УДК 003.26+004.56

Шутько Н. П., ст. преп., канд. техн. наук,
Урбанович П. П., проф., д-р техн. наук
(БГТУ, г. Минск)

ЗАЩИТА АВТОРСКИХ ПРАВ НА ТЕКСТОВЫЕ ДОКУМЕНТЫ НА ОСНОВЕ СТЕГАНОГРАФИЧЕСКОЙ МОДИФИКАЦИИ ЦВЕТА СИМВОЛОВ ТЕКСТА

Кроме скрытой передачи сообщений [1], стеганографические методы являются одним из перспективных инструментов для аутентификации и маркировки авторской продукции с целью защиты авторских прав на цифровые объекты от пиратского копирования. Такие специальные сведения могут рассматриваться в качестве доказательств при рассмотрении споров об авторстве или для доказательства нелегального копирования [2].

Актуальной является задача разработки новых методов, повышающих устойчивость к атакам, т. е. снижающим вероятность извлечения сообщения из контейнера. Один из новых метод для скрытия секретного сообщения в текстовом документе основывается на следующем положении. Цвет символа в текстовом процессоре Microsoft Word представлен в цветовой модели RGB. Незначительное изменение цвета символа не воспринимается человеческим глазом. Используя данную физиологическую особенность, можно незаметно производить встраивание информации.

При реализации известного метода LSB [1] встраивание производится в последние 1–2 бита цвета пикселя изображения. Адаптация алгоритма к тексту позволяет производить встраивание в последние 3–5 бит цвета символа. Увеличение числа используемых бит цвета в тексте, по сравнению с графикой, происходит из-за того, что изображение, как правило, содержит градации и переходы от одного цвета к другому. Текст монотонен и выполняется в большинстве случаев одним цветом, поэтому становится возможным увеличение используемого для встраивания цветового диапазона [3].

При скрытии данных в документе, который предназначен для последующей печати, в качестве изменяемых символов не могут использоваться невидимые знаки (пробелы, табуляции, переводы строк и т. д.), поэтому в этом случае производится дополнительная проверка. Выбор символов для хранения скрытой информации происходит случайным образом. В ходе экспериментов установлено, что модификация до 4-х младших символов цветовой координата каждого канала (RGB) в 100% случаев остается незамеченной поль-

зователем, которому не известен факт осаждения в документе невидимой информации.

Специально для реализации на практике данного метода было создано программное средство (*Sword*), диаграмма деятельности которого показана на рисунке 1.

