ПРОГРАМНИЙ ЗАХИСТ ІНФОРМАЦІЇ НА ОСНОВІ РЕАЛІЗАЦІЇ ГІБРИДНОЇ КРИПТОСТЕГАНОГРАФІЧНОЇ СХЕМИ

Кухарська Н. П., к.ф.-м.н., доцент; Лагун А. Е., к.т.н., доцент
Львівський державний університет безпеки життєдіяльності,
Львів, Україна

У розподілених системах передачі інформації одним із найбільш важливих є завдання забезпечення конфіденційності інформації. Для його вирішення, як правило, використовують різні криптографічні методи. Однак у багатьох випадках криптографічного захисту самого по собі не достатньо, оскільки він не дає змогу приховати сам факт наявності або передачі конфіденційної інформації. Крім того, криптографічні методи дещо втрачають свою надійність через зростання обчислювальних можливостей комп'ютерних технологій.

Враховуючи сучасний стан теоретичної бази, перспективність у вирішенні питання обмеження доступу до конфіденційної інформації сторонніх осіб має підхід, суть якого полягає у побудові гібридних систем передачі інформації на основі синтезу методів криптографії та стеганографії. Відповідно до цього підходу повідомлення під час передачі відкритими каналами зв'язку для підвищення ефективності захисту необхідно не тільки зашифрувати, але і приховати. Це передбачає використання методології комп'ютерної стеганографії, яка є технікою вкраплення секретної інформації у відкриті великі інформаційні масиви даних. Тоді спостерігач не зможе запідозрити існування вбудованої додаткової інформації.

Основою алгоритмів комп'ютерної стеганографії є ідея заміни незначущих або не використовуваних фрагментів масивів даних комп'ютерних файлів конфіденційною інформацією. У результаті стеганографічної обробки файлу-оригіналу отримують файл, який зберігає своє функціональне призначення, майже не відрізняється від оригіналу і водночас містить секретне зашифроване повідомлення, що дає можливість користувачу передати його під таким своєрідним прикриттям телекомунікаційними системами таємно.

Широкий спектр стеганографічних програм призначених для використання у навчальному процесі представлений в [1].

Переваги описаного вище криптостеганографічного підходу демонструються в дисципліні «Захист програмного забезпечення та програмні засоби захисту інформації», що читається у Львівському державному університеті безпеки життєдіяльності для підготовки фахівців освітньо-кваліфікаційного рівня «спеціаліст» за спеціальністю «Адміністративний менеджмент у сфері захисту інформації».

Як алгоритм шифрування у криптографічному модулі побудованої за допомогою універсальної математичної системи MathCad криптостеганог-

рафічної системи використовується відомий біграмний шифр заміни — шифр Плейфера [2]. Його основою є шифрувальна таблиця з випадково розташованими символами алфавіту початкового повідомлення. При розробці процедур шифрування та розшифрування у системі Плейфера використовувався 256-символьний алфавіт.

Інформаційними контейнерами вибрано WAVE-аудіо-файли у PCM-форматі, а як стеганографічний метод, що застосовується для вбудовування попередньо зашифрованої інформації — найпоширеніший на цей час метод кодування молодших розрядів даних [1].

Відомо, що цифровий звук — це ряд чисел, який представляє інтенсивність звукового сигналу у моменти часу, що йдуть послідовно. Молодші розряди цифрових відліків містять дуже мало корисної інформації про поточні параметри звуку. Іншими словами, заміна їх вмісту не відчутна для людського вуха, що і сприяє утаєнню додаткової інформації.

Зауважимо, що загальна стійкість розробленої криптостеганографічної системи є набагато вищою, ніж стійкість окремих її складових — криптографічної та стеганографічної підсистем.

Література

1. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю.Пузыренко. — К. : МК-Пресс, 2006. — 249 с.

2. Сулятицький П. Р. Класичні методи шифрування інформації простою заміною / П. Р. Сулятицький, Ю. І. Грицюк // Науковий вісник НЛТУ України : зб. наук.-техн. праць. — Львів : РВВ НЛТУ України. — 2011. — Вип. 21.9. — С. 306–317.

Анотація

Акцентується увага на перспективності підходу, в основі якого знаходиться процедура комбінування методів криптографії та стеганографії. У побудованій криптостеганографічній системі для приховування конфіденційної інформації під час пересилання її відкритими каналами зв'язку поєднано шифр Плейфера з кодуванням молодших розрядів даних WAVE-аудіо-файлів.

Ключові слова: криптографія, стеганографія, захист інформації.

Аннотация

Акцентируется внимание на перспективности подхода, в основе которого находится процедура комбинирования методов криптографии и стеганографии. В построенной криптостеганографической системе для утаивания конфиденциальной информации при передаче ее по открытым каналам связи сочетаются шифр Плейфера и кодирование младших разрядов данных WAVE-аудио-файлов.

Ключевые слова: криптография, стеганография, защита информации.

Abstract

Attention is accented on the prospects of approach based on the procedure combining the methods of cryptography and steganography. In the created cryptographic and steganographic system hiding of the confidential information during transfer by the open communication channels was combined the Playfair cipher and encoding the least significant bits of WAVE-audio files.

Keywords: cryptography, steganography, information security.