Винахід відноситься до техніки передавання інформації і може використовуватися в інформаційно-вимірювальних системах, комп'ютерних мережах та системах обміну інформацією.

Відомий спосіб передавання та приймання двійкових сигналів та пристрій для його реалізації [А.С. СРСР №1164892, МКІ Н03М13/00, Бюл. "Изобретения стран мира" №18, 1985].

Спосіб полягає в тому, що під час передавання перед кожним імпульсом перетворюваної послідовності формують додатковий, полярність якого встановлюють у відповідності з кореляційним перетворенням полярності імпульсів початкової двійкової послідовності, а під час приймання перед порівнянням кожного сигналу, отриманого після стробування із завданим порогом, визначають його полярність і формують сигнал, що відповідає полярності даного сигналу, отриманого після стробування і сигнал передбачення полярності наступного сигналу, що отримується після стробування в наступний відліковий момент часу у відповідності з кореляційним перетворенням, що здійснюється під час передавання, який порівнюється з сигналом, що відповідає полярності наступного сигналу, отриманого після стробування, а при їх невідповідності збільшують завданий поріг.

Відомий також спосіб кодування та передавання інформації [А.С. СРСР №1432788, МКІ Н03М13/00, бюлетень "Открытия. Изобретения" №39, 1988].

Спосіб вміщує в собі кодування інформаційної послідовності елементарних бінарних сигналів за допомогою частотної маніпуляції з неперервною фазою і наступне передавання модульованого сигналу каналом зв'язку. Завдяки передаванню кожних $n(n \geq 1)$, кодованих згортковим кодом елементарних двійкових сигналів інформаційної послідовності з некодованим елементарним двійковим сигналом цієї самої послідовності, після чого здійснюють частотну модуляцію з неперервною фазою. При цьому забезпечується підвищення швидкості передавання. Кодова відстань лишається незмінною.

Вказані способи мають той недолік, що призначені лише для фіксації помилок, що виникають під час передавання, а не для їх виправлення.

Найбільш близьким по технічній суті є спосіб кодування і передавання інформації із захистом та пристрій для його реалізації [Патент України на винахід №23491 А, МКІ Н03М 13/00, бюлетень "Промислова власність" №4, 1998].

Спосіб вміщує в собі моделювання послідовності елементарних двійкових сигналів і передавання їх каналом зв'язку у вигляді стандартного блока. На передавальному боці чисельними методами розраховуються коефіцієнти ряду Фур'є, отримані гармоніки по черзі відкидають, починаючи з кінця, до тих пір, поки похибка відновлення буде в межах 0,5, досягаючи мінімального складу ряду Фур'є. Отримані коефіцієнти розбивають на байти за правилами комп'ютерного адресування, перетворюють на послідовний код і передають до каналу зв'язку. На приймальному боці елементарні двійкові сигнали зчитують з каналу зв'язку, демодулюють, перетворюють на паралельний код по байтах, вводять до персонального комп'ютера, де за правилами комп'ютерного адресування з них формують коефіцієнти ряду Фур'є довжиною у стандартне машинне слово, розраховують значення функції для аргументу, що дорівнює 1, 2,..., n, де n - довжина стандартного блока інформації, а отримані значення округлюють до найближчого цілого числа.

Вказаний спосіб, як і попередні, розрахований на відновлення сигналу, що формується на передавальному пункті, із завданою похибкою. При цьому не враховуються завади, що діють у каналі зв'язку.

У відповідності із правилами побудови завадозахищених кодів, кодова відстань d визначає:

$$d \geq r + s + 1 \quad (1)$$

де r - кількість помилок, що виправляються;

s - кількість помилок, що виявляються.

Більшість завадозахищених кодів розрахована на виявлення чи виправлення однієї помилки. Причому перші є здебільшого вбудованими до засобів перетворення паралельного коду на послідовний (код з перевіркою на парність), а другі додатково реалізуються у пристроях обміну інформацією (циклічний, Хеммінга тощо). Але на практиці канали зв'язку здебільшого характеризуються наявністю помилок пакетного характеру.

Оскільки практично всі технічні засоби передавання інформації будуються зараз на базі мікропроцесорної техніки, то передавання інформації здійснюється в байтовому форматі (по вісім двійкових розрядів). 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.

Перераховані заходи дозволять уникнути недоліків, які властиві прототипові.

Таким чином, суттєвий ефект може дати побудова завадозахищеного коду з ознаками додаткового захисту від несанкціонованого проникнення.

В основу винаходу покладена задача створення способу кодування інформації, при якому за рахунок введення нових операцій забезпечується захист від завад у лінії зв'язку за рахунок виправлення помилок і захист від несанкціонованого проникнення за рахунок нероздільності коду.

