УДК 681.3.004

Кулик А.Я., Кривогубченко Д.С., Роптанова Ю.В.

ВИКОРИСТАННЯ ФУНКЦІЙ УОЛША-АДАМАРА ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ ПІД ЧАС ЇЇ ПЕРЕДАВАННЯ КАНАЛАМИ ЗВ'ЯЗКУ

В теперішній час у зв'язку з формуванням широких комп'ютерних інформаційних мереж, розрахованих на зберігання та передавання конфіденційної інформації, розвитку електронних пошт, систем банківських електронних платежів тощо, виникає потреба у забезпеченні захисту інформації. Заходи захисту інформації можна розподілити на організаційні та технічні [1]. Умовно систему передавання інформації в узагальненому вигляді можна зобразити у вигляді, поданому на рисунку 1. Більшість таких систем використовують лінії зв'язку колективного користування. Саме вони і є найбільш вразливим елементом у системі передавання. Якщо можливий несанкціонований доступ до інформації на центральному пункті зв'язку чи на абонентських пунктах, то саме розроблення системи передавання не має сенсу. Виходячи з цього, їх можна вважати абсолютно надійними.

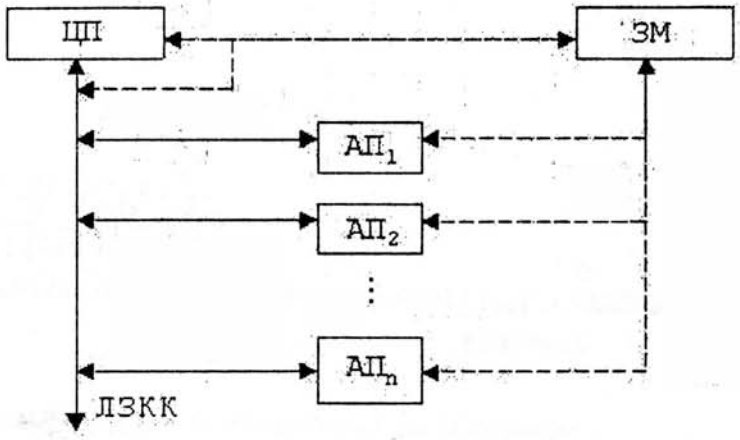

Рисунок 1 – Узагальнений вигляд системи передавання інформації: ЦП – центральний пункт зв'язку; $АП_n$ – n-ний абонентський пункт; ЗМ – зловмисник; ЛЗКК – лінія зв'язку колективного користування.

Одним з найбільш важливих аспектів у галузі передавання інформації є її захист як від завад у каналі зв'язку, так і від несанкціонованого доступу у випадку її конфіденційності. Найбільш поширений підхід полягає у криптографічному закритті інформації, а потім перетворенні за допомогою завадозахищених кодів. Разом з тим самі алгоритми завадозахищеного кодування вже вміщують елементи криптографічного закриття інформації.

Побудова засобів передавання на базі мікропроцесорної техніки накладає власні обмеження на розроблювані алгоритми кодування. Пристрої обміну інформацією будуються за класичною структурою, схема якої наведена на рисунку 2.

Основна особливість таких пристроїв полягає в тому, що дані зберігаються і передаються в байтовому форматі. Тобто, незалежно від довжини елементарного повідомлення послідовні інтерфейси передають повідомлення фіксованої довжини (вісім двійкових розрядів). Якщо довжина елементарного повідомлення менша, то пристрій сам доповнює повідомлення нулями і лише після цього передає його до каналу зв'язку. Побудова алгоритмів завадозахищеного кодування вимагає врахування співвідношень інформаційних і контрольних розрядів з метою знаходження оптимального режиму передавання: мінімальний обсяг даних – мінімальний час передавання – максимальна ефективність використання каналу з одного боку і максимальна кодова відстань – максимальний захист від завад з іншого. Певні спроби проаналізувати алгоритми завадозахищеного кодування в цьому аспекті вже здійснювались [2, 3]. При цьому розглядались найбільш поширені з них: код Хеммінга та циклічний, оскільки вони найбільш просто алгоритмізуються і дозволяють

здійснювати кодування та декодування в програмному режимі [4, 5]. При цьому сумарна кількість символів буде визначатися:

$$\mathbf{L = N + K}, \qquad (1)$$

де **N** – кількість інформаційних символів повідомлення; **K** – кількість контрольних символів.

