Работа может быть использована в учебных заведениях во внеклассной работе по изучению экспертизы качества потребительских товаров.

СИСТЕМЫ УПРАВЛЕНИЯ СОДЕРЖИМЫМ САЙТА

Бикбаев А.В., Прокофьева С.В.

ФГОУ ВПО «Башкирский государственный аграрный университет», Уфа, e-mail: arnomag6@gmail.com

Система управления содержимым сайта (Content Management System – CMS) является платформой и основой при написании сайта любой сложности; иными словами это пакет шаблонов, тестовых и графических наполнителей, которые предоставляют пользователю интерфейс при работе с сайтом.

Целью исследования являлось выявление оптимальной с точки зрения начинающего web-мастера системы для создания сайта. С этой целью были определены следующие критерии оценки CMS: наличие и удобство визуального редактора, безопасность и борьба со спамом, документация на русском языке, шаблоны оформления, работа с изображениями, экспорт/импорт данных, возможности комментирования материалов, использование XML-RPC и RSS, многопользовательские блоги, лагины, виджеты/блоки, кодировки, комментирование и ряд других. Также было важно, чтобы система была бесплатной и в тоже время производительной и функциональной.

В соответствии с приведенными выше характеристиками были рассмотрены распространенные CMS: «Joomla!», «Drupal», «Wordpress». По ряду критериев CMS «Joomla!» оказалась более понятной, функциональной, укомплектованной, что в итоге сказалось на общей оценке.

После выбора CMS, на ее основе был создан информационный сайт «Зерновые культуры», предоставляющий сведения о выращивании зерновых культур в республике Башкортостан, о хозяйствах, специализирующихся на растениеводстве, об итогах испытания зерновых культур и предложениях о реализации семян.

Таким образом, в ходе исследования были выявлены сравнительные характеристики систем управления содержимым сайта, проведена оценка нескольких систем и на платформе одной из них создан информационный ресурс. Материалы по итогам исследования могут быть использованы в учебных целях.

ЗАЩИТА ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ СТЕГАНОГРАФИИ

Боброва Е.М., Борисова С.Н.,

ГОУ ВПО «Пензенская государственная технологическая академия», Пенза, e-mail: iis@pgta.ru

Методы стеганографии (*стеганогра́фия* – наука о скрытой передаче информации путём сохранения в тайне самого факта передачи) [1] позволяют не только скрытно передавать данные, но и решать задачи помехоустойчивой аутентификации, защиты информации от несанкционированного копирования, отслеживания распространения информации по сетям связи, поиска информации в мультимедийных базах данных.

В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает факт передачи информации, который сам по себе может иметь решающее значение. Исторически стеганография появилась первой, но затем во многом была вытеснена криптографией.

Наибольший интерес представляет цифровая стеганография – это направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты (объекты, подвергшиеся цифровой обработке), вызывая при этом некоторые искажения этих объектов, как правило, незаметным для восприятия человеком. В рамках цифровой стеганографии, в отличие от компьютерной, не рассматриваются вопросы внедрения данных в заголовки *IP*-пакетов и файлов различных форматов, в текстовые сообщения.

Значительная часть исследований в области цифровой стеганографии посвящена встраиванию конфиденциальных сообщений и цифровых водяных знаков в статическую графику, например в файлы форматов, не использовавших сжатие (*BMP*, или *Windows Bitmap*), хотя на данный момент, предложено и достаточно большое количество алгоритмов встраивания информации и цифровых водяных знаков в графические файлы форматов, использующих сжатие с потерями (в том числе и *JPEG*) [2].

Один из методов, применяемый для скрытия текстовых сообщений в неподвижных изображениях – метод *LSB* (*Least Significant Bit*, наименьший значащий бит) — суть этого метода заключается в замене последних значащих битов в контейнере (изображения, аудио или видеозаписи) на биты скрываемого сообщения [1]. Младший значащий бит изображения несет в себе меньше всего информации. Известно, что человек в большинстве случаев не способен заметить изменений в этом бите. Фактически, НЗБ – это шум, поэтому его можно использовать для встраивания информации путем замены менее значащих битов пикселей изображения битами секретного сообщения. При этом для изображения в градациях серого объем встроенных данных может составлять 1/8 от общего объема контейнера. Например, в изображение размером 512×512 можно встроить около 32 кбит информации [1].

Ниже рассмотрен пример встраивания информации в графический файл. В качестве контейнера выбрано изображение размером 450×450 пикселей в формате *BMP* с глубиной цвета 24 бита (рис. 1,а), в качестве сообщения – первый абзац данной статьи.

б

а

Рис. 1. а – исходный файл; б – файл со скрытым сообщениема