УДК 004.056.55:003.26

Н.П. Кухарська, Ю.С. Кордунова, І.В. Хомич
Львівський державний університет безпеки життєдіяльності

Використання гібридного “криптографія+стеганографія” підходу для розв’язання задач захисту інформації

У роботі обґрунтовано доцільність об’єднання в рамках одного програмного рішення криптографічних і стеганографічних підходів захисту інформації та розроблено дві криптостеганосистеми для захисту конфіденційної інформації при передачі її відкритими каналами зв’язку. Описано принцип реалізації потокового шифру RC4 та блокового AES; викладено суть стеганографічного LSB-методу, застосування якого передбачає приховування інформації у цифрових об’єктах, так званих, контейнерах. У даній роботі у ролі стеганоконтейнерів використано растрові RGB-зображення та аудіо-файли формату WAVE. У випадку зображення-контейнера стеганографічний захист криптографічно закритої RC4 алгоритмом інформації здійснено шляхом вбудовування її у найменш значущі біти псевдовипадково обраних пікселів. Вибір растрового зображення формату RGB зумовлено тим, що такий тип зображень складається із набору пікселів червоної, зеленої та синьої складових, що в свою чергу створює достатню надлишковість та можливість вбудовування великих обсягів інформації. Вбудовування зашифрованого AES шифром текстового повідомлення у звуковий файл здійснено методом блокового приховування. Простота структури WAVE-файлу дає змогу без особливих додаткових зусиль реалізувати будь-які стеганографічні методи приховування даних.

Програмні комплекси, що реалізують криптостеганографічний захист даних, розроблено у середовищі комп’ютерної алгебри MathCAD, що має своє пояснення. Можливість використання безлічі вбудованих MathCAD-команд та інтуїтивно зрозумілий інтерфейс середовища дають змогу не лише створювати нові програмні модулі, а й модифікувати уже готові.

Ключові слова: стеганографія; криптографія; стеганоконтейнер; шифр RC4; шифр AES; LSB-метод; метод псевдовипадкової перестановки; метод блокового приховування.

N.P. Kukharska, Yu. S. Kordunova, I.V. Khomych
Lviv State University of Life Safety

USING A HYBRID “CRYPTOGRAPHY + STEGANOGRAPHY” APPROACH TO SOLVE INFORMATION SECURITY TASKS

The paper substantiates the feasibility of integrating as one software solution cryptographic and steganographic approaches to information security and developed two cryptosegano-systems to protect sensitive information and their transmission through open communication channels. The principle of implementation of RC4 stream cipher and block AES is described; the essence of the steganographic LSB method, the application of which involves the concealment of information in digital objects, so-called containers. In this paper, the RGB images and WAVE audio files are used as steganocontainers. In the case of a container image, the steganographic protection of the cryptographically enclosed RC4 information algorithm is accomplished by embedding it in the least significant bits of pseudo-randomly selected pixels. The choice of an RGB bitmap is because this type of image consists of a set of pixels of red, green and blue components, which in turn creates enough redundancy and the ability to embed large amounts of information. The embedding of an AES encrypted text message into an audio file is done by block hiding. The simplicity of the WAVE file structure makes it easy to implement any steganographic methods of hiding data without much effort.

Software complexes that implement crypto-steganographic data protection were developed in the environment of the computer algebra MathCAD, which has its explanation. The ability to use many built-in MathCAD commands and an intuitive environment interface not only allow you to create new software modules but also to modify them.

Keywords: steganography; cryptography; steganocontainer; RC4 cipher; AES cipher; LSB method; method of pseudo-random restructuring, block hiding method.

Питання захисту інформації від несанкціонованого доступу в останні роки стало як ніколи актуальним. Для збереження конфіденційності інформації при пересиланні її

відкритими каналами зв'язку традиційно використовують два способи програмного захисту: криптографічні та стеганографічні методи захисту. Суть криптографічного захисту полягає в тому, що інформація зашифровується певним алгоритмом в нечитабельний формат. У свою чергу, стеганографічний захист – це приховування самого факту існування інформації шляхом вбудовування її в цифрові об'єкти (контейнери), що спричиняє деякі спотворення цих об'єктів. Найпоширенішими типами таких контейнерів є текст, зображення, аудіодані, відеопослідовності.