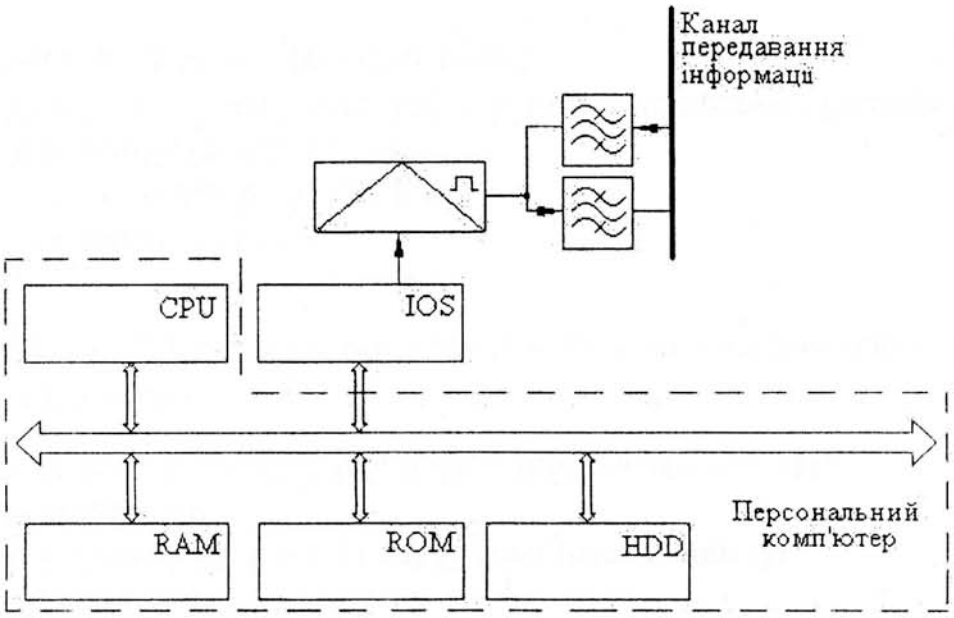

Рисунок 2 – Структура пристрою обміну інформацією

Під час передавання інформації суттєву роль відіграє спроможність коду визначати та виправляти помилки, що в свою чергу залежить від кодової відстані. Для виправлення одніє помилки використовуються код Хеммінга, циклічний тощо. Проведений аналіз можливих варіантів формування кодових слів дозволяє визначити оптимальний з них при передаванні в тих чи інших умовах. У випадку формування помилок пакетного типу необхідно користуватись кодами іншого типу із більшою кодовою відстанню. Виходячи з цього доцільно будувати такий формат коду, щоб загальна кількість його розрядів була кратною восьми, а кодова відстань була максимальною. При цьому код повинен бути нероздільним тобто у посиланні неможливо було б визначити інформаційні та контрольні розряди, що надасть йому умови захищеності від несанкціонованого проникнення.

Найбільш ефективним за принципом завадозахищеності є код з використанням функцій Уолша-Адамара, який має найбільшу кодову відстань d порівняно з іншими типами кодів. Оскільки необхідною вимогою є формування кодових комбінацій в байтовому форматі, то доцільно мати їх довжину у шістнадцять біт (два байти), що дозволяє отримати кодову відстань:

$$d = \frac{n}{2}, \qquad (2$$

де **n** – довжина кодової комбінації.

$$d = \frac{16}{2} = 8$$

Така кодова відстань дозволяє виправляти три помилки, що для такої довжини кодової комбінації недосяжно для інших кодів. У відповідності із правилами побудови складається матриця Адамара, яка має вигляд:

$$H_{16} = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\
1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\
1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1
\end{bmatrix} \qquad (3)$$

Приклад таблиці відповідності між кодовими комбінаціями та інформаційними повідомленнями

