ПОСТАНОВКА ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В ТЕКСТОВЫХ ФАЙЛАХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Манюк А. П.

Ярмолик В. Н. – д-р. техн. наук, профессор

Отправка зашифрованного сообщения очень часто привлекает внимание злоумышленников, которые намереваются или похитить или повредить передаваемые данные. В современном цифровом мире для того чтобы передавать сообщения между несколькими адресатами, не привлекая внимания к процессу общения, используется стеганография.

Рассмотрим комбинированный подход к сокрытию информации, который реализуется при помощи манипуляции с пробелами между словами и параграфами открытого текста.

В настоящее время манипуляции с пробелами кажутся выгодными и имеют свой потенциал в сокрытие информации, так как пробелы появляются в текстовых документах чаще, чем появляются слова. Также существует еще одно преимущество: злоумышленник не будет догадываться, что чистый лист может хранить в себе жизненно важную секретную информацию.

Реализация данного подхода предполагает, что длинна открытого текста будет генерироваться динамически в зависимости от длины секретного текста. Максимальный размер секретной информации зависит от размера незащищенного текста, который может равняться 4kB, 16kB, 32kb, 64kb, 128kb или 256kb. В таблице 1 представлены возможные варианты длины защищенного текста в зависимости от размера открытого текста. Блок открытого текста в 4kB используется в качестве нижней границы возможных размеров общедоступного текста. Данное ограничение накладывается по причине того, что 4kB это минимальный размер незащищенного текста, в котором можно передать хотя бы несколько символов секретного сообщения. Для открытого текста в данном подходе будем использовать детские стихотворения, так как после обработки, незащищенный текст принимает естественный вид, изображенный на рисунке 1.

Размер текста (kB)	
Секретный	Открытый
<4	4
<16	16
<32	32
<64	64
<128	128
<256	256

Таблица 1. – Размер сгенерированного открытого текста в зависимости от длинны секретного сообщения.

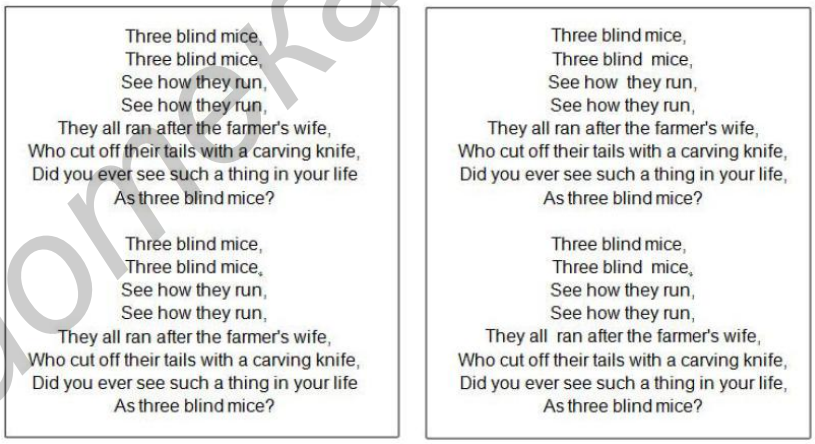

Рис. 1 – Вид оригинального текста (слева) и текста, содержащего в себе секретное сообщение (справа).

Анализ тенденций развития цифровых методов скрытой передачи информации показывает, что в ближайшие годы интерес к развитию таких методов будет усиливаться всё больше и больше. Предпосылки к этому уже сформировались сегодня. Общеизвестно, что актуальность проблемы информационной безопасности постоянно растет и стимулирует поиск новых методов защиты информации.

Список использованных источников:

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. - М.: СОЛОН-Пресс, 2002. - 272с.
2. Ярмолик В.Н., Портянко С.С., Ярмолик С.В. Криптография, стеганография и охрана авторского права. – Мн.: Издательский центр БГУ, 2007. – 242с.
3. J. Brassil, S. Low, N. Maxemchuk, and L. O'Garman. Electronic marking and identification tech-niques to discourage document copying. In IEEE Infocom 94, pages 1278–1287, 1994.
4. W. Bender, D. Gruhl, N. Morimoto, and A. Lu. Techniques for data hiding. In IBM Systems Journal, Vol. 35, Nos. 3-4, pages 313–336, February 1996.