На основі попередніх досліджень [6, 7], що стосуються використання тексту, як стеганоконтейнера, робимо висновок про те, що зображення та аудіо-файли є ефективнішими для реалізації стеганографічного захисту, оскільки характерною особливістю таких контейнерів є їх надлишковість, що дає можливість маскувати у них достатньо великий обсяг конфіденційної інформації. У роботі [10] детально описують цей факт.

І криптографічний, і стеганографічний підходи мають свої переваги і недоліки. Перспективним напрямком програмного захисту інформації є об'єднання методів криптографії та стеганографії, що дає змогу підвищити рівень захисту інформації та розробити більш ефективні нові нетрадиційні методи забезпечення інформаційної безпеки [1].

Питання щодо криптостеганографічних систем захисту інформації розглядались у [8, 11]. У цих роботах описано процес вбудовування зашифрованих повідомлень у зображення.

Метою даної роботи є розробити у середовищі універсальної математичної системи MathCAD програмні комплекси для створення криптостеганографічних систем захисту інформації. У ролі стеганоконтейнерів розглядатимемо як зображення, так і аудіофайли.

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

Побудова криптостеганосистеми на основі шифру RC4 та методу приховування інформації у псевдовипадково обраних бітах графічного файлу.

Перший крок – шифрування інформації з використанням потокового шифру RC4. Даний алгоритм широко застосовується у різних системах захисту інформації (протоколи SSL, TLS, WEP, WPA), що пояснюється його високою швидкістю та змінним розміром ключа.

На рис. 1 зображено схему шифрування повідомлення алгоритмом RC4.

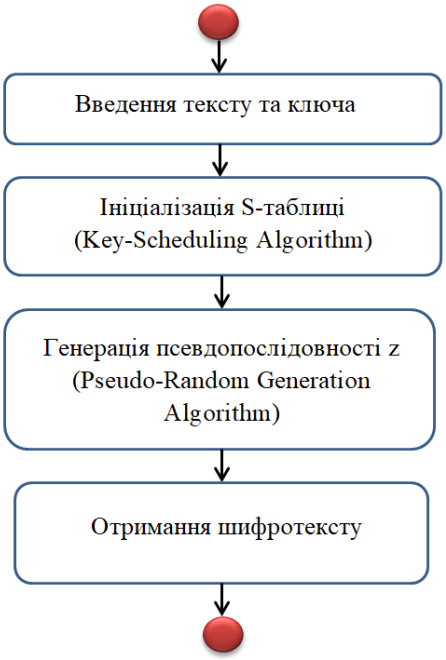

Рисунок 1 – Схема шифрування повідомлення алгоритмом RC4

Алгоритм RC4 використовує L-слівний ключ $K = K_0\, K_1 \ldots K_{L-1}$ і на його основі генерує послідовність слів $z=z_1 z_2 z_3 \ldots$. Стан генератора задається таблицею S (вектор ініціалізації) і двома змінними i та j. У кожен момент часу таблиця S містить всі можливі n-бітові числа в перемішаному вигляді. Оскільки значення кожного елементу таблиці належать проміжку $[0,\ 2^n - 1]$, то їх можна трактувати двояко: або як число, або як номер іншого елемента в таблиці [2].

Секретний ключ K задає початкове перемішування чисел в таблиці S, що реалізовується за допомогою алгоритму, який називають алгоритмом ключового розкладу (Key-Scheduling Algorithm):

$j \leftarrow 0, \quad S \leftarrow (0,1, \ldots . 2^n - 1);$

$FOR\ i = 0,1 \ldots \ldots, 2^n - 1\ DO$

$j \leftarrow (j + S_i + K_{i\ mod\ L}) mod 2^n,$

$S_j \leftrightarrow S_i;$

$i \leftarrow 0, j \leftarrow 0.$

У середовищі комп’ютерної алгебри MathCAD цей алгоритм реалізуємо таким чином:

```
S := | j ← 0
     | for i ∈ 0.. 2^n − 1
     |     | j ← mod[(j + S_{i+1} + KEY_{mod(i,L)+1}), 2^n]
     |     | P ← S_{i+1}
     |     | S_{i+1} ← S_{j+1}
     |     | S_{j+1} ← P
     | S
```

Рисунок 2 – Програмний код – Формування вектора ініціалізації *S*

Після цього генератор готовий до роботи. Генерація чергового випадкового слова z_i здійснюється у такий спосіб:

$i \leftarrow (i+1) mod 2^n;$

$j \leftarrow (j+S_i) mod 2^n;$

$S_j \leftrightarrow S_i;$

$t \leftarrow (S_i + S_j) mod 2^n;$

$z_i \leftarrow S_t.$

Ця частина алгоритму RC4 називається генератором псевдовипадкової послідовності (Pseudo-Random Generation Algorithm) (рис. 3).

