РОЗРОБКА ПРОГРАМНОГО КОМПЛЕКСУ ДЛЯ ПРИХОВУВАННЯ У ПСЕВДОВИПАДКОВО ОБРАНИХ БІТАХ РАСТРОВОГО ЗОБРАЖЕННЯ ЗАШИФРОВАНОГО ЗА ДОПОМОГОЮ ШИФРУ RC4 ПОВІДОМЛЕННЯ

Кордунова Ю., Кухарська Н.
Львівський державний університет безпеки життєдіяльності, м. Львів

У роботі описано процес розроблення програмного комплексу для створення криптостеганографічної системи захисту інформації.
Ключові слова: криптографія, стеганографія, шифр RC4, метод псевдовипадкової перестановки.

The article describes the process of developing a software complex of creating a crypto-steganographic information security system.
Keywords: cryptography, steganography, RC4 cipher, method of pseudorandom restructuring

Одним із найцінніших предметів сучасного життя є інформація. З появою комп'ютерних мереж одержання доступу до неї стало надзвичайно простим. Переваги подання та передачі даних у цифровому вигляді значно полегшують роботу користувачам, проте можуть бути перекреслені з такою ж легкістю, як і можливі їх викрадення й модифікація. Саме тому, питання захисту інформації особливо гостро постають в наш час.

У даній роботі було описано процес розроблення програмного комплексу на основі криптостеганографічного підходу захисту інформації.

Криптостеганографічною називають систему передачі інформації у відкритих каналах зв'язку, що базується на одночасному використанні криптографічних і стеганографічних алгоритмів.

Криптографічний захист – послідовність перетворень інформації з метою зробити її незрозумілою для непосвячених, приховання змісту повідомлень за рахунок шифрування [2].

У даній роботі повідомлення шифрувалося з допомогою потокового шифру RC4. Цей алгоритм працює з n-бітовими словами. Всі обчислення проводяться за модулем 2^n (остача $x \bmod 2^n$ обчислюється дуже швидко шляхом виділення n молодших біт в x з допомогою логічної операції «і»). Як відомо, RC4 використовує L-слівний ключ $K=K_0 K_1 \dots K_{L-1}$ і генерує послідовність слів $\bar{z}=z_1 z_2 z_3 \dots$, конкретний вигляд якої визначається ключем K. Стан генератора задається таблицею S (вектор ініціалізації) з 2^n слів і двома змінними i та j. У кожен момент часу таблиця S містить всі можливі *n*-бітові числа в перемішаному вигляді. Оскільки кожен елемент таблиці приймає значення в проміжку $[0, 2^n - 1]$, то його можна трактувати двояко: або як число, або як номер іншого елемента в таблиці [3].

Криптографічний захист не вирішує згадану вище проблему захисту інформації повністю, позаяк наявність шифрованого повідомлення привертає увагу зловмисника. Саме тому було прийнято рішення використати ще один метод захисту інформації – стеганографічний. Даний метод полягає у приховуванні ж самого факту існування секретних даних при їх передачі, зберіганні чи обробці.

Відповідно, у розробленому програмному комплексі реалізовано процес приховування зашифрованого тексту у растровому зображенні удосконаленим методом заміни найменш значу-щого біта. Молодший значущий біт зображення несе в собі найменше інформації, людина не здатна помітити зміни його значення [1]. Цим і пояснюється його використання для стеганогра-фічних цілей. Молодший біт замінюють бітами секретного повідомлення. У цій роботі дані вбудовуються не у всі пікселі растрового зображення, а лише в обрані псевдовипадково способом.

Можна зробити висновок: стеганографія займаючи свою нішу в інформаційній безпеці, не замінює, а доповнює криптографію, а у комплексі ці дві науки дають змогу здійснити надійний захист важливої інформації.

Література:

1. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. Киев : МК-Пресс, 2006. 288 с.

2. Хорошко В. А. Чекатков. А. А. Методы и средства защиты информации. Киев : ЮНИОР, 2003. 504 с

3. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. Москва : Горячая линия-Телеком, 2002. 175 с.