Інформаційне повідомлення	Кодова комбінація
00000	1111111111111111
00001	1010101010101010
00010	1100110011001100
00011	1001100110011001
00100	1111000011110000
00101	1010010110100101
00110	1100001111000011
00111	1001011010010110
01000	1111111100000000
01001	1010101001010101
01010	1100110000110011
01011	1001100101100110
01100	1111000000001111
01101	1010010101011010
01110	1100001100111100
01111	1001011001101001
10000	0000000000000000
10001	0101010101010101
10010	0011001100110011
10011	0110011001100110
10100	0000111100001111
10101	0101101001011010
10110	0011110000111100
10111	0110100101101001
11000	0000000011111111
11001	0101010110101010
11010	0011001111001100
11011	0110011010011001
11100	0000111111110000
11101	0101101010100101
11110	0011110011000011
11111	0110100110010110

Замінивши в рядках матриці (–1) на нуль можна отримати перші шістнадцять кодових комбінацій, а потім проінвертувавши їх, можна отримати додаткові шістнадцять кодових комбінацій. Ним у відповідність можна поставити тридцять дві інформаційні кодові комбінації, наприклад як це подано у таблиці. Таблиця відповідності може складатися випадково, що дозволяє досягти однозначності між інформа-ційними повідомленнями та кодовими комбінаціями лише для того, хто цю таблицю складав і для того сеансу обміну інформацією, де вона використовується.

Передавання інформації може здійснюватися в синхронному чи асинхронному режимі з використанням послідовних інтерфейсів, прий-мачів-передавачів або інших програмно-апаратних засобів. Протокол, режим передавання та швидкість визначаються зов-нішніми чинниками і на процес кодування не впливають. Реалізація може здійснюватися для режиму програмного обміну інформацією

чи для режиму переривань, кожний з яких має певні переваги та недоліки.

Використання послідовних універсальних приймачів-передавачів вимагає розбит кодової комбінації на два байти і окремого їх передавання. На приймальному боці прийн байти парами об'єднуються в єдину кодову комбінацію, яка порівнюється з таблиц базових. Якщо помилок під час передавання не виникло, то інформативне повідомлен може бути визначене одразу. У випадку виникнення помилок передавання, кодо комбінація має бути виправлена. Найбільш простим варіантом декодування є порівняння бітах отриманої кодової комбінації з базовими і вибір тієї, яка найбільше відповід отриманій. Цей принцип досить легко алгоритмізується і може реалізовуватись су програмним шляхом без будь-яких апаратних витрат з використанням класич мікропроцесорної структури, поданої на рисунку 2. Програмне забезпечення д приймальної та передавальної частини пристрою можна розроблювати у відповідності схемами, наведеними відповідно на рисунках 3 та 4.