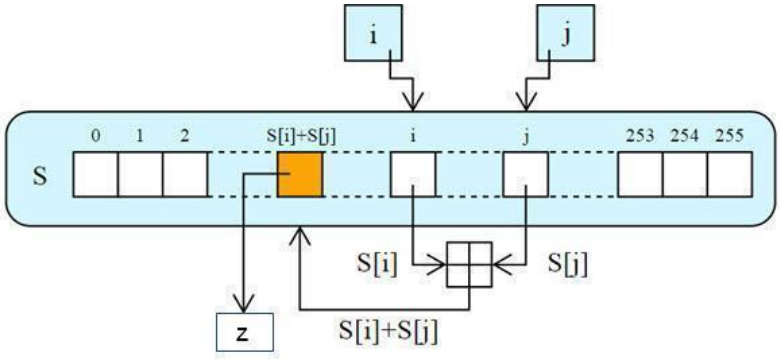

Рисунок 3 – Схематичне зображення генератора ключового потоку RC4 [2]

Шифрограма (c_i) згідно алгоритму RC4 отримується як результат додавання за модулем два псевдовипадкової послідовності (z_i) та відкритого тексту (m_i):

$$c_i = m_i \oplus z_i$$

Генерацію чергового псевдовипадкового слова та формування на його основі шифротексту здійснює програмний модуль (рис. 4):

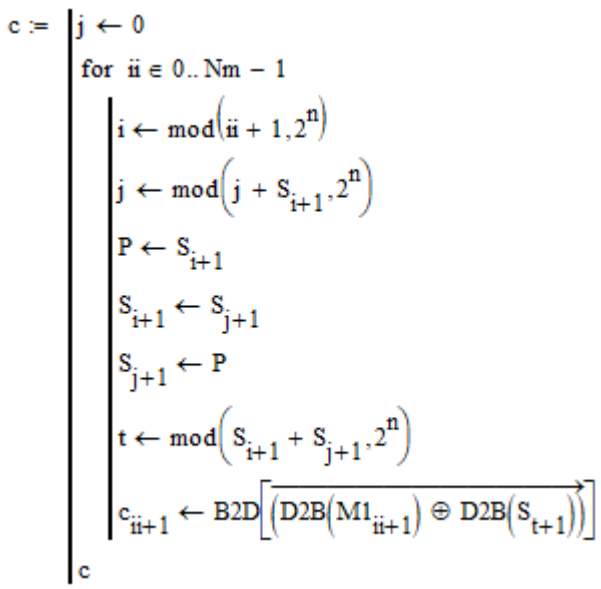

Рисунок 4 – Програмний код – Шифрування тексту з використанням алгоритму RC4

Розшифрування полягає в регенерації ключового потоку (z_i) та додаванні його та шифрограми (c_i) за модулем два. На основі властивості операції додавання за модулем два на виході ми отримаємо вихідний текст (m_i):

$$m_i = c_i \oplus z_i = (m_i \oplus z_i) \oplus z_i.$$

Після шифрування здійснюємо приховування даних у псевдовипадково обраних бітах растрового зображення. У роботі здійснюємо вбудовування інформації в канал синього кольору, так як до його модифікацій система людського зору найменш чутлива.

Для реалізації стеганографічного методу обираємо зображення формату RGB. Важливо, щоб відношення між об’ємами зображення та інформації було не менше 24:1. Це спричинено специфікою LSB-методу. У LSB-методах вбудовування повідомлень здійснюється в молодші найменш значущі біти (НЗБ) файлу-контейнера [4].

Вбудовування у пікселі зображення зашифрованого повідомлення здійснюватимемо за псевдовипадковим порядком, що залежить від ключа K_0 (рис. 5). Цей ключ не містить послідовності координат пікселів зображення, проте однозначно визначає їх. Даний метод детально описано у монографії [4].

