УКРАЇНА

(19) UA (11) 120982 (13) C2

(51) МПК (2020.01)
H03M 13/00
G06F 11/08 (2006.01)
H04L 1/00
G11C 8/10 (2006.01)

МІНІСТЕРСТВО РОЗВИТКУ ЕКОНОМІКИ, ТОРГІВЛІ ТА СІЛЬСЬКОГО ГОСПОДАРСТВА УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА ВИНАХІД

(21) Номер заявки: **a 2018 04082**

(22) Дата подання заявки: **16.04.2018**

(24) Дата, з якої є чинними права на винахід: **10.03.2020**

(41) Публікація відомостей про заявку: **25.10.2019, Бюл.№ 20**

(46) Публікація відомостей про видачу патенту: **10.03.2020, Бюл.№ 5**

(72) Винахідник(и):
Семеренко Василь Петрович (UA),
Халіна Юлія Сергіївна (UA)

(73) Власник(и):
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ,
Хмельницьке шосе, 95, м. Вінниця, 21021 (UA)

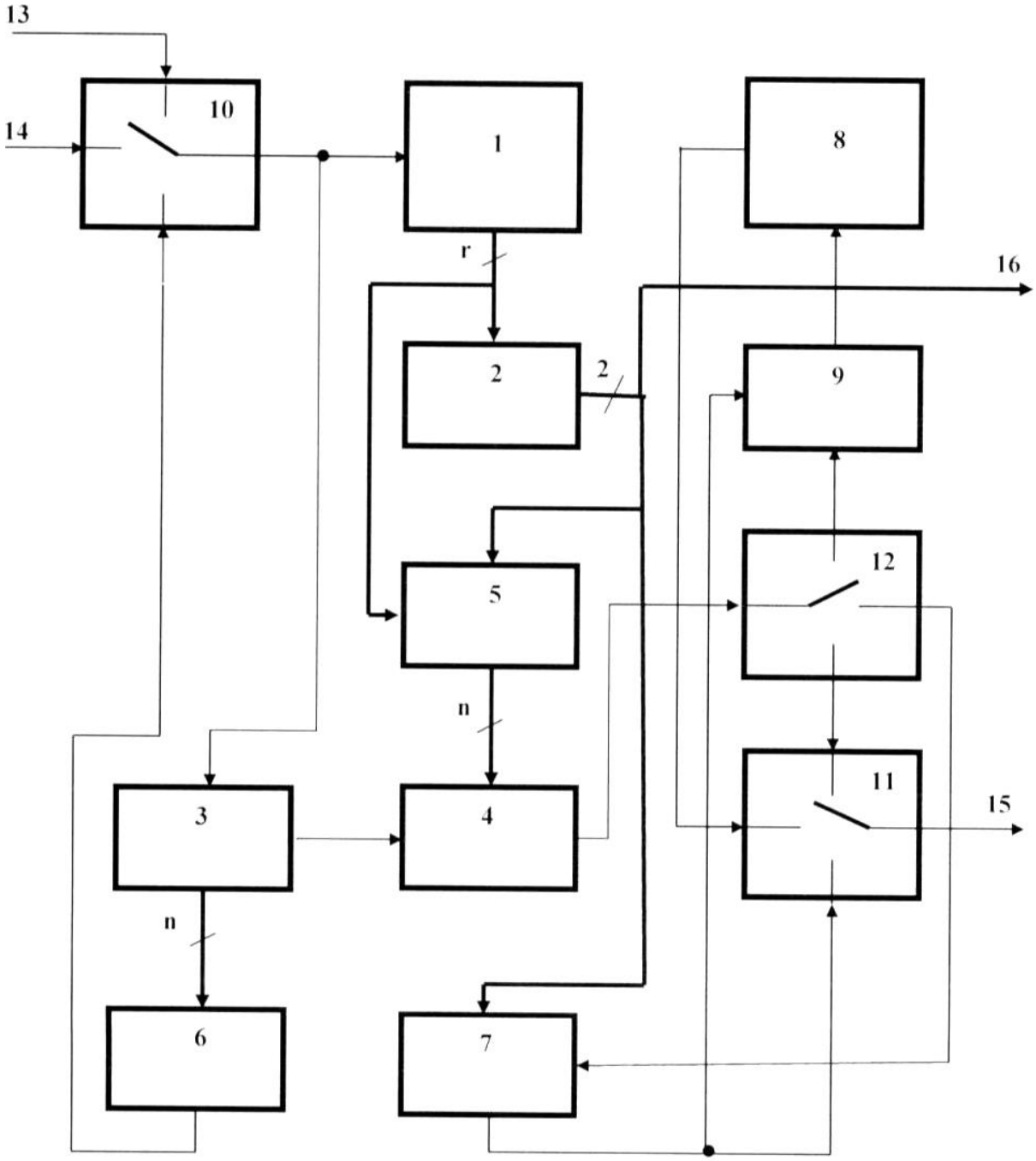
(56) Перелік документів, взятих до уваги експертизою:
UA 107590 U 10.06.2016
UA 84354 U, 25.10.2013
UA 108579 U, 25.07.2016
US 6751770 B2, 15.06.2004
US 3801955 A, 02.04.1974
US 3568148 A, 02.03.1971
Бітченко О. М. Неалгебраїчний декодер коригувальних кодів / О. М. Бітченко, Л. Б. Макаров, О. І. Цопа, Г. Ф. Коняхін // Радиотехника. - 2013. - Вип. 172. - С. 134-140.
Семеренко В. П. Оценка корректирующей способности циклических кодов на основе их автоматных моделей / В. П. Семеренко // Восточно-Европейский журнал передовых технологий. - 2015. - № 2(9). - С. 16-24.
Семеренко В. П. Паралельні циклічні коди / В. П. Семеренко // Вісник Вінницького політехнічного інституту. - 2014. - № 6. - С. 91-98

UA 120982 C2

(54) ПЕРЕСТАВНИЙ ДЕКОДЕР ДВІЙКОВИХ ЦИКЛІЧНИХ (n, k)-КОДІВ

(57) Реферат:

Винахід належить до галузі завадостійкого кодування і може бути використаний в цифрових каналах передачі та збереження даних, зокрема в супутниковому зв'язку, мобільному зв'язку, в комп'ютерних мережах та системах. Перестaвний декодер двійкових циклічних (n, k) кодів складається з лінійної послідовнісної схеми, логічного блока перевірки синдромів, буферного регістра, і коректора помилок, послідовний вхід якого з'єднано з першим послідовним виходом буферного регістра, r-розрядний вихід лінійної послідовнісної схеми з'єднано r-розрядним входом логічного блока перевірки синдромів, введені блок формування слова помилки, блок прямої перестановки, блок оберненої перестановки, "обернену" лінійну послідовну схему, схему АБО і три перемикачі (r=n-k). Технічним результатом, що досягається даним винаходом, є підвищення ступеня виявлення та виправлення помилок циклічними кодами.



Фіг. 1

Винахід належить до галузі завадостійкого кодування і може бути використаний в цифрових каналах передачі та збереження даних, зокрема в супутниковому зв'язку, мобільному зв'язку, в комп'ютерних мережах та системах.

Відомий неалгебраїчний декодер коригувальних кодів [патент України на корисну модель № 84354 м. кл., H04L 1/00, бюл. № 20, 2013], що містить синдромний (n-k)-розрядний регістр зсуву зі зворотними зв'язками (в подальшому лінійна послідовнісна схема), логічний блок перевірки синдромів за заданими критеріями, буферний n-розрядний регістр зсуву, коректор помилок, пристрій розв'язки вхідних сигналів, вихідний ключ, ланцюги з ключами, пристрій виділення інформаційної групи та модифікатор синдрому.