Вказана задача вирішується тим, що на передавальному боці формуються кодові послідовності у відповідності із алгоритмом формування коду, визначається таблиця відповідності інформаційних посилань кодовим послідовностям, дискретна інформація зчитується з носія, розбивається за довжиною на інформаційні повідомлення, перетворюється на кодові послідовності у відповідності із визначеною таблицею, перетворюється на послідовний код і передається до каналу зв'язку. На приймальному боці сигнал приймається з каналу зв'язку, інформація з послідовного коду перетворюється на паралельний, у випадку необхідності виправляються помилки передавання, за допомогою таблиці відповідності кодові комбінації перетворюються на інформаційні повідомлення і записуються на носій.

Суть способу полягає в тому, що за рахунок використання алгоритму побудови коду із максимальною кодовою відстанню для фіксованої кількості розрядів досягається його максимальна завадозахищеність (кількість помилок, що виправляються), а за рахунок алгоритму розбиття даних з носія на інформаційні повідомлення і

побудови таблиці відповідності між інформаційними повідомленнями і кодовими послідовностями з повідомлення вилучається явна інформація, за рахунок чого йому надаються ознаки захищеності від несанкціонованого проникнення.

Відомий пристрій для приймання дискретних сигналів з кореляційним кодуванням по рівню [Авторське свідоцтво СРСР №1164892, МКІ H03M13/00, бюлетень "Изобретения стран мира" №18, 1985], який вміщує в себе блок кодування і формувач сигналів на передавальному боці, а також формувач вхідного сигналу, блок вирішення, регістр зсуву, блок передбачення знаку, блок порівняння, елемент співпадання та інвертор.

Відомий також пристрій для реєстрації способу кодування і передавання інформації [Авторське свідоцтво СРСР №1432788, МКІ H03M13/12, бюлетень "Открытия. Изобретения" №39, 1988], який вміщує в собі комутатори, блок згорткового кодування, блок модуляції та канал зв'язку.

Недоліком даних пристроїв є те, що вони не захищають інформацію, що передається від завад у лінії та від несанкціонованого проникнення.

Найбільш близьким за технічною суттю є пристрій для реалізації способу кодування і передавання інформації із захистом [Патент України на винахід №23491 А, МКІ H03M13/00, бюлетень "Промислова власність" №4, 1998], який вміщує персональний комп'ютер у складі центрального процесора, оперативного запам'ятовувального пристрою, монітора, клавіатури та носія інформації, арифметичного співпроцесора, друкувального пристрою та системного каналу, канал передавання інформації, модем, програмований контролер переривань та послідовний порт, причому модем зв'язаний з каналом передавання інформації, по двонаправленій шині зв'язаний з інформаційним каналом послідовного порту, виходи запитів переривання якого підключені до входів програмованого контролера переривань, а за допомогою системного каналу центральний процесор зв'язаний з арифметичним співпроцесором, постійним та оперативним запам'ятовувальними пристроями, монітором, клавіатурою, друкувальним пристроєм та носієм інформації.

Недоліком цього пристрою є те, що він не враховує впливу завад, що діють у каналі зв'язку.

В основу винаходу поставлена задача удосконалення пристрою кодування дискретної інформації, в якому за рахунок введення нових блоків та зв'язків здійснюється кодування інформації кодом, ознаками якого є байтовий формат (кратність кількості двійкових розрядів восьми) максимальна кодова відстань та нероздільність кодових послідовностей.

Поставлена задача досягається тим, що до пристрою, який вміщує канал передавання інформації та персональний комп'ютер у складі центрального процесора, оперативного запам'ятовувального пристрою, та носія інформації додатково введені послідовний інтерфейс та модем, а також постійний запам'ятовувальний пристрій до складу персонального комп'ютера; причому до каналу передавання інформації підключені канальні вхід та вихід модему, інформаційні вхід та вихід якого з'єднані з послідовним інтерфейсом, за допомогою системного каналу центральний процесор зв'язаний з модулями персонального комп'ютера та послідовним інтерфейсом.

Введення до складу пристрою постійного запам'ятовувального пристрою, послідовного інтерфейсу та модему з відповідними зв'язками та програмним забезпеченням дозволяє суттєво підвищити ефективність передавання за рахунок збільшення завадозахищеності без порушення захисту від несанкціонованого проникнення.

На Фіг.1 наведена схема, що реалізує спосіб кодування дискретної інформації із захистом, на Фіг.2 - схема роботи пристрою в режимі передавання інформації, а на Фіг.3 - схема роботи пристрою в режимі приймання інформації.

Пристрій для кодування дискретної інформації із захистом вміщує канал передавання інформації 1, до якого підключені канальний вхід та вихід модему 2, інформаційні вхід та вихід якого з'єднані з відповідними виходом та входом послідовного інтерфейсу 3, системний канал 4, за допомогою якого центральний процесор 5 зв'язаний з послідовним інтерфейсом 3, оперативним 6 та постійним 7 запам'ятовувальними пристроями, а також носієм інформації 8, що входять до складу персонального комп'ютера 9.