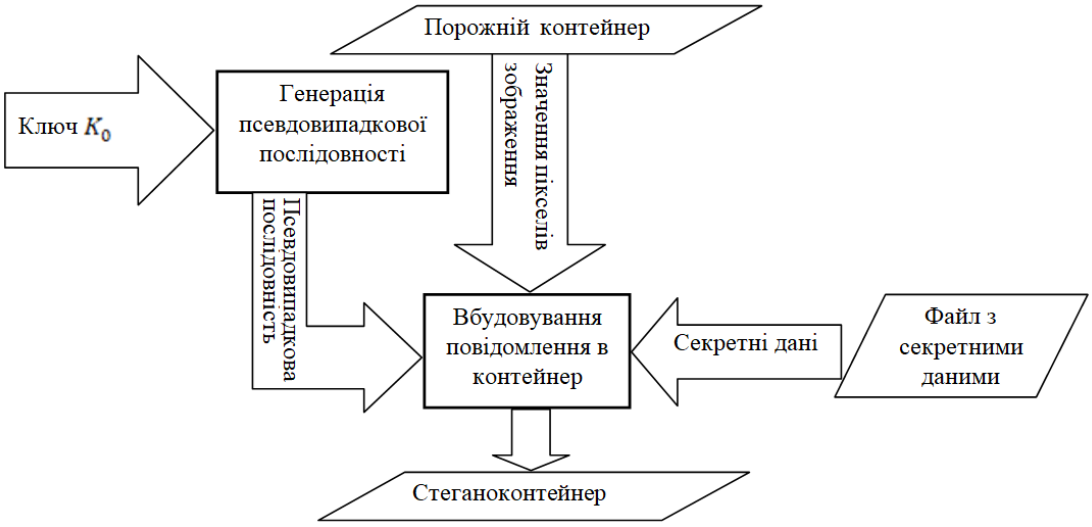

Рисунок 5 – Схема процесу вбудовування повідомлень у зображення [5]

Побудова криптостеганосистеми на основі шифру AES та методу блокового приховування інформації у звуковому файлі. Опишемо процес шифрування за допомогою шифру AES. Для шифрування використовуємо ключ розміром 128 біт, який представимо у вигляді матриці 4x4. На початку процесу шифрування, вхідне повідомлення розбиваємо на блоки (*state*) розміром 16 байт або 128 біт. Кожен блок згідно AES-алгоритму шифрується незалежно один від одного за декілька етапів – раундів.

Схема криптоперетворень виглядає наступним чином. Спочатку розширюємо ключ шифрування (*KeyExpansion)* для того, щоб мати набір даних для раундових ключів та сумуємо раундовий ключ з основним (*AddRoundKey*). Далі реалізовуємо наступні чотири кроки. Замінюємо байти *state* відповідно до таблиці замін (*SubBytes*), циклічно зміщуємо рядки (*ShiftRows)*, після чого здійснюємо перестановку стовпців (*MixColumns*) та знову підсумовуємо з раундовим ключем (*AddRoundKey*). Детальніше про ці криптоперетворення описано у працях [13, 8, 12]. Ці операції повторюємо на кожному з дев’яти раундів. Схематичне зображення одного раунду представлено на рис.6.

