ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

УКРАЇНА **(19) UA** **(11) 115973** **(13) U**

(51) МПК (2017.01)
H03M 13/00

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2016 07566**
(22) Дата подання заявки: **11.07.2016**
(24) Дата, з якої є чинними права на корисну модель: **10.05.2017**
(46) Публікація відомостей про видачу патенту: **10.05.2017, Бюл.№ 9**

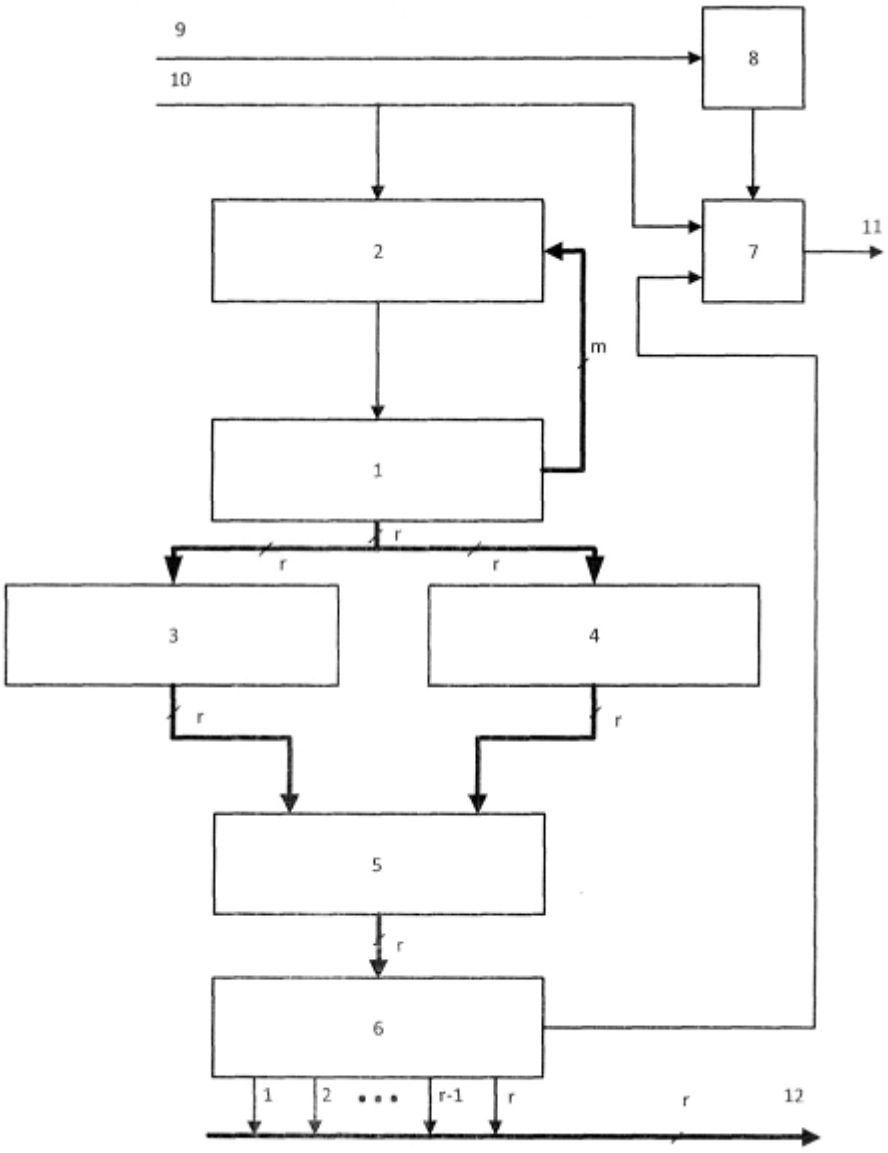
(72) Винахідник(и):
Семеренко Василь Петрович (UA),
Савчук Олександр Ігорович (UA)
(73) Власник(и):
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ,
Хмельницьке шосе, 95, м. Вінниця, 21021 (UA)

(54) ПРИСТРІЙ ДЛЯ КОДУВАННЯ ЦИКЛІЧНИХ КОДІВ

(57) Реферат:

Пристрій для кодування циклічних кодів містить r елементи пам'яті, де r - степінь породжувального полінома циклічного коду, тригер і ключовий елемент, вихід. Перший вхід і керуючий вхід якого з'єднані відповідно з послідовним виходом пристрою, інформаційним входом пристрою та з прямим виходом тригера, вхід якого з'єднаний з керуючим входом пристрою. Додатково містить багатовходовий суматор по модулю два, перший блок суматорів по модулю два, другий блок суматорів по модулю два, схема перемикання і регістр зсув. Послідовний вихід якого з'єднаний з другим входом ключового елемента. Виходи m ($m \le r$) елементів пам'яті з'єднані згідно з видом породжувального полінома циклічного коду з першими m входами багатовходового суматора по модулю два (m+1)-й вхід якого з'єднаний з інформаційним входом пристрою, а вихід - зі входом r-го елемента пам'яті. Виходи всіх r елементів пам'яті також з'єднані з відповідними r входами першого блока суматорів по модулю два та другого блока суматорів по модулю два. Паралельний r-розрядний вихід яких з'єднані відповідно з першим та другим паралельними r-розрядними входами схеми перемикання, паралельний r-розрядний вихід якої з'єднаний з паралельним r-розрядним входом регістра зсуву. Паралельний r-розрядний вихід якого з'єднаний з паралельним r-розрядним інформаційним виходом пристрою, послідовний вихід якого з'єднаний з виходом ключового елемента.

UA 115973 U



Фіг. 1

Корисна модель належить до техніки електрозв'язку і може застосовуватись в системах передачі даних та в комп'ютерних системах, що піддаються впливу завад.

Відомим аналогом є пристрій для кодування циклічних кодів [Авторське свідоцтво СРСР № 1083385, М. кл. Н 04 L 1/10; Н 03 К 13/02, опубл. 30.03.1984р., Бюл. № 12], який містить блок пам'яті, інформаційний регістр введення-виведення інформації, блоки суматорів по модулю два, елемент АБО, блок елементів І, блок вибору старшого розряду коду полінома і регістр коду полінома.

Недоліком аналога є великий час кодування: 7k тактів часу для k-бігового інформаційного повідомлення з одним постійним породжувальним поліномом циклічного коду. Час кодування може бути зменшений лише в режимі передавання інформації групі абонентів і регулярної зміни породжувальних поліномів.

Найближчим аналогом до корисної моделі є пристрій для кодування циклічних кодів [Авторське свідоцтво СРСР № 1448413. М. кл. Н 03 М 13/00, опубл. 30.12.1988р., Бюл. №48], що містить r елементів пам'яті, де r - степінь породжувального полінома, (r-1) перших логічних блоків, другий логічний блок, елемент НІ, два елементи АБО, ключовий елемент і тригер, перший і другий входи якого з'єднані з об'єднаними входами ключового елемента, вихід якого є виходом пристрою, третій вхід ключового елемента є інформаційним входом пристрою, перші і другі виходи перших і других логічних блоків з'єднані з першими І другими входами однойменних елементів пам'яті, перший і другий виходи і-го (i=3…r) елемента пам'яті з'єднані відповідно з першим і другим входами і-го логічного блока та з третім і четвертим входами (і-1)-го логічного блока, перший і другий виходи першого елемента пам'яті з'єднані з першим і другим входами однойменного першого логічного блока та з третім і четвертим входами другого логічного блока, перший і другий виходи другого елемента пам'яті з'єднані з першим і другим входами однойменного першого логічного блока третім і четвертим входами попереднього першого логічного блока та з п'ятим і шостим входами другого логічного блока, третій і четвертий виходи першого логічного блока з'єднані з входами першого елемента АБО, вихід якого з'єднаний з входом ключового елемента, сьомий і восьмий входи другого логічного блока підключені до відповідних виходів тригера, вихід елемента НІ з'єднаний з дев'ятим входом другого логічного блока і з першим входом другого елемента АБО, другий вхід якого підключений до другого виходу тригера, вихід - до п'ятих входів перших логічних блоків, десятий вхід другого логічного блока і вхід елемента НІ об'єднані та підключені до третього входу пристрою.

У відомому пристрої для кодування циклічних кодів процедура кодування закінчується після (k+r)-го такту роботи, де k кількість інформаційних розрядів кодового слова, що передається по каналу зв'язку.

Недоліками найближчого аналога є тривалий час процедури кодування та використання породжувального полінома лише виду g(x) - $1+x+x^h$.

В основу корисної моделі поставлена задача створення пристрою для кодування циклічних кодів, в якому за рахунок введення нових блоків та зв'язків, досягається можливість прискорення операції кодування та розширення функціональних можливостей пристрою.