Недоліком відомого пристрою є складність процедури декодування і великий інтервал часу для виявлення помилок.

Найбільш близьким по технічній суті до запропонованою пристрою є модифікований неалгебраїчний декодер коригувальних кодів [патент України на корисну модель № 107590 м. кл., H04L 1/00, бюл. № 11, 2016|, що містить перший пристрій розв'язки вхідних сигналів, перший вхід якого з'єднаний з входом декодера v(x), лінійна послідовнісна схема, вихід старшого розряду якої з'єднано з першим входом модифікатора синдрому, а з виходу молодшого розряду видається інформаційна посилка, яка через перший ключ подається на вихід декодера, виходи кожного тригера лінійної послідовнісної схеми з'єднані з входами логічного блока перевірки синдромів за заданими критеріями, буферний n-розрядний регістр зсуву, вихід якого з'єднаний з першим входом коректора помилок, другий вхід якого з'єднано з другим входом модифікатора синдрому, другий ключ, якого встановлено між виходом (n-k)-го осередку буферного n-розрядного регістра зсуву і третім входом першого пристрою розв'язки вхідних сигналів. Крім цього, в нього додатково введені третій ключ, який одним кінцем з'єднаний з виходом логічного блока перевірки синдромів за заданими критеріями, а другим - з другим входом коректора помилок та першим входом модифікатора синдрому, другий пристрій розв'язки вхідних сигналів, перший вхід якого з'єднано з входом декодера v(x) та першим входом першого пристрою розв'язки вхідних сигналів, другий вхід - з виходом коректора помилок, а вихід з входом буферного n-розрядного регістра зсуву.

Недоліками даного пристрою є залежність його структури від особливостей конкретного двійкового циклічного коду, необхідність попереднього обчислення деяких величин та неможливість виявлення великої кількості можливих комбінацій помилок.

В основу винаходу поставлена задача створення переставного декодера двійкових циклічних (n-k)-кодів при використанні систематичного і несистематичного кодування, а також підвищення кількості виявлених помилок, що дозволить завдяки використанню автоматного представлення циклічних кодів досягнути універсального способу декодування будь-яких двійкових циклічних кодів при їх систематичному або несистематичному кодуванні. Завдяки використанню способу степеневої перестановки кодових слів збільшується ступінь виявлення та виправлення помилок циклічними кодами.

Поставлена задача вирішується тим, що в переставному декодері двійкових циклічних (n,k)-кодів, який складається з лінійної послідовнісної схеми, логічного блока перевірки синдромів, буферного регістра і коректора помилок, послідовний вхід якого з'єднано з першим послідовним виходом буферного регістра, а r-розрядний вихід лінійної послідовнісної схеми з'єднано з r-розрядним входом логічного блока перевірки синдромів, крім того, введені блок формування слова помилки, блок прямої перестановки, блок оберненої перестановки, "обернену" лінійну послідовнісну схему, схему АБО і трьох перемикачів, інформаційний вхід пристрою зв'язаний з першим входом першого перемикача, вхід допоміжних даних пристрою зв'язаний з другим входом першого перемикача, інформаційний вихід пристрою зв'язаний з виходом другого перемикача, дворозрядний керуючий вихід пристрою зв'язаний з дворозрядним керуючим виходом логічного блока перевірки синдромів, з дворозрядним керуючим входом блока формування слова помилки та з дворозрядним керуючим входом блока оберненої перестановки, послідовний вихід якого зв'язаний з першим входом другого перемикача та з першим входом схеми АБО, вихід якої зв'язаний з послідовним входом "оберненої" лінійної послідовнісної схеми, послідовний вихід якої зв'язаний з другим входом другого перемикача, третій вхід якого зв'язаний з першим виходом третього перемикача, вхід якого зв'язаний з виходом коректора помилок, n-розрядний вхід якого зв'язаний з n-розрядним виходом блока формування слова помилки, n-розрядний вхід якого зв'язаний також з r-розрядним виходом лінійної послідовнісної схеми, вихід першого перемикача зв'язаний з послідовним входом лінійної послідовнісної схеми та з послідовним входом буферного регістра, n-розрядний вихід якого зв'язаний з n-розрядним входом блока прямої перестановки, вихід якого зв'язаний з третім входом першого перемикача, другий і третій виходи третього перемикача зв'язані відповідно з

другим входом схеми АБО та з інформаційним входом блока оберненої перестановки (r=n-k), крім того, логічний блок перевірки синдромів містить лічильник, вузол нам'яті, RS-тригер, елемент АБО, елемент І, перший вхід якого з'єднаний з інверсним виходом RS-тригера, S-вхід якого з'єднаний з виходом переносу лічильника, паралельний ($\log\tau$)-розрядний (де τ - максимальна кількість помилок, яку може виправити вибраний циклічний код) вхід якого з'єднаний з інформаційним виходом вузла пам'яті, перший розряд r-розрядного входу блока зв'язаний з входом віднімання лічильника, з другим входом елемента І та з першим входом елемента АБО, решта входів якого з'єднані з рештою розрядів r-розрядного входу блока, виходи елемента АБО і елемента І утворюють дворозрядний керуючий вихід пристрою, блок формування слова помилки містить лічильник, n-розрядний регістр зсуву, RS-тригер, перший елемент І, другий елемент І і третій елемент І, входи якого з'єднані з дворозрядним керуючим виходом пристрою, а вихід з'єднано з S-входом RS-тригера, прямий і інверсний виходи якого з'єднані відповідно з першими входами першого елемента 1 і другого елемента І, на другі входи яких кожного такту надходять синхросигнали з синхровходу, вихід першого елемента 1 з'єднаний з входом віднімання лічильника та з входом зсуву регістра, вихід другого елемента І з'єднаний з входом додавання лічильника, прямий вихід RS-тригера з'єднаний також з входом паралельного запису регістра, вихід якого є n-розрядним виходом блока, а r-розрядний вхід якого з'єднаний зі старшими r розрядами регістра в оберненому порядку, блок прямої перестановки містить n-розрядний регістр зсуву, причому j-й розряд регістра зв'язаний з i-м входом блока за правилом: j=(2i-I) mod n, n - непарне, а блок оберненої перестановки містить перший лічильник, другий лічильник, n-розрядний кільцевий регістр зсуву, перший елемент І, другий елемент І, елемент АБО та інвертор, вихід якого з'єднаний з першим входом першого елемента І, вихід якого з'єднаний з входом додавання першого лічильника, m-розрядний вихід якого з'єднаний з m-розрядним входом другого лічильника, вихід переносу якого з'єднаний з першим входом елемент АБО, другий вхід та вихід якого з'єднані відповідно з виходом другого елемента І та з входом дозволу паралельного запису в другий лічильник, інформаційний вихід якого з'єднаний з входом зсуву регістра, перший (молодший) розряд якого з'єднаний з інформаційним входом блоку, послідовний вихід якого з'єднаний з n-м розрядом регістра, перший розряд дворозрядного керуючого входу блока з'єднаний з другим входом першого елемента І та з першим входом другого елемента І, а другий розряд дворозрядного керуючого входу блока з'єднаний з входом інвертора та з другим входом другого елемента І.

На фіг. 1 представлена функціональна схема пристрою; на фіг. 2 - логічний блок перевірки синдромів; на фіг. 3 - блок формування слова помилки; на фіг. 4 - блок прямої перестановки; на фіг. 5 - блок оберненої перестановки; на фіг. 6 - приклад лінійної послідовнісної схеми (ЛПС) для породжувального поліному $g(x)=1+x^4+x^5+x^6+x^8$; на фіг. 7 приклад "оберненої" ЛПС для породжувального поліному $g(x)=1+x^4+x^5+x^6+x^8$.