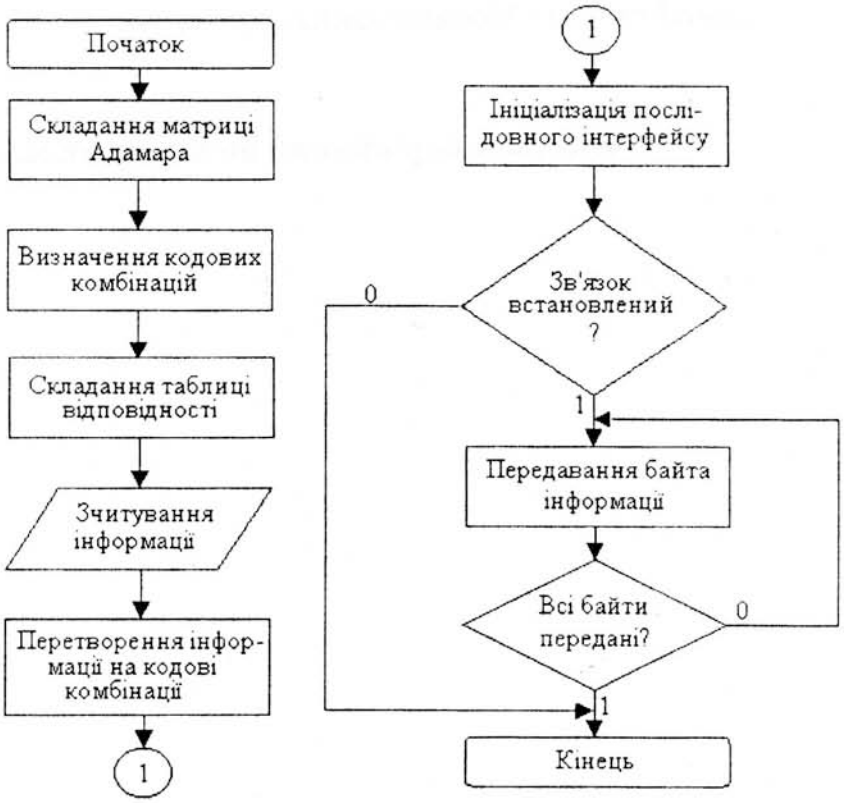

Рисунок 3 – Схема програмного забезпечення передавача

Апаратна реалізація кодувальних та декодувальних пристроїв за класични принципом побудови вимагає розташування контрольних символів у кодовій комбінації н місцях, номер розряду якого відповідає степені двійки. Це дозволяє зразу отримати номе розряду, в якому виникла помилка. Але по-перше це здійснюється лише для виправлен одної помилки, а по-друге суттєво знижує криптографічну стійкість коду, оскільк початково відомі місця розташування інформаційних та контрольних символів. Програм реалізація алгоритму кодування та декодування виключає останній недолік тому, що нема закономірності у розташуванні інформаційних та контрольних розрядів на фіксовани позиціях. Це вже вилучає однозначність кодової комбінації і допускає можливість реалізац складного алгоритму перестановок.

Запропонований алгоритм кодування, який базується на побудові матриці Адамара в принципі не вміщує інформаційних та контрольних символів, тобто є нероздільним. На відміну від алгоритмів Хеммінга та циклічного кодування, в цьому випадку доводиться оперувати не з окремими розрядами, а з цілими комбінаціями. Фактично, байти, що передаються не вміщують інформації. Класичні алгоритми криптографічного захисту інформації з таємним ключем (підстановки та комбінований) вимагають саме цього [5]. При реалізації розробленого алгоритму кодування інформацію вміщує послідовність байтів, що передаються, і таблиця відповідності, складання якої вже реалізує класичний алгоритм підстановки. Можливість перестановок кодових комбінацій у таблиці реалізує алгоритм перестановок. Тобто за своєю суттю розроблений алгоритм завадозахищеного кодування природно вміщує в собі класичний комбінований алгоритм криптографічного закриття інформації. Функцію таємного ключа в даному випадку виконує таблиця перекодування.

