Защита авторских прав на программные средства и текстовые документы с помощью специальных методов

Пласковицкий В.А.; Шутько Н.П.; Урбанович П.П.
Кафедра информационных систем и технологий
Белорусский государственный технологический университет
Минск, Республика Беларусь
e-mail: {upp, nadya_ur}@rambler.ru, vaplas20@gmail.com

***Аннотация*—Предлагается метод для защиты авторских прав в текстовых документах с помощью стеганографии, а также анализируются некоторые важные аспекты защиты программных средств с помощью методов обфускации. Предлагаемые методы реализованы в авторских программных средствах.**

Ключевые слова: защита авторских прав, стеганография, обфускация

I. Введение

В настоящее время остро стоит проблема защиты прав собственности на информацию, представленную в цифровом виде, от несанкционированного доступа. В данной работе предлагаются два метода, с помощью которых можно встроить необходимую (авторскую) информацию тайно в текст.

II. Стеганографическая защита данных

Методы стеганографии предназначены для скрытия информации, что можно использовать в текстовых документах для тайного размещения сведений, позволяющих установить авторство.

Предлагаемый в работе метод стеганографической защиты базируется на алгоритме LSB (Least Significant Bit). При этом особенностью является использование цветовых характеристик символов для скрытия данных. Сущность данного метода заключается в изменении цвета символа на некоторую величину, не заметную для человека, но определяемую компьютерным анализом. Алгоритм модификации цветовых параметров символов текста состоит в следующем. В настройках задается отклонение от основного цвета, либо задаются статические цвета для символов скрытия в системе RGB. Затем производится выборка символов, используемых для скрытия в документе с произвольным распределением. При этом выбираются два идущих подряд символа: первый — образец, второй — тот, в который будет записана информация для последующего извлечения скрываемого текста. Цвет символов скрытия формируется исходя из цвета символа-образца и заданного в настройках смещения либо статического образца. Произвольный выбор символов позволяет осуществлять процесс скрытия за время, пропорциональное числу скрываемых символов, а процесс извлечения – за время, пропорциональное общему числу символов в документе, что существенно повышает устойчивость к несанкционированному анализу. Для реализации предлагаемого метода авторами было разработано программное средство Sword 1.0 (рисунок 1). В программе реализованы такие возможности, как: выбор кодировки, сжатие данных, вывод символьной статистики документа, используемого для скрытия, индикаторы процесса скрытия и извлечения данных, шаблоны для сохранения выбранных настроек и другие [1].

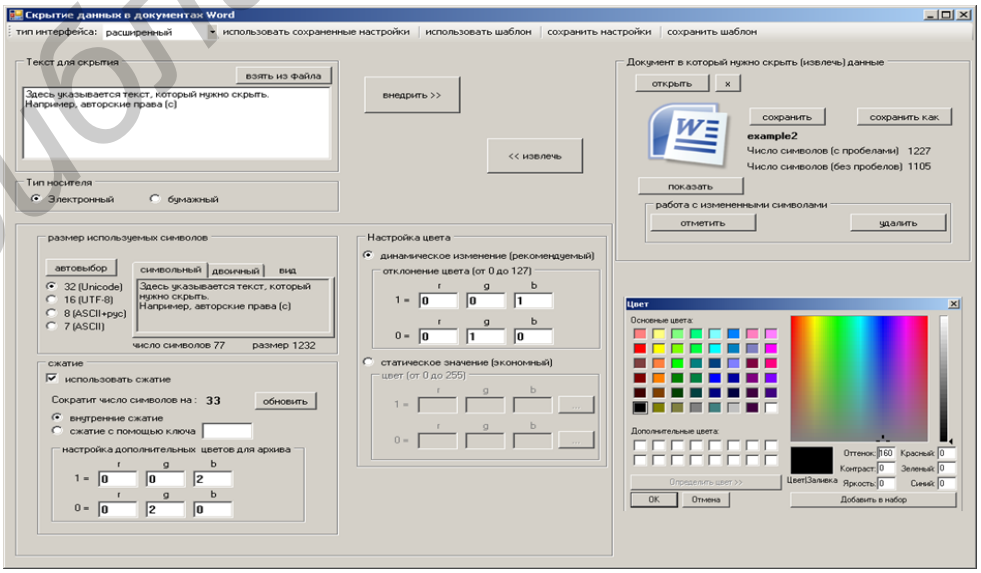

Рис.1. Интерфейс программного средства Sword 1.0

III. Обфускационная защита данных

Другим способом охраны права на программные средства является обфускация. По многим причинам код современных программных приложений представляет собой промежуточный вид (байт-код). Сложность анализа такого кода приближается к изучению исходного кода, что значительно снижает устойчивость к взлому и ограничивает возможные методы защиты. Еще более серьезной проблемой является защита клиентской и серверной части веб-приложений, которые по своей специфике хранятся на уровне исходных кодов [2]. Применение обфускации (запутывание кода) — практически единственный способ программной защиты таких приложений. С помощью этой технологии нельзя добиться абсолютной защиты, но зачастую можно сделать затраты на взлом сравнимыми с самостоятельным производством. Это делает разработку обфускаторов все более популярным направлением защиты за рубежом. К сожалению, активность развития отечественных разработок в данном направлении крайне низка. В работе представлены авторские наработки в данном направлении в виде программного комплекса «Prok», которое обладает рядом отличительных возможностей:

организация защитных алгоритмов выполнена в виде отдельных модулей, взаимодействующих с основной программой через файлы либо сокеты;

интерфейс для ввода пользовательских команд имеет расширенную поддержку регулярных выражений, позволяет сохранять несколько команд в виде отдельного шаблона;

подсветка измененных данных с навигацией по всему списку изменений и возможностью отмены отдельных действий (см. рис. 2);

каталогизация всех возможных действий без ограничения на число уровней вложенности;

возможность внесения изменений вручную;

возможность полного восстановления исходного вида данных, даже при использовании необратимых действий, благодаря возможности хранить историю любых производимых изменений в отдельном файле-ключе;

возможность обработки только указанной части документа.

Программное средство позволяет производить не только обфусцирующую защиту, но и защиту методом шифрования, а также произвольную обработку структурированных документов.

IV. Заключение

В докладе анализируются возможности стеганографии и обфускации как технологий защиты авторских прав. Предложены варианты их использования с учетом современных возможностей программных технологий. Представлены разработанные авторами программные средства «Sword», реализующее приведенный метод скрытия данных, и «Prok», реализующее ряд методов обфускации и других защитных функций.

[1] N. Urbanovich, V. Plaskovitsky, “The use of steganographic techniques for protection of intellectual property rights”, 2011, p. 147 – 148

[2] В.А. Пласковицкий, П.П. Урбанович. Защита программного обеспечения от несанкционированного использования и модификации методами обфускации. Труды БГТУ. Мн.: БГТУ, 2011, с. 173 – 176.

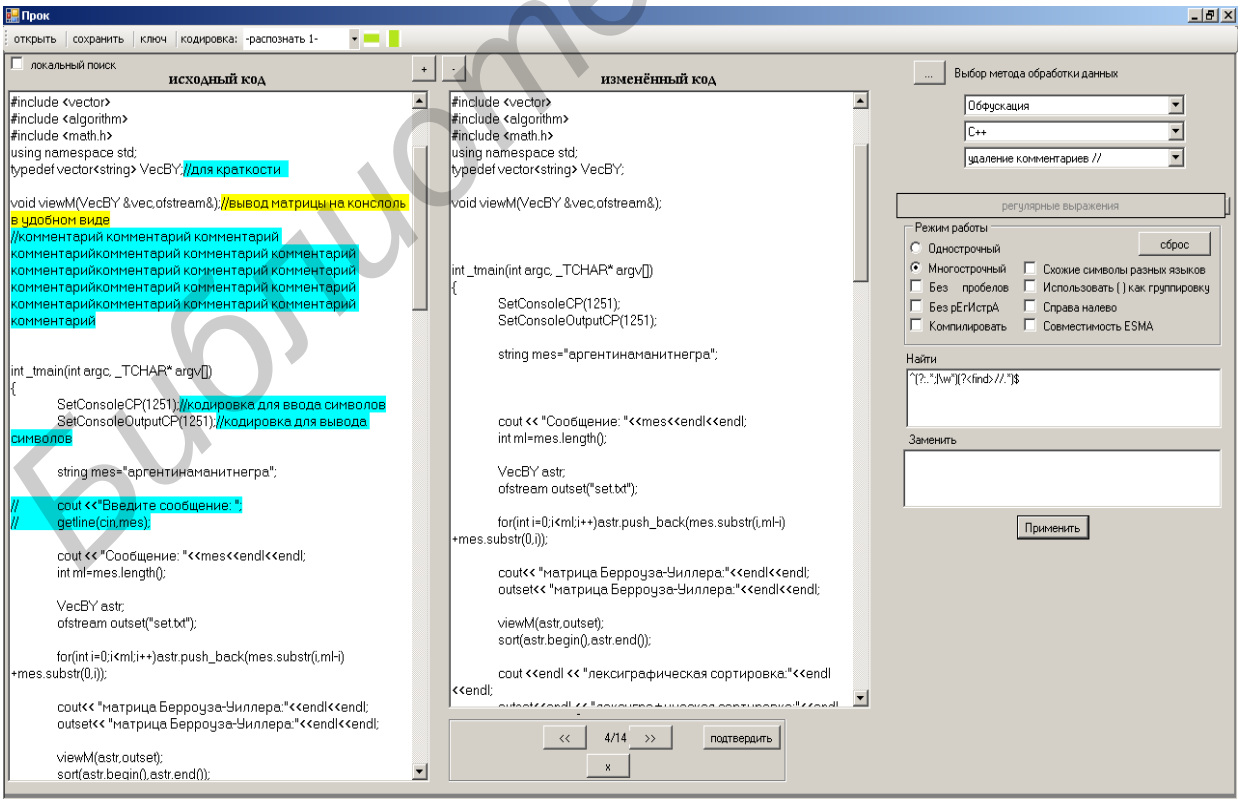

Рис.2. Интерфейс программного средства Prok 1.0