Поставлена задача вирішується тим, що пристрій для кодування циклічних кодів, складається із r елементів пам'яті, де r - степінь породжувального полінома циклічного коду, тригера і ключового елемента, вихід, перший вхід і керуючий вхід якого з'єднані відповідно з послідовним виходом пристрою, інформаційним входом пристрою та з прямим виходом тригера, вхід якого з'єднаний з керуючим входом пристрою, згідно з корисною моделлю, введені багатовходовий суматор по модулю два, перший блок суматорів по модулю два, другий блок суматорів по модулю два, схема перемикання і регістр зсуву, послідовний вихід якого з'єднаний з другим входом ключового елемента, виходи m ($m \le r$) елементів пам'яті з'єднані згідно з видом породжувального полінома циклічного коду з першими m входами багатовходового суматора по модулю два, (m+1)-й вхід якого з'єднаний з інформаційним входом пристрою, а вихід - зі входом r-го елемента пам'яті, виходи всіх r елементів пам'яті також з'єднані з відповідними r входами першого блока суматорів по модулю два та другого блока суматорів по модулю два, паралельний r- розрядний вихід яких з'єднані відповідно з першим та другим паралельними r-розрядними входами схеми перемикання, паралельний r-розрядний вихід якої з'єднаний з паралельним r- розрядним входом регістра зсуву, паралельний r- розрядний вихід якого з'єднаний з паралельним r- розрядним інформаційним виходом пристрою, послідовний вихід якого з'єднаний з виходом ключового елемента.

Корисна модель пояснюється кресленням, де на фіг. 1 представлена функціональна схема пристрою; на фіг. 2 приклад пристрою для породжувального полінома $g(x)=1+x^3+x^4$.

Пристрій для кодування циклічних кодів даних (фіг. 1) містить r елементів пам'яті 1, де r - степінь породжувального полінома циклічного коду, багатовходовий суматор 2 по модулю два, перший блок суматорів 3 по модулю два, другий блок суматорів 4 по модулю два, схему перемикання 5, регістр зсуву 6, ключовий елемент 7 і тригер 8, вхід якого з'єднаний з керуючим входом 9 пристрою, а вихід з керуючим входом ключового елемента 7, перший вхід якого з'єднаний з інформаційним входом 10 пристрою, виходи m ($m \le r$) елементів пам'яті 1 з'єднані згідно з видом породжувального полінома циклічного коду з першими т входами багатовходового суматора 2 по модулю два, (m+1) -й вхід якого з'єднаний з інформаційним входом 10 пристрою, а вихід - зі входом r-то елемента пам'яті 1, виходи всіх r елементів пам'яті 1 також з'єднані з відповідними r входами першого блока суматорів 3 по модулю два та другого блока суматорів 4 по модулю два, паралельний r- розрядний вихід яких з'єднаний відповідно з першим та другим паралельними r- розрядними входами схеми перемикання 5, паралельний r- розрядний вихід якого з'єднаний з паралельним r- розрядним входом регістра зсуву 6, паралельний r-розрядний вихід якого з'єднаний з паралельним r- розрядним інформаційним виходом 12 пристрою, послідовний вихід 11 якого з'єднаний з виходом ключового елемента 8, другий вхід якого з'єднаний з послідовним виходом регістра зсуву 6.

Приклад пристрою для породжу вального полінома $g(x) = 1 + x^3 + x^4$ (фіг. 2) містить чотири елементи пам'яті 1.1÷1.4, багатовходовий суматор 2 по модулю два, суматор 3.1 першого блока суматорів 3 по модулю два, суматори 4.2÷4.4 другого блока суматорів 4 по модулю два, елементи перемикання 5.1÷5.4 схеми перемикання 5, тригери 6.1-6.4 регістра зсуву 6, ключовий елемент 7, тригер 8, керуючий вхід 9 пристрою, інформаційний вхід 10 пристрою, послідовний вихід 11 пристрою, паралельний r- розрядний вихід 12 пристрою.

Пристрій працює наступним чином.

В початковому стані всі елементи пам'яті 1 і тригер 8 знаходяться в нульовому стані. В підготовчому такті роботи на керуючий вхід 9 пристрою надходить сигнал, який встановлює тригер 8 в стан логічної одиниці. В результаті протягом перших k тактів роботи дозволяється передача k - розрядного інформаційного слова I від інформаційного входу 10 пристрою через ключовий елемент 7 на послідовний вихід 11 пристрою. Одночасно відбувається процес кодування циклічного коду, результатом якого є контрольне слово Ψ.