Найбільш ефективним за принципом завадозахищеності є код Адамара [Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. - М.: Связь, 1979. - С. 52-63], 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:

$$d = \frac{n}{2} \quad (2)$$

де n - довжина кодової комбінації.

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

Виходячи з виразу (1) така кодова відстань дозволяє виправляти чотири помилки, що для такої довжини кодової комбінації недосяжно для інших кодів. У відповідності із правилами побудови складається матриця Адамара, яка має вигляд (3).

Замінивши в рядках матриці (-1) на нуль можна отримати перші шістнадцять кодових комбінацій, а потім проінвертувавши їх, можна отримати додаткові шістнадцять кодових комбінацій, їм у відповідність можна поставити тридцять дві інформаційні кодові комбінації, наприклад як це подано у таблиці 1. Таблиця відповідності може складатися випадково, що дозволяє досягти однозначності між інформаційними повідомленнями та кодовими комбінаціями лише для того, хто цю таблицю складав і для того сеансу обміну інформацією, де вона використовується. Кількість можливих варіантів перестановок комбінацій визначається формулою (4).

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).

$$A_{16} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 \end{bmatrix} \quad (3)$$

Таблиця 1

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

$N_k=k_k!$ (4)

де k_k - кількість кодових комбінацій.

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

де N- об'єм файлу, що має передаватися, байт.

Після перекодування інформаційних повідомлень центральним процесором 5 персонального комп'ютера 9, він налаштовує послідовний інтерфейс 3 на обмін інформацією в необхідному режимі. Кодові комбінації розбиваються на байти і за допомогою послідовного інтерфейсу 3 через модем 2 пересилаються до каналу зв'язку 1. Процес продовжується, поки всі кодові комбінації не будуть переслані до приймача.

На приймальному боці центральний процесор 5 постійно опитує послідовний інтерфейс 3 щодо надходження на нього інформації з каналу зв'язку 1 через модем 2. У випадку надходження інформації центральний процесор 3 зчитує її і записує до оперативного запам'ятовувального пристрою 6 персонального комп'ютера 9. Кожні два байти, що надійшли з каналу зв'язку об'єднуються до однієї кодової комбінації, яка порівнюється з базовими, що наявні у таблиці відповідності. Якщо жодна з тридцяти двох базових комбінацій не відповідає отриманій, то вона була спотворена під час передавання лінією зв'язку і з таблиці шляхом побітового порівняння вибирається та, що найбільш близька до отриманої (за умови якнайменшої кількості змінюваних бітів). Якщо кількість бітів, що мають змінюватися перевищує чотири, то умова працездатності коду порушується і зв'язок є неможливим, про що інформується передавальна частина.

Коли з каналу зв'язку 1 через модем 2 і послідовний інтерфейс 3 надходять всі кодові комбінації і вони записані до оперативного запам'ятовувального пристрою 6 персонального комп'ютера 9, зв'язок переривається і центральний процесор 5 розпочинає перекодування отриманих комбінацій на інформаційні повідомлення, з яких належним чином формується вихідний файл і записується на носій 8.

Описаний спосіб вміщує дії у такій послідовності:

- на передавальному боці:

формування кодових комбінацій з використанням матриць Адамара за допомогою персонального комп'ютера 9;

формування персональним комп'ютером 9 таблиці відповідності між інформаційними повідомленнями та кодовими комбінаціями;

зчитування дискретної інформації з носія 8;

перетворення інформації на кодові комбінації центральним процесором 5 персонального комп'ютера 9;

ініціалізація послідовного інтерфейсу 3 і встановлення зв'язку між приймачем та передавачем у завданому режимі;

побайтове передавання кодових комбінацій до каналу зв'язку 1 через послідовний інтерфейс 3 та модем 2;

- на приймальному боці:

побайтове приймання кодових комбінацій з каналу зв'язку 1 через модем 2 та послідовний інтерфейс 3;

об'єднання пари байтів у єдину кодову комбінацію і її порівняння з базовими, що зберігаються у таблиці відповідності, розташованій в оперативному запам'ятовувальному пристрою 6 персонального комп'ютера 9;

виправлення помилок у випадку необхідності шляхом підбирання найбільш близької кодової комбінації за допомогою персонального комп'ютера 9;

перетворення кодових комбінацій на інформаційні повідомлення, що здійснюється центральним процесором 5 персонального комп'ютера 9;

формування вихідного файлу і записування його на носій 8 персонального комп'ютера 9.

