производственных процессов: материалы конференции. — Минск, 2009. — С. 67-69.
- 3 Urbanovich, N. The use of steganographic techniques for protection of intellectual property rights / N. Urbanovich, V. Plaskovitsky // New Electrical and Electronic Technologies and their Industrial Implementation. — 2011. — P. 147-148.
- 4 Sword v.1.0: свидетельство о регистрации компьютерной программы № 383 / Н. П. Урбанович, В. А. Пласковицкий; заявитель и правообладатель УО «Бел. гос. технол. ун-т». — № С20110095; заявл. 07.12.2011; зарегистр. 04.01.2012. — [1] с.

УДК 008:379.85

Дж. Н.Машокиров, асп. (Вильнюсский технический университет им. Гедиминаса, Республика Литва, г. Вильнюс)

РАЗРАБОТКА СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В МЕНЕДЖМЕНТЕ ТУРИЗМА И ТУРИСТИЧЕСКИХ ОРГАНИЗАЦИЯХ

Понятие, процесс разработки и особенности система поддержка принятий решений. Управленческое решение представляет собой закономерный результат деятельности руководителя и реализуется в форме директивного целенаправленного воздействия на объект менеджмент туризма [1, с.25].

Система поддержка принятий решений в менеджмент туризм — акт целенаправленного изменения ситуации, разрешения проблемы, вариант воздействия на систему и процессы, происходящие в ней. Система поддержка принятий решений предполагают действия руководства, ведущие к разрешению противоречия и изменению ситуации. Любое решение основывается на анализе данных, характеризующих