Елементи пам'яті 1 і багатовходовий суматор 2 утворюють r- розрядну лінійну послідовну схему (ЛПС), за допомогою якої здійснюється систематичне кодування циклічного (n, k) - коду довжиною n і розмірністю k (n-k+r). Нульовий стан елементів пам'яті 1 означає нульовий стан S(0) ЛПС.

Протягом наступних k тактів роботи ЛПС почергово переходить в наступні стани S(t) згідно формули:

$$S(t+1) = A \times S(t) + B \times U(t), \qquad (1)$$

де t - дискретний час; $A = \lfloor a_{ij} \rfloor_{r \times r}$, $B = \lfloor b_{ij} \rfloor_{r \times \ell}$ - характеристичні матриці;

$S(t) = \lfloor s_i \rfloor_r$ - слово стану $U(t) = \lfloor u_i \rfloor_\ell$ - вхідне слово; "x" операція множення по модулю 2, "+ " - операція додавання по модулю 2.

Характеристичні матриці ЛПС мають вигляд:

$$A = \begin{vmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & 1 \\ g_0 & g_1 & g_2 & \dots & g_{r-1} \end{vmatrix}, \quad B = \begin{vmatrix} 0 \\ 0 \\ 0 \\ \dots \\ 1 \end{vmatrix}, \qquad (2)$$

Останній рядок матриці А в (2) містить коефіцієнти породжувального полінома g(x) циклічного коду степені r:

$$g(x) = g_0 + g_1 x + g_2 x^2 + \dots + g_{r-1} x^{r-1} + g_r x^r, \qquad (3)$$

Матриця А визначає внутрішню структуру ЛПС, тобто спосіб з'єднання виходів елементів пам'яті 1 і входів багатовходового суматора 2. Якщо в матриці А елемент $a_{i,j}=1$ ($a_{i,j}=0$), тоді існує зв'язок (відсутній зв'язок) між виходом j-го елемента пам'яті 1 і входом і-го елемента

пам'яті 1. Вхід r-го елемента пам'яті 1 завжди з'єднаний з виходом багатовходового суматора 2. Вихід першого елемента пам'яті 1 завжди з'єднаний з першим входом багатовходового суматора 2 по модулю 2, а інші (m-1) входів якого з'єднані з виходами елементів пам'яті 1 згідно з видом породжувального полінома циклічного коду (3).

Протягом перших k тактів роботи з послідовного входу 10 пристрою на його послідовний вихід 11 буде передано інформаційне слово $I=\imath_1\imath_2 \ldots \imath_k$ починаючи з першого розряду $\imath_1$, і буде сформовано проміжний стан S(k) ЛПС: і-й елемент пам'яті 1 буде зберігати і-й розряд s_i^k стану S(k).

$$S(k)=\begin{bmatrix} s_1^k \\ s_2^k \\ \ldots \\ s_{r-1}^k \\ s_r^k \end{bmatrix}, \qquad (3)$$

На (k+1)-му такті роботи пристрою за допомогою першого блока суматорів 3 формується r-розрядне контрольне слово $\psi=\{\psi_1\psi_2\ldots\psi_r\}$, розряди якого обчислюються за такої системи рівнянь:

$$L_r \times\psi = A^r \times S(k), \qquad (4)$$

де (r×r) - матриця L має вигляд:

$L_r = \lfloor A^{r-1}\times B,\ A^{r-2}\times B, \ldots, A\times B,\ B \rfloor$.

Для характеристичних матриць А і В виду (2) матриця L матиме вигляд:

$$L_r = \begin{bmatrix} 1 & 0 & \ldots & 0 & 0 \\ \ell_{2,1} & 1 & \ldots & 0 & 0 \\ \ell_{3,1} & \ell_{3,2} & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \ell_{r,1} & \ell_{r,2} & \ldots & \ell_{r,r-1} & 1 \end{bmatrix},\ \ell_{i,j}=\{0,1\},\ i\neq j. \qquad (5)$$