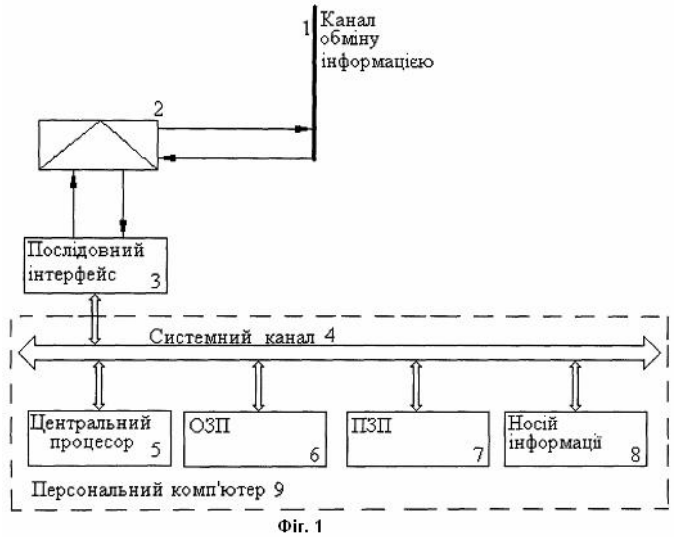
Оскільки для передавання інформації використано код із кодовою відстанню 8, то він може виправляти чотири помилки у кожній кодовій комбінації. Отже завадозахищеність обміну інформацією значно підвищується.

Крім цього формування таблиць відповідності і перекодування інформації, що передається сприяє її захищеності від несанкціонованого доступу. Повна кількість можливих варіантів перекодування складає:

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

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

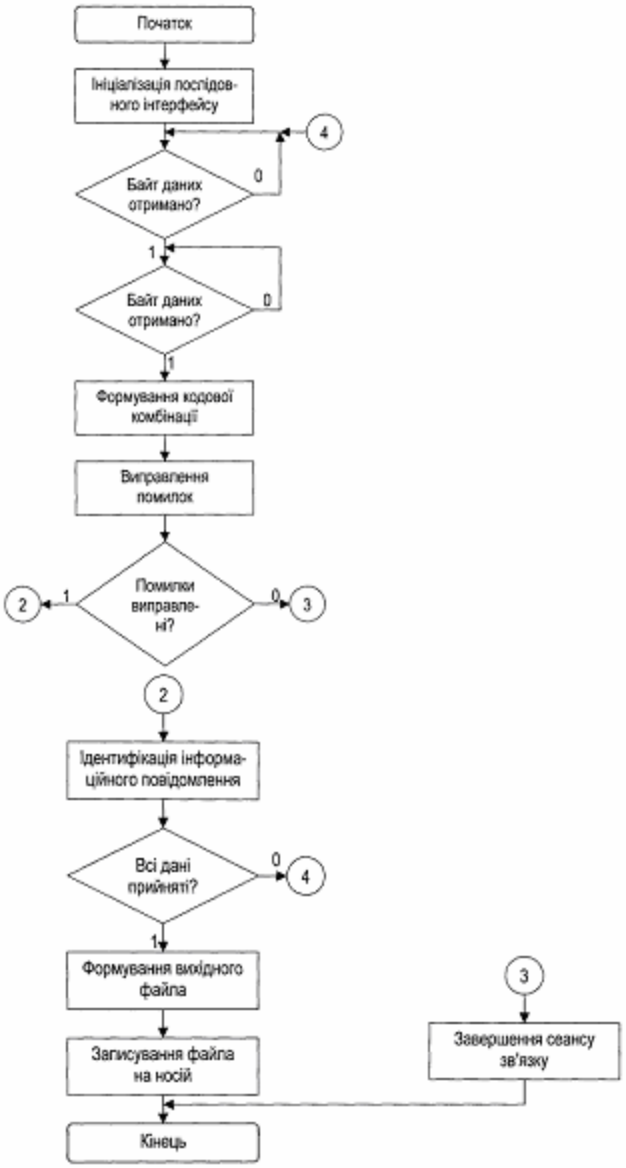
Пропоновані спосіб та пристрій для його реалізації доцільно будувати на базі персонального комп'ютера IBM PC. Послідовні інтерфейси та модеми випускаються серійно.



Фіг. 1


Початок
Складання матриці Адамара
Визначення кодових комбінацій
Складання таблиці відповідності
Зчитування інформації
Перетворення інформації на кодові комбінації
Ініціалізація послідовного інтерфейсу
Зв'язок встановлений?
0
1
Передавання байта інформації
Всі байти передані?
0
1
Кінець

Фіг. 2


Початок
Ініціалізація послідовного інтерфейсу
4
Байт даних отримано?
0
1
Байт даних отримано?
0
1
Формування кодової комбінації
Виправлення помилок
Помилки виправлені?
1
2
0
3
2
Ідентифікація інформаційного повідомлення
Всі дані прийняті?
0
4
1
Формування вихідного файла
Записування файла на носій
3
Завершення сеансу зв'язку
Кінець

Фіг. 3