Переставний декодер двійкових циклічних (n, k) - кодів (фіг. 1) містить ЛПС 1, логічний блок перевірки синдромів 2, буферний регістр 3, коректор помилок 4, блок формування слова помилки 5, блок прямої перестановки 6, блок оберненої перестановки 7, "обернену" ЛПС 8, схему АБО 9, перший перемикач 10, другий перемикач 11, третій перемикач 12, інформаційний вхід 13 пристрою зв'язаний з першим входом першого перемикача 10, вхід допоміжних даних 14 пристрою зв'язаний з другим входом першого перемикача 10, інформаційний вихід 15 пристрою зв'язаний з виходом другого перемикача 11, дворозрядний керуючий вихід 16 пристрою зв'язаний з дворозрядним керуючим виходом блока 2, з дворозрядним керуючим входом блока 5 та з дворозрядним керуючим входом блока 7, послідовний вихід якого зв'язаний з першим входом другого перемикача 11 та з першим входом схеми АБО 9, вихід якої зв'язаний з послідовним входом "оберненої" ЛПС 8, послідовний вихід якої зв'язаний з другим входом другого перемикача 11, третій вхід якого зв'язаний з першим виходом третього перемикача 12, вхід якого зв'язаний з виходом коректора помилок 4, перший і другий n-розрядний входи якого зв'язані відповідно з першим послідовним виходом буферного регістра 3 та з n-розрядним виходом блока 5, r-розрядний вхід якого зв'язаний з r-розрядним входом блока 2 і з r-розрядним виходом ЛПС 1, вихід першого перемикача 10 зв'язаний з послідовним входом ЛПС 1 та з послідовним входом буферного регістра 3, послідовний і n-розрядний виходи якого зв'язані відповідно з послідовним входом блока 4 із n-розрядним входом блока 6, вихід якого зв'язаний з третім входом першого перемикача 10, другий і третій виходи третього перемикача 12 зв'язані відповідно з другим входом схеми АБО 9 та з інформаційним входом блока 7.

Логічний блок 2 перевірки синдромів (фіг. 2) містить лічильник 17, вузол пам'яті 18, RS-тригер 19, елемент АБО 20, елемент І 21, перший вхід якого з'єднаний з інверсним виходом RS-тригера 19, S-вхід якого з'єднаний з виходом переносу лічильника 17, паралельний $\log\tau$-

розрядний (де τ максимальна кількість помилок, яку може виправити вибраний циклічний код) вхід якого з'єднаний з інформаційним виходом вузла пам'яті 18, перший розряд r-розрядного входу блока зв'язаний з входом віднімання лічильника 17, з другим входом елемента І 21 та з першим входом елемента АБО 20, решта входів якого з'єднані з рештою розрядів r-розрядного входу блока, виходи елемента АБО 20 і елемента І 21 утворюють дворозрядний керуючий вихід 16 пристрою.

Блок 3 формування слова помилки (фіг. 3) містить лічильник 22, n-розрядний регістр зсуву 23, RS-тригер 24, перший елемент І 25, другий елемент І 26 і третій елемент І 27, входи якого з'єднані з дворозрядним керуючим виходом 16 пристрою, а вихід з'єднано з S-входом RS-тригера 24, прямий і інверсний виходи якого з'єднані відповідно з першими входами першого елемента І 25 і другого елемента І 26, на другі входи яких кожного такту надходять синхросигнал і з синхровходу 28, вихід першого елемента І 25 з'єднаний з входом віднімання лічильника 22 та з входом зсуву регістра 23, вихід другого елемента 1 26 з'єднаний з входом додавання лічильника 22, прямий вихід RS-тригера 24 з'єднаний також з входом паралельного запису регістра 23, вихід якого є n-розрядним виходом блока, а r-розрядний вхід якого з'єднаний зі старшими r розрядами регістра 23 в оберненому порядку.

Блок 6 прямої перестановки (фіг. 4) містить n-розрядний регістр зсуву 29, причому j-й розряд регістра 29 зв'язаний з j-м входом блока за правилом:

j=(2i-l)mod n, n-непарне.

Блок 7 оберненої перестановки (фіг. 5) містить перший лічильник 30, другий лічильник 31, n-розрядний кільцевий регістр зсуву 32, перший елемент І 33, другий елемент І 34, елемент АБО 35 та інвертор 36, вихід якого з'єднаний з першим входом першого елемента І 33, вихід якого з'єднаний з входом додавання першого лічильника 30, m-розрядний вихід якого з'єднаний з m-розрядним входом другого лічильника 31, вихід переносу якого з'єднаний з першим входом елемента АБО 35, другий вхід та вихід якого з'єднані відповідно з виходом другого елемента І 34 та з входом дозволу паралельного запису в другий лічильник 31, інформаційний вихід якого з'єднаний з входом зсуву регістра 32, перший (молодший) розряд якого з'єднаний з інформаційним входом блока, послідовний вихід якого з'єднаний з n-м розрядом регістра 32, перший розряд дворозрядного керуючого входу блока з'єднаний з другим входом першого елемента 1 33 та з першим входом другого елемента І 34, а другий розряд дворозрядного керуючого входу блока з'єднаний з входом інвертора 36 та з другим входом другого елемента 1 34.

ЛПС 1 містить r-розрядний регістр зсуву з лінійними оберненими зв'язками, який складається з елементів пам'яті (тригерів) та суматорів за модулем два між окремими елементами нам'яті. Структура лінійних обернених зв'язків визначається вибраним породжувальним поліномом циклічного коду:

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

де коефіцієнти g_i можуть приймати значення $\{0,1\}$, $i = 1 \div r$.

Приклад ЛПС для породжувального поліному $g(x) = 1 + x^4 + x^5 + x^6 + x^8$ (фіг. 6) містить вісім елементів пам'яті 33.1÷33.8, чотири суматори по модулю два 34.1÷34.4, синхровхід 35, інформаційний вхід, r-розрядний інформаційний вихід.

Обернена ЛПС 8 також містить r-розрядний регістр зсуву з лінійними оберненими зв'язками, який складається з елементів пам'яті (тригерів) та суматорів за модулем два між окремими елементами пам'яті. Структура лінійних обернених зв'язків залежить від породжувального поліному (1), але відрізняється від ЛПС 1.

Приклад "оберненої" ЛПС для породжувального поліному $g(x) = 1 + x^4 + x^5 + x^6 + x^8$ (фіг. 7) містить вісім елементів пам'яті 36.1÷36.8, чотири суматори за модулем два 37.1÷37.4, синхровхід 38, інформаційний вхід, r-розрядний інформаційний вихід.

Пристрій працює таким чином.

Теоретичною основою кодування і декодування циклічних кодів є математичний апарат лінійних послідовнісних схем (ЛПС). Двійкова ЛПС, як лінійний автомат, в дискретні такти часу і описується лінійною функцією переходів (станів):

$$S(t+1) = A \times S(t) + B \times U(t), \quad (2)$$

та лінійною функцією виходів:

$$Y(t) = S(t),$$

де $A = \|a_{ij}\|_{r \times r}$, $B = \|b_i\|_r$ - характеристичні матриці ЛПС,

$S = \|s_i\|_r$ - слово стану, $U = \|u_i\|_l$ - вхідне слово, $Y = \|u_j\|_m$ - вихідне слово.