Систему рівнянь (4) можна записати у вигляді:

$$\begin{cases} \psi_1 = a_{r,1}s_1^k + a_{r,2}s_2^k + \ldots + a_{r,r}s_r^k,\ GF(2), GF(2); \\ \psi_1\ell_{2,1} + \psi_2 = a_{r-1,1}s_1^k + a_{r-1,2}s_2^k + \ldots + a_{r-1,r}s_r^k,\ GF(2): \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots . \\ \psi_1\ell_{r,1} + \ldots + \psi_{r-1}\ell_{r,r-1} + \psi_r = a_{1,1}s_1^k + a_{1,2}s_2^k + \ldots + a_{1,r}s_r^k,\ GF(2), \end{cases} \qquad (6)$$

де $a_{i,j}$ - (i, j) -та компонента матриці $A^r\ (a_{i,j}\in A^r;\ i=1..r;\ j=1..r)$;

s_i^k - і-й розряд слова стану $S(k)\ \ (s_{i-1}^k \in S_k)$.

Сформовані розряди контрольного слова $\psi=\{\psi_1\psi_2\ldots\psi_r\}$ через схему перемикання 5 записуються у регістр зсуву 6. Далі контрольне слово У передається з регістра зсуву 6 на паралельний r- розрядний вихід 12 пристрою на (k+2)-му такті роботи, або, починаючи з розряду ψ_1, передається протягом r тактів через ключовий елемент 7 на послідовний вихід 11 пристрою.

Можливий також другий спосіб кодування циклічних кодів. В цьому випадку після передачі інформаційного слова $I=\imath_1\imath_2 \ldots \imath_k$ далі протягом наступних r тактів роботи на послідовний вхід 10 пристрою надходять нульові сигнали і на (k+r)-му такті роботи буде сформовано проміжний стан S(n) ЛПС: і-й елемент пам'яті 1 буде зберігати розряд s_i^n стану S(n).

$$S(n)=\begin{bmatrix} s_1^n \\ s_2^n \\ \ldots \\ s_{r-1}^n \\ s_r^n \end{bmatrix}$$

На (n+1)-му такті роботи пристрою за допомогою другого блока суматорів 4 формується r-розрядне контрольне слово $\psi=\{\psi_1\psi_2\ldots\psi_r\}$, розряди якого обчислюються за такої системи рівнянь:

$$L_r \times \psi = S(n), \qquad (7)$$

Систему рівнянь (7) можна записати у вигляді:

$$\begin{cases} \psi_r = s_1^n \\ \psi_r \ell_{2,1} + \psi_{r-1} = s_2^n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots . \\ \psi_r \ell_{2,1} + \ldots + \psi_2 \ell_{r,r-1} + \psi_1 = s_r^n \end{cases}, \qquad (8)$$

де s_i^n - і-розряд слова стану $S(n)$ $\left(s_i^n \in S(n); i = 1 \div r\right)$ S(n),

$\ell_{i,j}$ $-(i,j)$ - та компонента матриці (5).

Сформовані розряди контрольного слова $\psi=\{\psi_1\psi_2\ldots\psi_r\}$ із системи рівнянь (8) через схему перемикання 5 також записуються у регістр зсуву 6. Далі контрольне слово Ψ може бути передано на паралельний r- розрядний вихід 12 пристрою на (n+2)-му такті роботи або передано протягом r тактів через ключовий елемент 7 на послідовний вихід 11 пристрою.

В обох випадках за допомогою пристрою буде сформоване однакове кодове слово

$\iota_1\iota_2\ldots\iota_k\ \psi_1\psi_2\ldots\psi_r$ 1,1₂ …I_AV|/,V(/₂ …\|/,.

Розглянемо приклад кодування першим способом для циклічного (15,11)-коду, що задається породжувальним поліномом $g(x)=1+x^3+x^4$. Характеристичні матриці ЛПС цього коду згідно з (2) мають вигляд:

$$A=\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix},\ B=\begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

Нехай на інформаційний вхід 8 надходить таке інформаційне слово:

$$I = \iota_1\iota_2\iota_3\iota_4\iota_5\iota_6\iota_7\iota_8\iota_9\iota_{10}\iota_{11} = 1\,1\,0\,10\,0\,11\,0\,1\,0;$$

Для обчислення за формулою (1) сформуємо розряди вхідного слова ЛПС:

$$\begin{matrix} U(0)=\iota_1=1; & U(1)=\iota_2=1; & U(2)=\iota_3=0; & U(3)=\iota_4=1; \\ U(4)=\iota_5=0; & U(5)=\iota_6=0; & U(6)=\iota_7=1; & U(7)=\iota_8=1; \\ U(8)=\iota_9=0; & U(9)=\iota_{10}=1; & U(10)=\iota_{11}=0; & \end{matrix}.$$