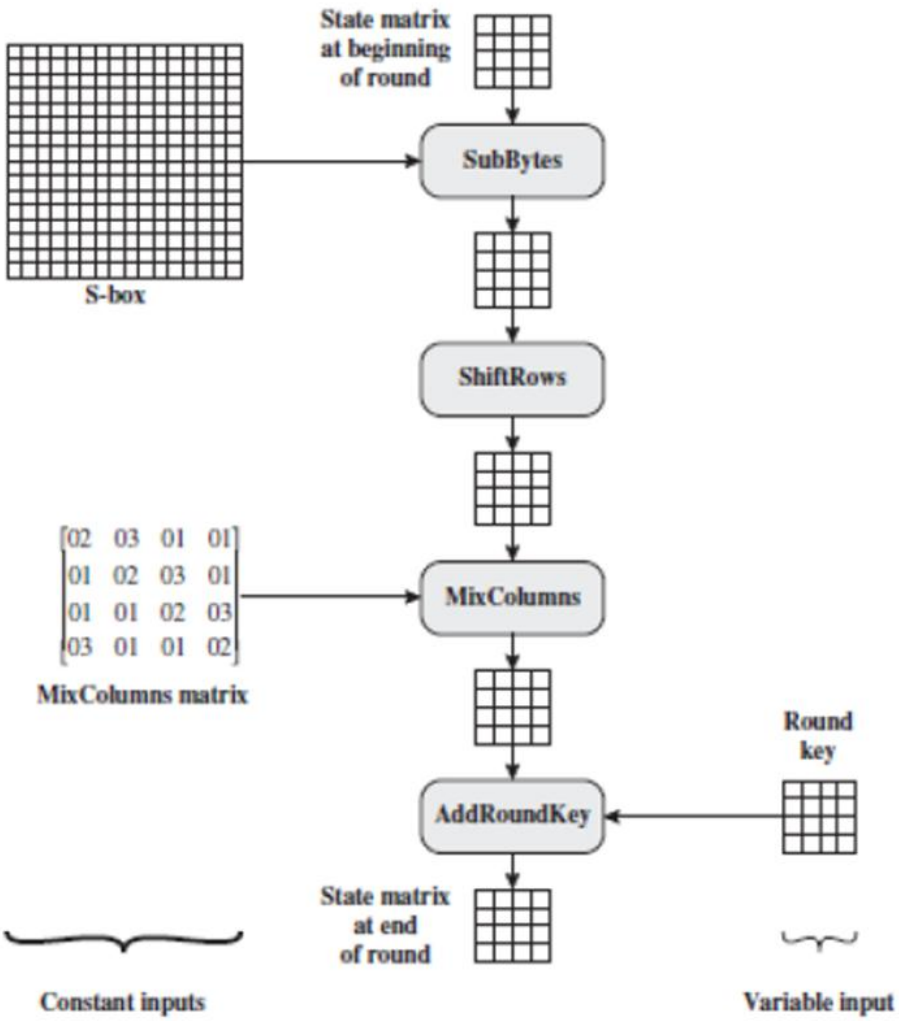

Рисунок 6 – Схематичне зображення одного з дев'яти раундів AES-шифрування [12]

Після цього реалізовуємо десятий завершальний раунд, який включає в себе наступні три кроки: *SubBytes, ShiftRows, AddRoundKey*

На рис. 7-9 зображено реалізацію описаних криптоперетворень в програмному середовищі комп'ютерної алгебри MathCAD.

```
ShiftRowsx(x) := | for m ∈ 1..3
                 |   for k ∈ 1..m
                 |     zap ← x[m,0]
                 |     for k1 ∈ 0..2
                 |       x[m,k1] ← x[m,k1+
                 |     x[m,3] ← zap
                 | x
```

```
SubBytes(x) := | for m ∈ 0..3
               |   for k ∈ 0..3
               |     ff ← D2H(x[m,k])
               |     b[m,k] ← S_box[ff1,ff0]
               | b
```