У формулі (2) символи '+' та 'x' позначають відповідно операції додавання та множення за модулем два. Під дією вхідного слова

$U = u(1), u(2), \ldots, u(t)$,

яке надходить на вхід ЛПС, відбувається послідовна зміна її внутрішніх станів

$S = s(1), s(2), \ldots, s(t)$,

для обчислення яких використовується формула (2).

Апаратною реалізацією двійкової ЛПС в пристрої є регістр зсуву з лінійними оберненими зв'язками. Математично структура обернених зв'язків в цьому регістрі описується такими характеристичними матрицями:

$$A = \begin{vmatrix} 0 & 0 & \ldots & 0 & g_0 \\ 1 & 0 & \ldots & 0 & g_1 \\ 0 & 1 & \ldots & 0 & g_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & g_{r-1} \end{vmatrix}, B = \begin{vmatrix} 1 \\ 0 \\ 0 \\ \ldots \\ 0 \end{vmatrix}. \qquad (3)$$

Елементи останнього стовпчика матриці A в (3) являють собою коефіцієнти породжувального полінома (1) циклічного коду.

Матриця A визначає внутрішню структуру ЛПС, тобто спосіб з'єднання між собою елементів пам'яті. Якщо елемент a_{ij} матриці A дорівнює одиниці, тоді повинен існувати зв'язок між виходом j-го елемента пам'яті і входом i-го елемента пам'яті (напряму або через суматор за модулем два), а якщо $a_{ij} = 0$, тоді зв'язок між вказаними елементами пам'яті відсутній. Вхід першого елемента пам'яті завжди з'єднаний з виходом першого суматора за модулем два, перший вхід якого з'єднаний з інформаційним входом 39 ЛПС, а другий вхід - з виходом j-го елемента пам'яті. Кількість суматорів за модулем два дорівнює кількості одиниць в останньому стовпці матриці A.

Матриця B визначає структуру входів ЛПС: якщо елемент b_{ij} матриці B дорівнює одиниці, тоді має існувати зв'язок між j-м входом ЛПС і входом i-го елемента пам'яті, а якщо $b_{ij} = 0$, тоді такий зв'язок відсутній.

Процес кодування циклічного (n, k)-коду полягає в тому, що k-розрядні інформаційні слова відображаються в n-розрядні кодові слова, які і передаються по каналу зв'язку. При систематичному кодуванні інформаційне слово I і контрольне слово Ψ відокремлені один від другого і кодове слово Z 10 можна записати як Z=IΨ. При несистематичному кодуванні k - розрядне інформаційне слово U перетворюється у n-розрядне кодове слово Z, в якому інформаційні та контрольні розряди не містяться в явному вигляді.

Процес декодування циклічних кодів також можна розділити на три етапи:

- встановлення факту відсутності чи наявності помилки в слові Z;
- виправлення помилки при її наявності в слові Z;
- виділення інформаційного слова I в слові Z.

Кожний етап здійснюється протягом однієї або кількох ітерацій. Максимальна тривалість кожної ітерації не перевищує 2n тактів часу. Кожний такт часу складається з r мікротактів.

З позицій автоматного представлення циклічних кодів перший етап полягає в знаходженні стану $S(n)$, в який перейде ЛПС після подачі на її вхід кодового слова. Для цього використовується рекурсивна формула (2), в якій вхідним словом U служить n-розрядне кодове слово Z.

$S(j+1) = A \times S(j) + B \times z_j, GF(2),\ z_j \in Z,\ j = 1 \div n$.

Під час першої ітерації роботи пристрою кодове слово Z записується в буферний регістр 3 і за допомогою ЛПС 1 протягом n тактів 1 відбувається обчислення стану $S(n)$. Стан $S(n)$ прийнято йменувати синдромом помилки: нульове значення цього стану свідчить про відсутність помилок в переданому кодовому слові в межах виявляючої здатності циклічного коду. При наявності помилки кратності т в кодовому слові, яке позначимо як $Z_{err}^{(\tau)}$, буде отримано ненульовий синдром помилки $S_{err}^{(\tau)}$.

Ненульовий синдром помилки може бути регулярним або нерегулярним. Для їх розрізнення використовується перевірочне вікно $X^{(i)}$ - безперервна циклічна послідовність r розрядів

кодового слова Z або слова $Z_{err}^{(\tau)}$, причому крайній правий розряд $X^{(i)}$ є і-м розрядом кодового слова Z. Перевірочне вікно $X^{(i)}$ містить синдром регулярної помилки, якщо і-й розряд кодового слова Z або слова $Z_{err}^{(\tau)}$, містить 1, а всі інші розряди в межах перевірочного вікна містять не більше τ-1 одиниць, де τ - максимальна кількість помилок, який може виправити вибраний циклічний код. У всіх інших випадках перевірочне вікно $X^{(i)}$ містить синдром нерегулярної помилки.

Аналіз синдрому помилки здійснюється за допомогою логічного блока 2 перевірки синдромів. Результат аналізу синдрому помилки, який передається з дворозрядного керуючого виходу блока 2, може мати такі значення синдрому помилки: "00" або "01" нульове значення, "11" ненульове регулярне значення, "10" - ненульове нерегулярне значення.

При нульовому значенні синдрому помилки декодер переходить до третього етапу роботи, під час якого відбувається виділення інформаційного слова I та його порозрядна видача протягом k тактів на інформаційний вихід 15 пристрою. Цей етап роботи залежить від способу формування кодового слова циклічного коду.

При систематичному кодуванні в буферному регістрі 3 після завершення першої ітерації тривалістю n тактів часу в k молодших розрядах кодового слова Z міститься інформаційне слово I і в r старших розрядах контрольне слово Ψ:

$$Z = I\Psi = \iota_1\iota_2\ldots\iota_k\psi_1\psi_2\ldots\psi_r = z_1z_2\ldots z_n,\ r = n-k.$$

Запис слова I в буферний регістр 3 розпочинається із молодшого розряду ι_1. Видача слова I з буферного регістра 3 відбувається протягом другої ітерації тривалістю k тактів часу через коректор помилок 4. При запису і видачі даних буферний регістр 3 працює в режимі прямого зсуву. Для забезпечення шляху передачі даних від буферного регістра 3 до інформаційного виходу 15 пристрою вхід третього перемикача 12 з'єднується з його першим виходом, а третій вхід другого перемикача 11 з'єднується з його виходом.

При несистематичному кодуванні на послідовний вхід ЛПС 1 подається протягом першої ітерації n-розрядне кодове слово Z, тоді інформаційне слово I формується в ЛПС 1 протягом останніх k тактів часу. Оскільки результат перевірки правильності передачі даних за допомогою синдрому помилки формується лише в кінці першої ітерації, тому безпомилкове інформаційне слово I передати на вихід 15 пристрою можна лише на другій ітерації його роботи. Щоб знову отримати слово I можна обнулити ЛПС 1 і знову подати на її вхід слово Z.

Скоротити час формування інформаційного слова I можна за допомогою "оберненої" ЛПС 8. Обернена ЛПС 8, як лінійний автомат, в дискретні моменти часу t описується лінійною функцією переходів (станів):

$$S(t) = A_{inv} \times (S(t+1) + B \times U(t)),\ GF(2). \qquad (4)$$

та лінійною функцією виходів:

$$Y(t) = S(t),$$

Початковим станом "оберненої"" ЛПС 8 є нульове слово, а вхідним словом $U(t)$ в (4) служить n-розрядне кодове слово Z, причому дані мають надходити в протилежному порядку, ніж в першій ітерації (першим на вхід "оберненої"" ЛПС 8 надходить розряд z_n кодового слова Z, який надійшов останнім).

$$S(t) = A_{inv} \times (S(t+1) + B \times z_{n-j}),\ z_{n-j} \in Z,\ j = 1 \div n\ GF(2).$$

Для переходу від матриці A до матриці A_{inv} необхідно виконати такі операції [3]:

1) циклічно зсунути доверху всі рядки матриці A;

2) в отриманій матриці циклічно зсунути вправо всі стовпці.