Стани елементів пам'яті 1.1-1.4 формують 4-розрядний стан ЛПС (фіг.2). Для знаходження стану S(k) для k=11 виконуються обчислення згідно з формулою(1):

$$S(1)=A\times S(0)+B\times U(0)=\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}+\begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}[1]=\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}+\begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}=\begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix};$$

$$S(2)=A\times S(1)+B\times U(1)=\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&1\end{bmatrix}\begin{bmatrix}0\\0\\0\\1\end{bmatrix}+\begin{bmatrix}0\\0\\0\\1\end{bmatrix}[1]=\begin{bmatrix}0\\0\\1\\1\end{bmatrix}+\begin{bmatrix}0\\0\\0\\1\end{bmatrix}=\begin{bmatrix}0\\0\\1\\0\end{bmatrix};$$

. . . .

$$S(11)=A\times S(10)+B\times U(10)=\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&1\end{bmatrix}\begin{bmatrix}1\\1\\1\\1\end{bmatrix}+\begin{bmatrix}0\\0\\0\\1\end{bmatrix}[0]=\begin{bmatrix}1\\1\\1\\0\end{bmatrix}+\begin{bmatrix}0\\0\\0\\0\end{bmatrix}=\begin{bmatrix}1\\1\\1\\0\end{bmatrix};$$

Визначимо контрольне слово Ψ за допомогою системи рівнянь (6). Оскільки структура цієї системи рівнянь буде незмінною для одного й того ж циклічного коду, тому можна наперед визначити r-у степінь матриці А:

$$A^4=A\times A\times A\times A=\begin{bmatrix}1&0&0&1\\1&1&0&1\\1&1&0&1\\1&1&1&0\end{bmatrix}.$$

Далі визначимо матрицю (4):

$$L_4=\left[A^3\times B\ A^2\times B\ \ A\times B\ B\right]=\begin{bmatrix}1&0&0&0\\1&1&0&0\\1&1&1&0\\1&1&1&1\end{bmatrix}.$$

В результаті отримаємо таку систему рівнянь:

$$L_4\times\psi=A^4\times S(11),$$

або, згідно з системою (6):

$$\begin{cases}\psi_1=s_1+s_4\\ \psi_1+\psi_2=s_1+s_2+s_4\\ \psi_1+\psi_2+\psi_3=s_1+s_2+s_3+s_4\\ \psi_1+\psi_2+\psi_3+\psi_4=s_1+s_2+s_3\end{cases},\qquad(9)$$

В результаті розв'язання системи рівнянь (9) отримаємо такі значення розрядів контрольного слова $\psi=\{\psi_1\ \psi_2\ \psi_3\ \psi_4\}$;

$\psi_1=s_1+s_4=1+1=0,$

$\psi_2=s_2=1,$

$\psi_3=s_3=0,$

$\psi_4=s_4=1.$

Ці розряди контрольного слова $\psi=[0\,1\,0\,1]$ формуються після 11-го такту роботи на виходах першого блока суматорів 3.1-3.4 і записуються у відповідні тригери 6.1-6.4 регістра зсуву 6. Далі контрольне слово $\psi=[0\,1\,0\,1]$, починаючи з розряду ψ_1, передається протягом r тактів через ключовий елемент 7 на послідовний вихід 11 пристрою. В результаті буде сформовано кодове слово:

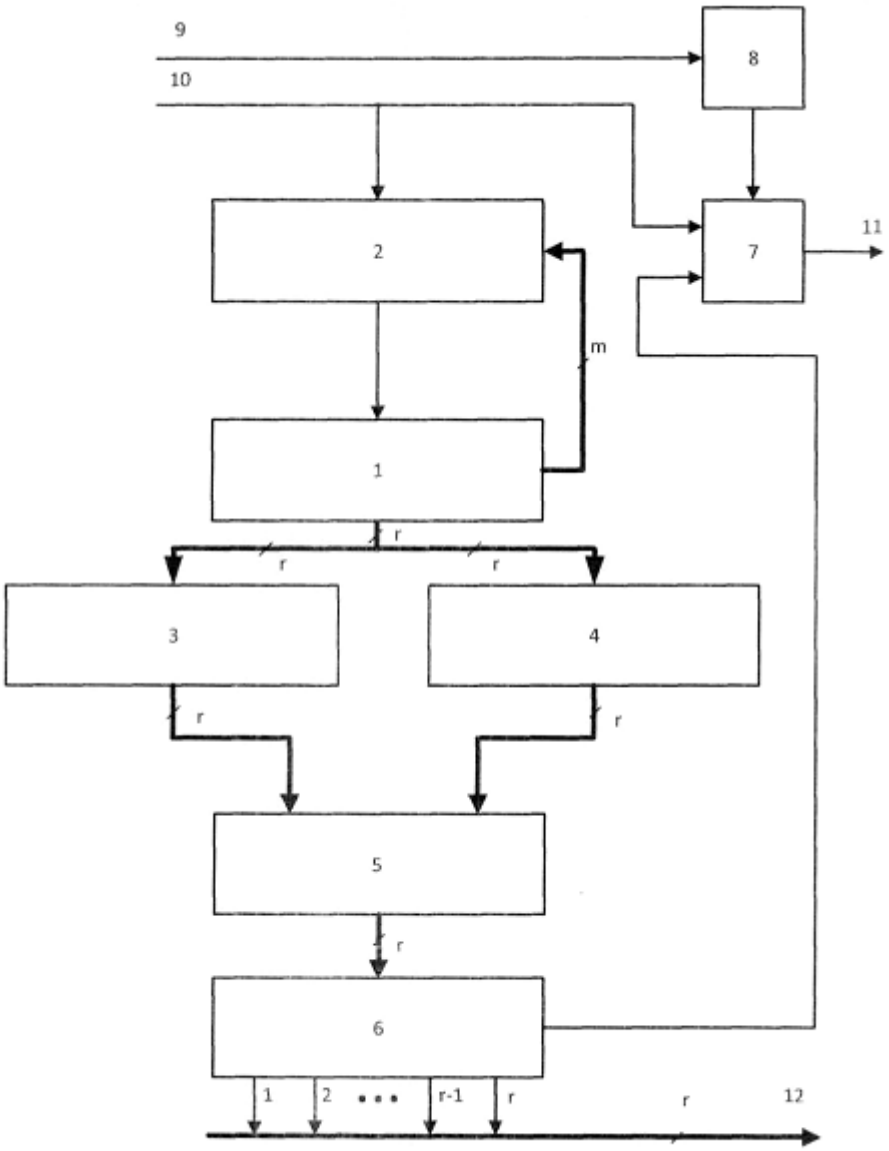
1 1 0 1 0 0 1 1 0 1 0 0 1 0 1.

Аналогічним чином знаходиться розв'язання системи рівнянь (8) і будуть отримані такі ж значення компонент контрольного слова Ψ.