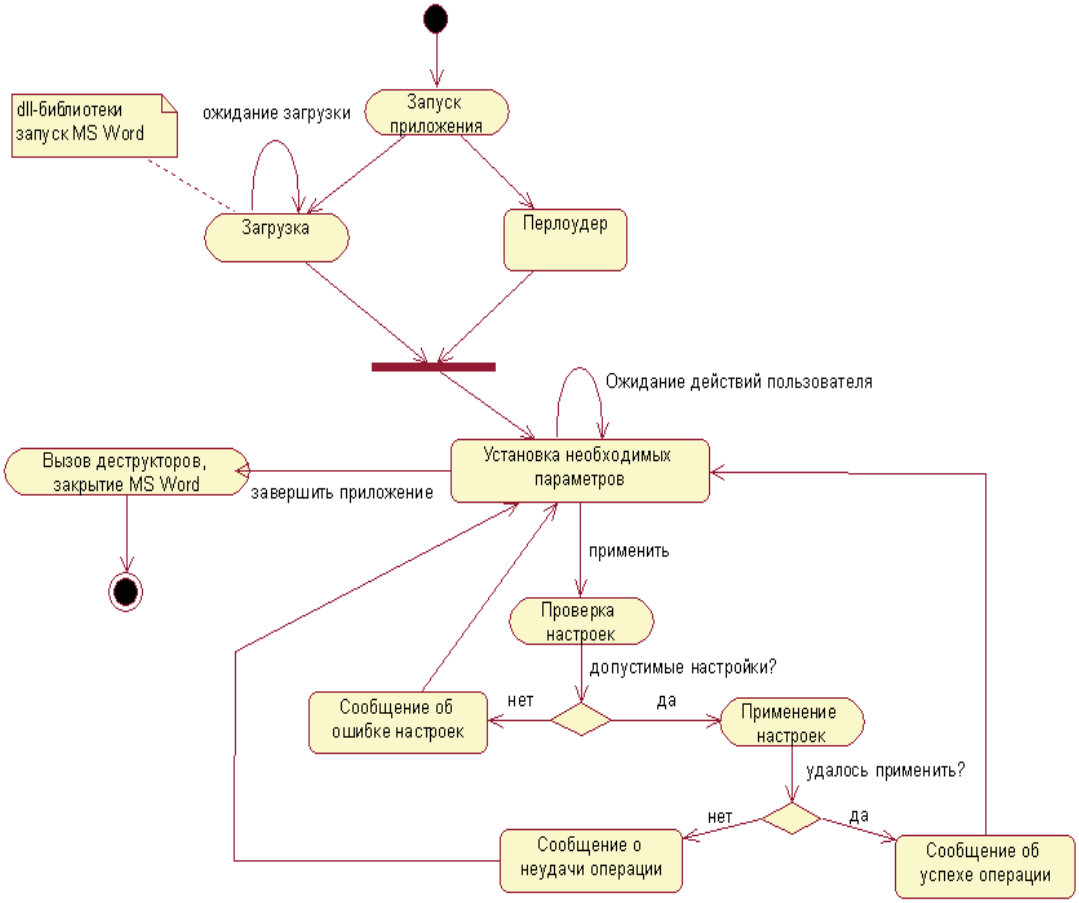

Рисунок 1 – Диаграмма деятельности программного средства *SWord*

Обязательными требованиями для работы программного средства являются наличие на компьютере пользователя Framework 2.0 или выше, а также MS Office Word 2003 или выше. Данным требованиям соответствует большинство компьютеров, работающих на операционных системах Windows. Программное средство реализовано с помощью языка программирования C# в среде разработки Visual Studio 2008 Express, для взаимодействия с объектами MS Office Word используется dll-библиотека Microsoft.Office.Interop.Word.

Установка необходимых параметров в программе осуществляется с помощью трех блоков, в которых задается: стегосообщение (в случае извлечения заполнять не надо), контейнер и настройки, на основе которых происходит скрытие/извлечение сообщения (ключ).

Цвет символа, в котором будет производиться скрытие, форми-

руется исходя из цвета символа-образца и заданного в настройках смещения. По умолчанию это смещение добавляется к основному цвету.

После встраивания необходимой информации есть возможность просмотреть измененный документ нажатием кнопки «*Показать*». При использовании кнопки «*Отметить*» синим маркером будут выделены символы и пробелы, в которые проводилось встраивание необходимой информации (рис. 2).

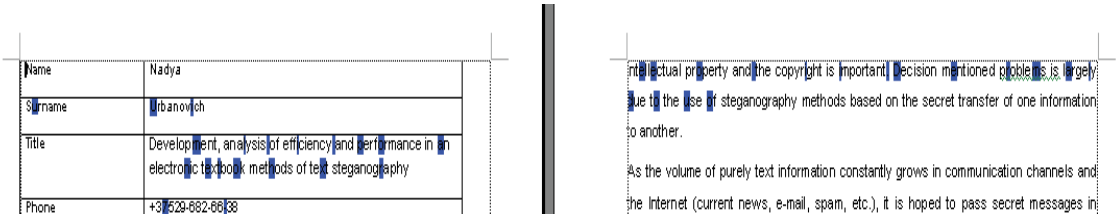

Рисунок 2 – Фрагмент стеганоконтейнера со встроенным сообщением

При скрытии данных в документе, который предназначен для последующей печати, в качестве изменяемых символов не могут использоваться невидимые знаки (пробелы, табуляции, переводы строк и т. д.). В ходе экспериментов установлено, что модификация до 4-х младших символов цветовой координата каждого канала (RGB) в 100% случаев остается незамеченной пользователем, которому не известен факт осаждения в документе невидимой информации.

ЛИТЕРАТУРА

1. Урбанович, П.П. Защита информации методами криптографии, стеганографии и обфускации / П.П. Урбанович. – Минск: БГТУ, 2016. – 220 с.

2. Шутько, Н.П. Моделирование стеганографической системы в задачах по охране авторских прав/ Н.П. Шутько, Н.И. Листопад, П.П. Урбанович// Восьмая МНТК «Информационные технологии в промышленности» (ITI'2015) : тезисы докладов (2–3 апреля 2015 года, Минск). – Минск: ОИПИ НАН Беларуси, 2015. – С. 30-31.

3. Шутько, Н. П. Математическая модель системы текстовой стенографии на основе модификации пространственных и цветовых параметров символов текста / Н. П. Шутько, Д. М. Романено, П. П. Урбанович // Труды БГТУ. – Минск : БГТУ, 2015. – № 6 (179). – С. 152-156.