В результаті протягом перших k тактів роботи "оберненої" ЛПС 8 із несистематичного n-розрядного кодового слова Z знову буде сформоване k-розрядне інформаційне слово I.

Для забезпечення шляху передачі слова I від "оберненої" ЛПС 8 до інформаційного виходу 15 пристрою другий вхід другого перемикача 11 з'єднується з його виходом.

Отримання після першої ітерації в ЛПС 1 ненульового регулярного синдрому помилки $S_{err}^{(\tau)}(t)$ свідчить про те, що всі помилки кодового слова $Z_{err}^{(\tau)}$ попали в перевірочне вікно $X^{(i)}$, тобто, помилкові розряди знаходяться в інтервалі $z_i \div z_j$, де $j = (i-r+1) \bmod n$. Для виправлення цих помилок блок 2 дозволяє передати синдром помилки $S_{err}^{(\tau)}(t)$ із ЛПС 1 в блок 5 і зсунути його на і розрядів в бік старших розрядів слова $Z_{err}^{(\tau)}$. В результаті в блоці 5 буде сформоване n-розрядне слово помилки $E^{(i)}$. Далі відбувається зчитування по одному розряду відповідно слова помилки

$E^{(i)}$ із блока 5 та кодового слова $Z_{err}^{(\tau)}$ із буферного регістра 3 та їх передачу на входи блока 4. В блоці 4 за допомогою суматора по модулю 2 протягом n тактів другої ітерації відбувається виправлення помилок в слові $Z_{err}^{(\tau)}$ і отримання безпомилкового кодового слова Z:

$$Z = Z_{err}^{(\tau)} + E^{(i)}, GF(2).$$

Одночасно протягом перших k тактів другої ітерації відбувається виділення інформаційного слова I із кодового слова Z способом, яке залежить від способу кодування слова Z.

При систематичному кодуванні слова Z перші k виправлених розрядів слова Z, які утворюють k-розрядне інформаційне слово I, із блока 4 надходять на інформаційний вихід 15 пристрою. Для забезпечення шляху передачі слова I від блока 4 до інформаційного виходу 15 пристрою вхід третього перемикача 12 з'єднується з його першим виходом, а також третій вхід другого перемикача 11 з'єднується з його виходом.

При несистематичному кодуванні слова Z виділення інформаційного слова I із виправленого кодового слова Z відбувається за допомогою "оберненої" ЛПС 8. На послідовний вхід "оберненої" ЛПС 8 надходить виправлене кодове слово Z із блока 4 через схему АБО 9 при з'єднанні входу третього перемикача 12 з його другим виходом.

Для забезпечення шляху передачі слова I від "оберненої" ЛПС 8 до інформаційного виходу 15 пристрою другий вхід другого перемикача 11 з'єднується з його виходом.

Отримання після першої ітерації в ЛПС 1 ненульового нерегулярного синдрому помилки $S_{err}^{(\tau)}(t)$ свідчить про те, що не всі помилки кодового слова $Z_{err}^{(\tau)}$ попали в перевірочне вікно $X^{(i)}$. Тому далі декодер переходить до наступної ітерації роботи, протягом якої формуються чергові стани S(t) ЛПС 1 при нульових вхідних сигналах згідно з формулою

$$S(j+1) = A \times S(j).$$

Якщо протягом цієї ітерації буде отримано регулярний стан S(t) тоді далі відбувається виправлення в слові знайденої помилки кратності не більше τ, як було описано раніше.

В протилежному випадку відбувається циклічна степенева перестановка розрядів кодового слова $Z_{err}^{(\tau)}$, яка еквівалентна множенню на 2^{υ} по модулю n відповідного показника степеня коефіцієнта кодового полінома

$$z(x) = z_0 + z_1 x + z_2 x^2 + \ldots + z_{n-1} x^{n-1}.$$

В результаті циклічної степеневої перестановки кодового слова $Z_{err}^{(\tau)} = z_0 z_1 z_2 \ldots z_{n-1}$ (n-непарне) буде отримано переставлене кодове слово $Z_{err,\,p}^{(1)}$, в якому розряди переставлені по правилу

$$z_j^{''} = z_i,\ j = (2i-1) \bmod n,\ z_i \in Z_{err}^{(\tau)},\ z_j^{''} \in Z_{err,\,p}^{(1)}. \quad (5)$$

Наприклад, для кодового слова $Z_{err}^{(\tau)} = z_0 z_1 z_2 z_3 z_4 z_5 z_6$ переставлене кодове слово буде $Z_{err,\,p}^{(1)} = z_0 z_2 z_4 z_6 z_1 z_3 z_5$.

Циклічна степенева перестановка кодового слова $Z_{err}^{(\tau)}$ відбувається за допомогою блока 6 прямих перестановок. Переставлене кодове слово $Z_{err,\,p}^{(1)}$, з виходу блока 6 протягом наступної ітерації тривалістю n тактів надходить на вхід ЛПС 1 та на вхід буферного регістра 3. Для забезпечення шляху передачі слова $Z_{err,\,p}^{(1)}$ від блока 6 до входів ЛПС 1 та буферного регістра 3 третій вхід першого перемикача 10 з'єднується з його виходом.

В кінці цієї ітерації в буферному регістрі 3 буде записано слово $Z_{err,\,p}^{(1)}$, а в ЛПС 1 буде сформовано новий синдром помилки $S_{err,\,p}^{(\tau)}(t)$.

Отримання в ЛПС 1 ненульового регулярного синдрому помилки $S_{err,\,p}^{(\tau)}$ свідчить про те, що всі помилки кодового слова $Z_{err,\,p}^{(1)}$ попали в перевірочне вікно $X^{(i)}$, тоді далі відбувається його виправлення раніше описаним способом. Далі вхід третього перемикача 12 з'єднується з його третім виходом і виправлене кодове слово $Z_p^{(1)}$ з блока корекції 4 надходить на вхід блока 7 оберненої перестановки, в якому формується відновлене кодове слово Z.

Якщо кодове слово $Z_p^{(1)}$ було отримано систематичним кодуванням, тоді з виходу блока 7 виправлене і відновлене інформаційне слово I надходить на інформаційний вихід 15 пристрою.

Для забезпечення шляху передачі слова I від блока 7 до інформаційного виходу 15 пристрою перший вхід другого перемикача 11 з'єднується з його виходом.

При несистематичному кодуванні слова $Z_p^{(1)}$ виділення інформаційного слова I із виправленого і відновленого кодового слова Z відбувається за допомогою "оберненої" ЛПС 8. На послідовний вхід "оберненої"" ЛПС 8 надходить виправлене і відновлене кодове слово Z із блока 7 через елемент АБО 9. Для забезпечення шляху передачі слова I від "оберненої" ЛПС 8 до інформаційного виходу 15 пристрою другий вхід другого перемикача 11 з'єднується з його виходом.

Отримання в ЛПС 1 ненульового нерегулярного синдрому помилки $S_{err,\,p}^{(\tau)}(t)$) свідчить про те, що не всі помилки кодового слова $Z_{err,\,p}^{(1)}$ попали в перевірочне вікно $X^{(i)}$, тоді далі відбувається його нова перестановка раніше описаним способом.