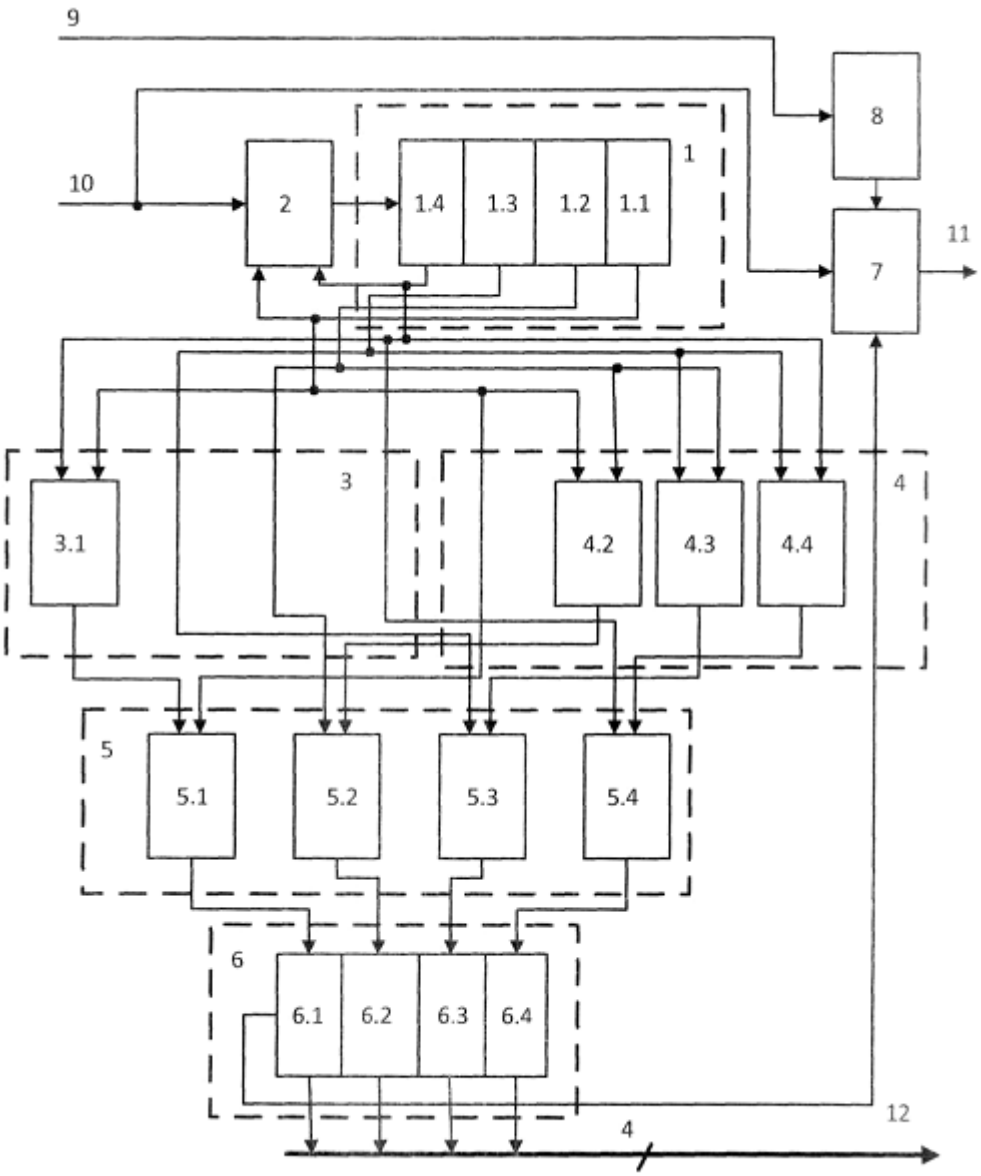
Таким чином, в пристрої можливі чотири варіанти формування і видачі контрольного слова Ψ: паралельний варіант з видачею результату на (k+2)-му такті роботи пристрою, послідовний варіант з видачею результату після (k+r+1)-му такті роботи пристрою, паралельний з видачею результату на (k+r+2) -му такті, послідовний з видачею на (k+2r+1)-му такті роботи пристрою. У відомому пристрою результат кодування видається завжди після n-го такту роботи пристрою. У запропонованому пристрої реалізовано універсальний спосіб систематичного кодування циклічного коду, який не залежить від виду породжувального полінома g(x) коду.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Пристрій для кодування циклічних кодів, що містить r елементи пам'яті, де r - степінь породжувального полінома циклічного коду, тригер і ключовий елемент, вихід, перший вхід і керуючий вхід якого з'єднані відповідно з послідовним виходом пристрою, інформаційним входом пристрою та з прямим виходом тригера, вхід якого з'єднаний з керуючим входом пристрою, який **відрізняється** тим, що додатково містить багатовходовий суматор по модулю два, перший блок суматорів по модулю два, другий блок суматорів по модулю два, схема перемикання і регістр зсуву, послідовний вихід якого з'єднаний з другим входом ключового елемента, виходи m ($m \leq r$) елементів пам'яті з'єднані згідно з видом породжувального полінома циклічного коду з першими m входами багатовходового суматора по модулю два, (m+1)-й вхід якого з'єднаний з інформаційним входом пристрою, а вихід - зі входом r-го елемента пам'яті, виходи всіх r елементів пам'яті також з'єднані з відповідними r входами першого блока суматорів по модулю два та другого блока суматорів по модулю два, паралельний r-розрядний вихід яких з'єднані відповідно з першим та другим паралельними r-розрядними входами схеми перемикання, паралельний r-розрядний вихід якої з'єднаний з паралельним r-розрядним входом регістра зсуву, паралельний r-розрядний вихід якого з'єднаний з паралельним r-розрядним інформаційним виходом пристрою, послідовний вихід якого з'єднаний з виходом ключового елемента.



Фіг. 1



Фіг. 2

Комп'ютерна верстка Л. Ціхановська

Державна служба інтелектуальної власності України, вул. Василя Липківського, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут інтелектуальної власності", вул. Глазунова, 1, м. Київ – 42, 01601