Рисунок 7 – Програмні коди – Перетворення *ShiftRows* та *SubBytes*

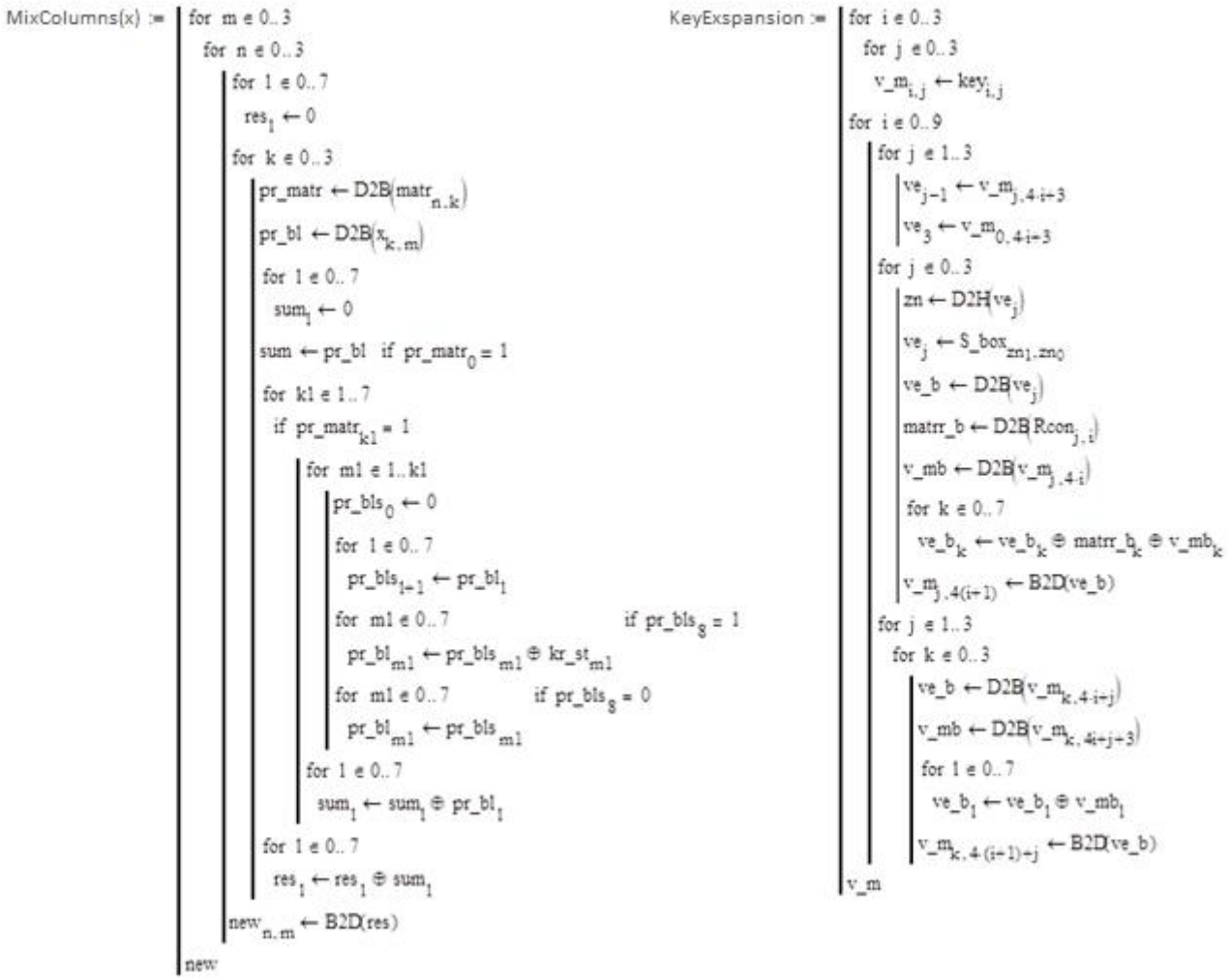

Рисунок 8 – Програмні коди – Перетворення *MixColumns* та *KeyExpansion*

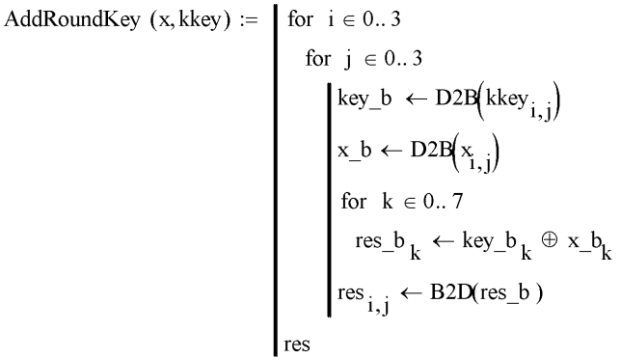

Рисунок 9 – Програмний код – Перетворення *AddRoundKey*

Зашифроване вище описаним способом повідомлення вбудовуємо в аудіоконтейнер методом блокового приховування інформації. Метод блокового приховування також належить до LSB-методів. Вважається, що молодші біти аудіо-інформації, представленої в форматах файлів без втрат (наприклад, WAVE), не несуть істотних відомостей про сигнал, тому що перебувають на рівні шуму. Людина, через особливості своєї слухової системи, не здатна відчути зміни у цих бітах [4]. Метод блокового приховування інформації був реалізований у середовищі MathCAD у роботі [5] для випадку приховування інформації у

зображенні. Його можна реалізувати і для аудіоконтейнера. Згідно алгоритму методу ASCII-коди символів повідомлення подаємо у вигляді вектора бітів. Послідовність звукових амплітуд файла контейнера розбиваємо на *n* блоків, де *n* – кількість біт повідомлення. Приховуючи *i*-ий біт повідомлення, виконуємо наступні дії. В *i*-ому блоці аудіо-файла сумуємо за модулем 2 найменші значущі біти усіх його елементів. Отриману суму порівнюємо із значенням біта повідомлення. Якщо вони не дорівнюють один одному, інвертуємо НЗБ будь-якого, обраного випадковим чином, елемента блоку. У підсумку отримаємо, що у кожному блоці аудіо-сигналу буде "зашито" по одному бітові повідомлення. Під час процедури видобування отримуємо їх, додаючи за модулем 2 НЗБ усіх елементів блоків [9].