Циклічна степенева перестановка для кожного породжувального полінома циклічного коду має свою кількість w зазначених перестановок, після яких відбувається повернення до початкового кодового слова Z.

Якщо після w зазначених перестановок не вдалося отримати в ЛПС 1 ненульового синдрому регулярної помилки $S_{err}^{(\tau)}(t)$, тоді це означатиме неможливість виправлення $Z_{err}^{(\tau)}$. внаслідок недостатньої коректувальної властивості вибраного породжувального полінома циклічного коду.

Логічний блок 2 перевірки синдромів працює таким чином.

На початку кожного такту роботи пристрою RS-тригер 19 по R-входу встановлюється в нульове значення і у вузол пам'яті 18 записується число τ, де τ - максимальна кількість помилок, яку може виправити вибраний циклічний код. Після закінчення першої ітерації роботи пристрою на r-розрядний вхід блока надходить з r-розрядного виходу ЛПС 1 синдром помилки $S_{err}^{(\tau)}(t)$. Якщо синдром помилки $S_{err}^{(\tau)}(t)$ буде нульовим, тоді на всі r входів елемента АБО 20 надходять нульові логічні значення і на виході цього елемента та виході першого розряду дворозрядного керуючого виходу блока 2 буде нульове значення. Тому на дворозрядному керуючому виході блока 2 будуть сформовані значення "00" або "01".

Якщо було отримано ненульове значення синдрому помилки $S_{err}^{(\tau)}(t)$, тоді для цього стану та всіх наступних станів S(t) ЛПС 1 визначається їх належність до регулярному типу стану. З цією метою в лічильник 17 із вузла пам'яті 18 записується паралельний код числа τ. На кожному мікротакті роботи пристрою один розряд r-розрядного слова стану послідовно передається із останнього елемента пам'яті ЛПС 1 на вхід віднімання лічильника 17. Кожний одиничний розряд слова стану ЛПС 1 зменшує вміст лічильника 17.

Якщо після r мікротактів роботи кількість одиничних розрядів слова стану перевищить число $\tau-1$, тоді в лічильнику 17 виникне сигнал переносу, який встановить по S-входу RS-тригер 19 в одиничне значення. В результаті на одному вході і на виході елемента I 21 будуть нульові значення, тому на дворозрядному керуючому виході блока 2 буде сформоване значення "10", що свідчитиме про ненульове нерегулярне значення чергового слова стану ЛПС 1.

Якщо після r мікротактів роботи кількість одиничних розрядів слова стану не перевищить число $\tau-1$, тоді в лічильнику 17 не виникне сигнал переносу і RS-тригер 19 залишиться в початковому нульовому значенні. В результаті на обох входах і на виході елемента I 21 будуть одиничні значення, тому на дворозрядному керуючому виході блока 2 буде сформоване значення "11", що буде свідчити про ненульове регулярне значення чергового слова стану ЛПС 1.

Блок 3 формування слова помилки працює таким чином.

На початку кожної ітерації лічильник 22, регістр 23 та RS-тригер 24 встановлюються в нульове значення. В цьому стані синхросигнали кожного такту проходять одночасно з синхровходу 28 та через елемент I 26 на вхід додавання лічильника 22.

Як тільки в ЛПС 1 буде виявлено регулярний тип стану S(t), тоді на дворозрядному керуючому вході 16 пристрою буде сформовано код "11", який надходить також на входи елемента I 27. В результаті RS-тригер 24 перемикається в одиничний стан, який дозволяє записати стан S(t) через r-розрядний вхід блока в регістр 23. Одночасно синхросигнали кожного такту з синхровходу 28 проходять вже через елемент I 25 на вхід віднімання лічильника 22 та одночасно на вхід зсуву регістра 23. На кожному наступному такті виконується операція циклічного зсуву вправо (в бік старших розрядів) вмісту регістра 23, тобто стану S(t). Як тільки лічильник 22 досягне нульового значення регістр 23 перестає виконувати операцію зсуву. В результаті в блоці буде сформовано слово помилки E.

Блок 6 прямої перестановки працює таким чином.

На вхід блока надходить n (n-непарне) розрядів кодового слова $Z_{err}^{(\tau)}$, а в регістр 29 паралельно записується вже переставлене кодове слово $Z_{err,\,p}^{(1)}$, в якому вхідні розряди слова $Z_{err}^{(\tau)}$ переставлені по правилу (5), причому $v = \frac{n+1}{2}$. З виходу блока кодове слово $Z_{err,\,p}^{(1)}$ передається по одному розряду кожного такту, починаючи з молодшого розряду $z_1^{"}\left(z_1^{"} \in Z_{err,\,p}^{(1)}\right)$.

Блок 7 оберненої перестановки працює таким чином.

Перед початком роботи пристрою кільцевий регістр зсуву 32 встановлюється в нульове значення, в перший лічильник 30 записується одиниця, а в другий лічильник 31 нуль. На дворозрядний керуючий вхід блока надходить код стану ЛПС 1. З кожним приходом коду "10" (нерегулярний тип стану) перший лічильник 30 збільшує свій стан на одиницю. Якщо приходить код "01" (регулярний тип стану), тоді поточний вміст m стану першого лічильника 30 паралельно записується в другий лічильник 31.

Кожного наступного такту часу на інформаційний вхід 37 блока приходить один розряд кодового слова $Z_p^{(1)}$. Протягом одного такту часу один розряд кодового слова $Z_p^{(1)}$ спочатку записується в перший (молодший) розряд регістра 32, а далі другий лічильник 31 формує m сигналів зсуву, в результаті чого відбувається кільцевий зсув вмісту регістра 32 в бік старших розрядів на 2m розрядів. З кожним сигналом зсуву вміст другого лічильника 31 зменшується на одиницю і з досягненням значення нуля сигнали зсуву перестають надходити.

З кожним наступним тактом часу в другий лічильник 31 перезаписується значення m із першого лічильника 30. Через n тактів часу в регістрі 32 буде сформоване відновлене кодове слово Z, яке далі потактно видається на інформаційний вихід 38 блока.

Розглянемо на прикладі декодування циклічного (17,9)-коду з породжувальним поліномом $g(x) = 1 + x^3 + x^4 + x^5 + x^8$, якому відповідають такі характеристичні матриці ЛПС 1:

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

Нехай на вхід декодера надійшло таке систематичне кодове слово:

$Z_{err}^{(\tau)} = 10001000010001100$. (6)

Спочатку за допомогою ЛПС 1 протягом 17 тактів формуються слова станів згідно з функцією (2):

$S(0) = 00000000;$

$S(1) = A \times S(0) + B \times z_0 = 00000000 + 10000000 = 10000000;$

$S(2) = A \times S(1) + B \times z_1 = 01000000 + 00000000 = 01000000;$

. . . . . .

$S(16) = A \times S(15) + B \times z_{15} = 10011111 + 00000000 = 10011111;$

$S(17) = A \times S(16) + B \times z_{16} = 11010010 + 00000000 = 11010010.$

Стан $S(17)$ з синдромом помилки $S_{err}^{(\tau)}(t)$. Отримання ненульового синдрому помилки свідчить про наявність помилок в кодовому слові (6). Заданий циклічний код має мінімальну кодову відстань $d_{min} = 5$, яка дозволяє виправляти помилки кратності $\tau = 1$ або $\tau = 2$. Тому стан $S(17)$ є ознакою ненульового синдрому нерегулярної помилки. Тому декодер переходить до другого етапу роботи - виправлення помилок.