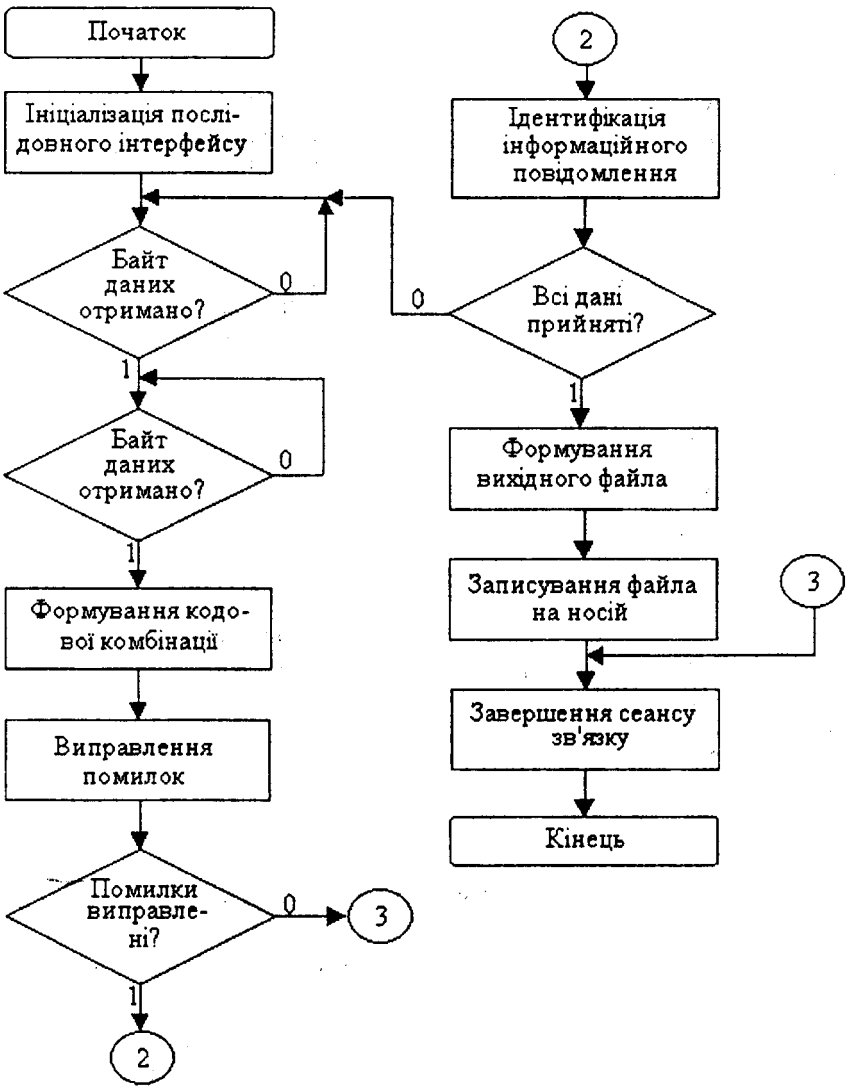

Рисунок 4 – Схема програмного забезпечення приймача

Існує багато критеріїв визначення криптографічної стійкості алгоритмів закриття інформації, але найбільш об'єктивним є імовірнісний, який базується на визначенні кількості можливих переборів варіантів.

Кількість можливих варіантів перестановок комбінацій визначається формулою (4).

$$N_k = k_k ! \tag{4}$$

де k_k - кількість кодових комбінацій.

Складена таблиця визначає відповідність між п'ятьма двійковими інформаційними розрядами та кодовими комбінаціями. Виходячи з цього, зчитану з носія інформацію, що має передаватися, необхідно розбити на інформаційні повідомлення по п'ять двійкових розрядів. Кількість можливих варіантів таких сполучень буде визначатися формулою (5).

$$N_n = C_{8 \cdot N}^{5} \tag{5}$$

де N – об'єм файла, що має передаватися, байт.

З точки зору стороннього спостерігача, якому невідома таблиця відповідності між інформаційними повідомленнями і кодовими комбінаціями, встановлення цього зв'язку, тобто криптографічний аналіз повідомлення є досить складною задачею. Повна кількість можливих варіантів перекодування складає:

$$N_\Sigma = N_k \cdot N_n = k_k ! \cdot C_{8 \cdot N}^{5} = \frac{k_k ! \cdot (8 \cdot N)!}{5! \cdot (8 \cdot N - 5)!} \tag{6}$$

Навіть передавання 100 байт інформації за цим принципом для дешифрування вимагає перебору $7 \cdot 10^{47}$ можливих варіантів, що показує досить високу криптостійкість даного способу.

При цьому немає необхідності реалізовувати два окремі алгоритми – криптографічного закриття і завадозахищеного кодування, оскільки запропонований алгоритм виконує обидві функції.

Список літератури

1. Васюра А.С. та ін. Мікропроцесорні засоби передавання інформації. – Вінниця: ВДТУ, 1998. – 136 с.

2. Кривогубченко С.Г., Компанець М.М., Кулик А.Я. Особливості використання завадозахищених кодів для закриття інформації при передаванні колективними лініями зв'язку // Збірник наукових праць Донецького державного технічного університету, серія "Електротехніка і енергетика", 2000, № 17, с. 65 – 69.

3. Кулик А.Я., Компанець М.М., Кривогубченко С.Г. Аналіз алгоритмів циклічного кодування при передаванні інформації колективними лініями зв'язку // Збірник наукових праць Донецького державного технічного університету, серія "Обчислювальна техніка та автоматика", 2000, № 20, с. 181 – 185.

4. Васюра А.С. та ін. Техніка передавання дискретної інформації. – Вінниця: ВДТУ, 1998 – 101 с.

5. Кулик А.Я. Використання інтерфейсних мікросхем при проектуванні мікропроцесорних засобів автоматики. – Вінниця: ВДТУ, 1999 – 130 с.

Надійшла 21.11.2001