Програмна реалізація цього методу подана на рис.10.

```
Sv := | Mvec_bin ← D2B(M1_0)
      | for j ∈ 1.. rows(M1) − 1
      |   Mvec_bin ← stack(Mvec_bin, D2B(M1_j))
      | for σ ∈ 1.. dov
      |   r1 ← (σ − 1)·χ
      |   r2 ← σ·χ − 1
      |   Δ1 ← submatrix(Cv, r1, r2, 0, 0)
      |   b ← 0
      |   for x ∈ 1.. χ
      |     | LSB ← mod(Δ1_(x−1), 2)
      |     | b ← b ⊕ LSB
      |   trace(b)
      |   B_(σ−1) ← b
      |   if b ≠ Mvec_bin_(σ−1)
      |     | n ← ceil(rnd(χ − 1))
      |     | Δ1_n ← Δ1_n + 1  if mod(Δ1_n, 2) = 0
      |     | Δ1_n ← Δ1_n − 1  otherwise
      |     | l ← 0
      |     | for k ∈ r1.. r2
      |     |   | Cv_k ← Δ1_l
      |     |   | l ← l + 1
      | Cv
```

Рисунок 10 – Програмний код – Блокове приховування інформації в аудіоданих

Блоковий метод приховування інформації має таку ж стійкість до спотворення, як і метод заміни НЗБ, оскільки є його модифікацією.

Висновок. Обмін інформацією через дротові та бездротові канали зв'язку не є безпечним з точки зору збереження конфіденційності та цілісності даних. Цілком ймовірно,

що в учасників інформаційного обміну може виникнути необхідність переслати конфіденційне повідомлення, а це вимагає розробки та впровадження захищеної системи. У статті розглянуто підхід до побудови захищеної системи обміну інформацією мережею, який базується на інтеграції двох алгоритмів захисту інформації: криптографічного та стеганографічного. Одночасне використання стосовно конфіденційних даних процедур шифрування та приховування дасть змогу забезпечити подвійний рівень захисту і таким чином отримати більш надійну систему зв'язку.

У статті описано процес побудови у середовищі системи комп'ютерної алгебри MathCAD двох криптостеганографічних систем: однієї – на основі потокового шифру RC4 та методу приховування інформації у псевдовипадково обраних бітах зображення, другої – на основі шифру AES та методу блокового приховування інформації у звуковому файлі.

Розроблені MathCAD-комплекси можуть бути використані під час пересилання даних відкритими каналами зв'язку з метою збереження їх конфіденційності, а також, завдяки наочності та можливості модифікацій, у навчальних цілях для підготовки фахівців з кібербезпеки.

Список літератури:

1) Алиев А. Т., Аграновский А. В. Вопросы построения криптостеганографических систем. Модель стеганографического канала передачи данных. *Информационное противодействие угрозам терроризма.* 2006. № 8. С. 79-91.

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

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

4) Конахович Г. Ф., Прогонов Д. О., Пузиренко А. Ю. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних : підручник. Київ : ЦУЛ, 2018. 555 с.

5) Кордунова Ю. С., Кухарська Н. П., Приховування даних у псевдовипадково обраних бітах растрового зображення. *Проблеми та перспективи системи безпеки життєдіяльності*: зб. наук. праць XIII Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів, м. Львів, 22-23 берез. 2018 р. Львів, 2018. С. 224-225.

6) Кухарська Н. П. Аналіз стеганографічних методів довільного інтервалу. *Вісник ЛДУ БЖД. Львів*, 2016. № 14. С. 7-16.

7) Кухарська Н. П. Програмна реалізація алгоритмів приховування інформації методами довільного інтервалу. *Вісник ЛДУ БЖД.* Львів, 2018. № 14. С. 41-48.

8) Швідченко І. В. Побудова криптостеганосистем для розв’язання задач інформаційної безпеки: дис. ... на здобуття наук. ступеня канд. фіз.-мат. наук : 01.05.01. Київ, 2011. 128 с.