Протягом наступних тактів першої ітерації ЛІ 1С 1 продовжує формувати слова станів S(t) при нульових вхідних значеннях:

$S(18) = A \times S(17) = 11110101;$

$S(19) = A \times S(18) = 11100110;$

. . . . . .

$S(33) = A \times S(32) = 10011111;$

$S(34) = A \times S(33) = 11010011.$

Оскільки жодного регулярного стану не отримано, тому далі відбувається степенева перестановка розрядів отриманого кодового слова за правилом (6):

$Z^{(1)}_{err,\,p} = 10100001000001010.$ (7)

Далі за допомогою ЛПС 1 протягом перших 17 тактів другої ітерації формуються слова станів згідно з функцією (2) за умови, що на вхід ЛПС 1 надходить кодове слово (7):

$S(0) = 00000000;$

$S(1) = A \times S(0) + B \times z_0 = 00000000 + 10000000 = 10000000;$

$S(2) = A \times S(1) + B \times z_1 = 01000000 + 00000000 = 01000000;$

. . . . . .

$S(16) = A \times S(15) + B \times z_{15} = 00111111 + 10000000 = 10111111;$

$S(17) = A \times S(16) + B \times z_{16} = 11000011 + 00000000 = 11000011.$

Протягом наступних тактів другої ітерації ЛПС 1 продовжує формувати слова станів S(t) при нульових вхідних значеннях:

$S(18) = A \times S(17) = 11111101;$

$S(19) = A \times S(18) = 11100010;$

. . . . . .

$S(24) = A \times S(23) = 10001000.$

Отже, на такті 24 другої ітерації отримано регулярний стан $S(24)$, що свідчить про можливість виправлення виявленої помилки. Тому далі за допомогою блока 5 відбувається формування 17-розрядного слова помилки. Спочатку формується базове слово помилки

$E_{base} = 00000000000010001,$

а далі воно циклічно зсувається вправо на (24-17) позицій

$E^{(7)} = 00100010000000000.$ (8)

Далі слово помилки (8) порозрядно додається до кодового слова (7), в результаті буде отримано виправлено переставлене кодове слово

$Z^{(1)}_{p} = 10000011000001010.$

Нарешті, за допомогою блока 7 формується початкове виправлене кодове слово:

$Z = 10000000010011100.$

Перевагою запропонованого пристрою в порівнянні з відомим пристроєм є його універсальна апаратна структура, яка не залежить від особливостей конкретного циклічного коду. В запропонованому пристрої немає потреби в попередньому обчисленні будь-яких величин і забезпечується більший ступінь виявлення та виправлення помилок. Кількість тактів роботи для виявлення та виправлення помилок залежить від етапу роботи декодера, довжини n коду та кількості w перестановок. В таблиці 1 наведені дані про тривалість тактів роботи запропонованого декодера в залежності від типу помилок.

Зі збільшенням кратності помилок, які потрібно виправити, збільшується кількість перестановок і, відповідно, тривалість роботи пристрою.

Таблиця 1

Часові параметри переставного декодера циклічних (n, k)-кодів

Етапи роботи декодера	Мінімальна кількість тактів роботи декодера	Максимальна кількість тактів роботи декодера
Виявлення помилок різних типів	n	n
Виправлення помилок регулярного типу	n	2n
Виправлення помилок нерегулярного типу	n(2w+1)	2n(w+1)

В таблиці 2 наведені дані про ступінь виправлення помилок різної кратності запропонованим декодером для коду Голея в залежності від кількості перестановок. У відомому пристрої не виявляється і не виправляється 8-10 % можливих комбінацій помилок.

Таблиця 2

Ступінь виправлення помилок для (23,12)-коду Голея

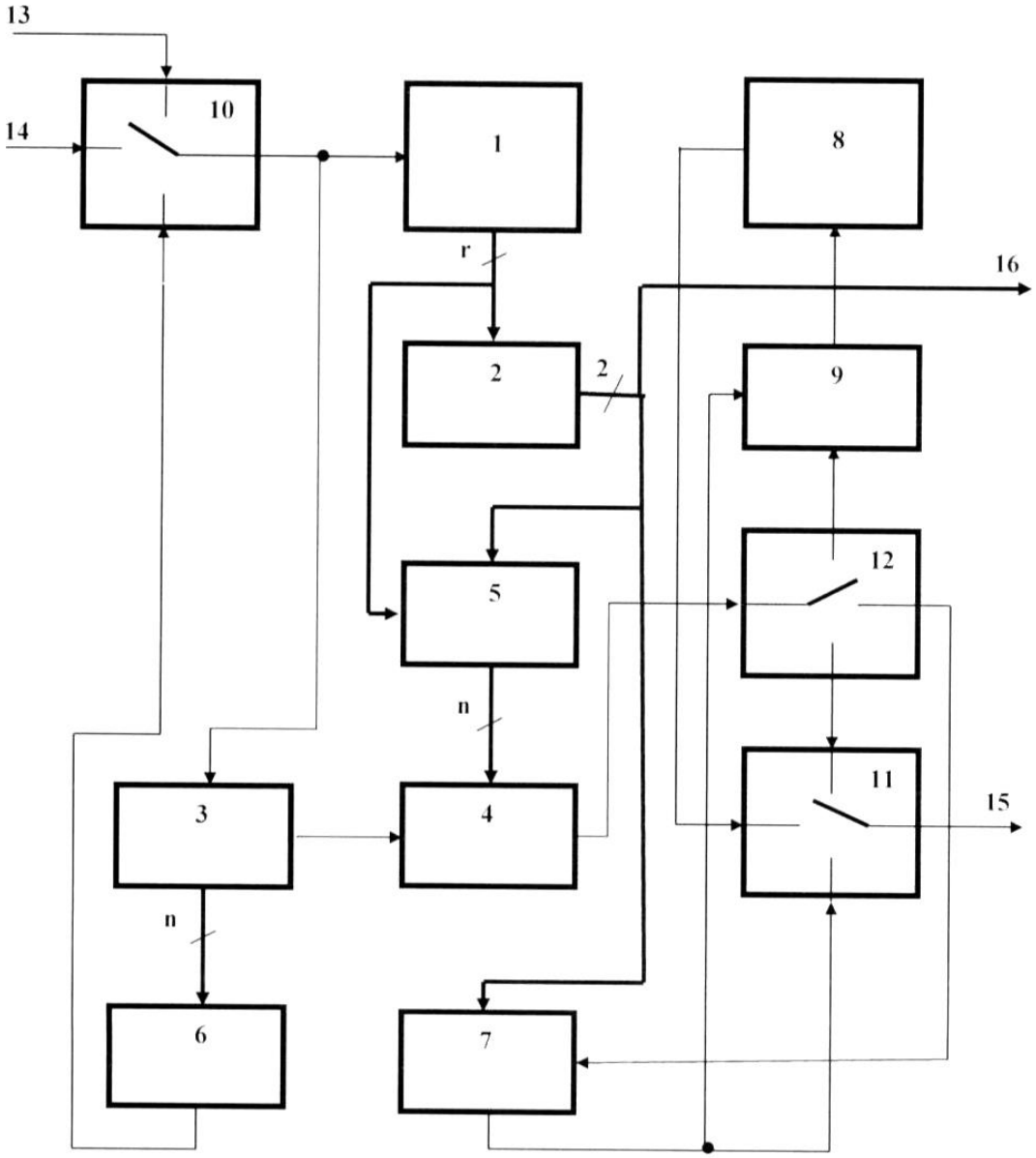
Кратність помилок, які виправляються	Кількість перестановок w і максимальна кількість тактів декодування			
	w=0 26	w=1 52	w=2 78	w=3 156
$\tau = 1$	100 %	100 %	100 %	100 %
$\tau = 2$	90 %	100 %	100 %	100 %
$\tau = 3$	58 %	88 %	99 %	100 %

Запропонований пристрій може використовуватись для декодування як систематичних кодових слів, так і несистематичних кодових слів. В першому випадку відсутня потреба в "оберненій" ЛПС 8.