9) Хомич І. В., Кухарська Н. П. Реалізація методу блокового приховування текстового повідомлення у звукових файлах. *Проблеми та перспективи системи безпеки життєдіяльності* : зб. наук. праць XIII Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів, м. Львів, 22-23 берез. 2018 р. Львів, 2018. С. 253-254.

10) Юдін О., Зюбіна Р., Фролов О. Аналіз стеганографічних методів приховування інформаційних потоків у контейнерах різних форматів. *Радиоэлектроника и информатика*. 2015. № 3. С. 13-21.

11) Abdullah A. M., Aziz R. H. New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm. *International Journal of Computer Applications*. 2016. Vol. 143, No 4. P. 11-17.

12) Abdullah, A. M. (2017). Advanced Encryption Standard (AES). Algorithm to Encrypt and Decrypt Data. *Cryptography and Network Security*. URL: https://www.researchgate.net/publication/317615794

13) Jerry Shi, Z. Advanced Encryption Standard. URL: https://docplayer.net/42681857-Advanced-encryption-standard-z-jerry-shi-department-of-computer-science-and-engineering-university-of-connecticut.html

References:

1) Alyev, A. T. and Agranovskij, A. V. (2006). Issues of building crypto-steganographic systems. Model steganographic data channel. *Information counteraction to threats of terrorism*, no. 8, pp. 79–91 (in Russ).

2) Barychev, S. G., Honcharov, V. V. and Serov, R. E (2002). *Osnovy sovremennoi kriptografiia.* [The basics of modern cryptography]. Moscow: Goriachaia liniia-Telekom (in Russ).

3) Konakhovych, G. F., and Puzyrenko, A. Yu. (2006). *Komp'juternaja steganografija. Teorija i praktika.* [Computer steganography. Theory and practice.], Kyiv: MK-PRESS (in Russ).

4) Konakhovych, H. F., Prohonov, D. O., and Puzyrenko, O. Yu. (2018). *Komp’iuterna stehanohrafichna obrobka y analiz multymediinykh danykh*.[Computer steganographic processing and analysis of multimedia data]. Kyiv: TUL (in Ukr.).

5) Kordunova, Yu. S., and Kukharska, N. P.(2018). Hiding data to the pseudo-random bits of a raster image. The collection of abstracts of International Scientific and Practical Conference of Young Scholars, Cadets and Students "Problems and prospects of life safety", Lviv, March 22-23, 2018, pp. 224-225 (in Ukr.).

6) Kukharska, N. P. (2016). Analysis of steganography methods of random interval. *Bulletin of Lviv State University of Life Safety*, no. 14, pp. 7-16 (in Ukr.)

7) Kukharska, N. P. (2018). Program implementation of algorithms of hiding of information by methods of a random interval. *Bulletin of Lviv State University of Life Safety*, no. 18, pp. 41-48 (in Ukr.).

8) Shvidchenko, I. V. (2016). Cryptosteganographic algorithms for solution the problems of information security. Candidate's thesis. Kyiv (in Ukr.).

9) Khomych, I. V., and Kukharska, N. P. (2018). Implementation the method of blocking concealment of a text message in audio files. The collection of abstracts of International Scientific and Practical Conference of Young Scholars, Cadets and Students "Problems and prospects of life safety", Lviv, March 22-23, 2018, pp. 253-254 (in Ukr.).

10) Yudin, O. K., Ziubina, R. V., and Frolov, O. V. (2015). Analysis of the steganographic methods of the collection of information flow in containers of the format format. *Radioelectronics and informatics*, no. 3, pp. 13-2. Retrieved from http://nbuv.gov.ua/UJRN/reii_2015_3_5 (in Ukr.)

11) Abdullah, A. M. and Aziz, R. H. (2016). New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm. *International Journal of Computer Applications*, vol. 143, no. 4, pp. 11-17.

12) Abdullah, A. M. (2017). Advanced Encryption Standard (AES). Algorithm to Encrypt and Decrypt Data. *Cryptography and Network Security*. Retrieved from https://www.researchgate.net/publication/317615794

13) Jerry Shi, Z. (2012). Advanced Encryption Standard. Retrieved from https://docplayer.net/42681857-Advanced-encryption-standard-z-jerry-shi-department-of-computer-science-and-engineering-university-of-connecticut.html