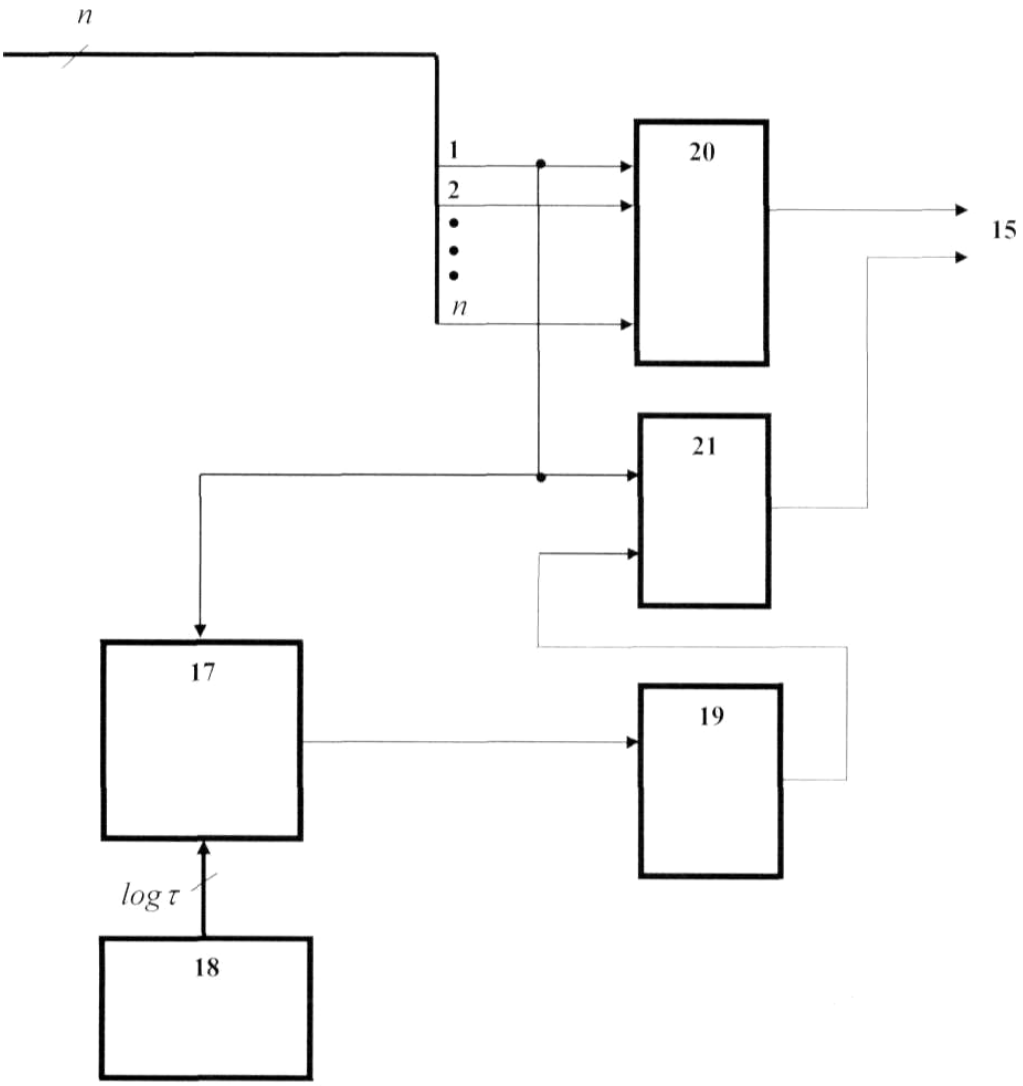
ФОРМУЛА ВИНАХОДУ

Переставний декодер двійкових циклічних (n, k)-кодів, який складається з лінійної послідовної схеми синдромного r-розрядного регістра зсуву зі зворотними зв'язками, логічного блока перевірки синдромів, буферного регістра і коректора помилок, послідовний вхід якого з'єднано з першим послідовним виходом буферного регістра, n-розрядний вихід лінійної послідовної схеми з'єднано з r-розрядним входом логічного блока перевірки синдромів, який **відрізняється** тим, що додатково введені блок формування слова помилки, блок прямої перестановки, блок оберненої перестановки, "обернену" лінійну послідовну схему, схему АБО і три перемикачі, при цьому інформаційний вхід пристрою зв'язаний з першим входом першого перемикача, вхід допоміжних даних пристрою зв'язаний з другим входом першого перемикача, інформаційний вихід пристрою зв'язаний з виходом другого перемикача, дворозрядний керуючий вихід пристрою зв'язаний з дворозрядним керуючим виходом логічного блока перевірки синдромів, з дворозрядним керуючим входом блока формування слова помилки та з дворозрядним керуючим входом блока оберненої перестановки, послідовний вихід якого зв'язаний з першим входом другого перемикача та з першим входом схеми АБО, вихід якої зв'язаний з послідовним входом "оберненої" лінійної послідовної схеми, послідовний вихід якої зв'язаний з другим входом другого перемикача, третій вхід якого зв'язаний з першим виходом третього перемикача, вхід якого зв'язаний з виходом коректора помилок, n-розрядний вхід якого зв'язаний з n-розрядним виходом блока формування слова помилки, r-розрядний вхід якого зв'язаний також з r-розрядним виходом лінійної послідовної схеми, вихід першого перемикача зв'язаний з послідовним входом лінійної послідовної схеми та з послідовним входом буферного регістра, n-розрядний вихід якого зв'язаний з n-розрядним входом блока прямої перестановки, вихід якого зв'язаний з третім входом першого перемикача, другий і третій виходи третього перемикача зв'язані відповідно з другим входом схеми АБО та з інформаційним входом блока оберненої перестановки (r=n-k), а логічний блок перевірки синдромів містить лічильник, вузол пам'яті, RS-тригер, елемент АБО, елемент І, перший вхід якого з'єднаний з інверсним виходом RS-тригера, S-вхід якого з'єднаний з виходом переносу лічильника, паралельний ($\log\tau$)-розрядний вхід якого з'єднаний з інформаційним виходом вузла пам'яті, перший розряд r-розрядного входу блока зв'язаний з входом віднімання лічильника, з другим входом елемента І та з першим входом елемента АБО, решта входів якого з'єднані з рештою розрядів r-розрядного входу блока, виходи елемента АБО і елемента І утворюють дворозрядний керуючий вихід пристрою, блок формування слова помилки містить лічильник, n-розрядний регістр зсуву, RS-тригер, перший елемент І, другий елемент І і третій елемент І, входи якого з'єднані з дворозрядним керуючим виходом пристрою, а вихід з'єднано з S-входом RS-тригера, прямий і інверсний виходи якого з'єднані відповідно з першими входами першого елемента І і другого елемента І, на другі входи яких кожного такту надходять синхросигнали з синхровходу, вихід першого елемента І з'єднаний з входом віднімання лічильника та з входом зсуву регістра, вихід другого елемента І з'єднаний з входом додавання лічильника, прямий вихід RS-тригера з'єднаний також з входом паралельного запису регістра, вихід якого є n-розрядним виходом блока, а r-розрядний вхід якого з'єднаний зі старшими r розрядами регістра в оберненому

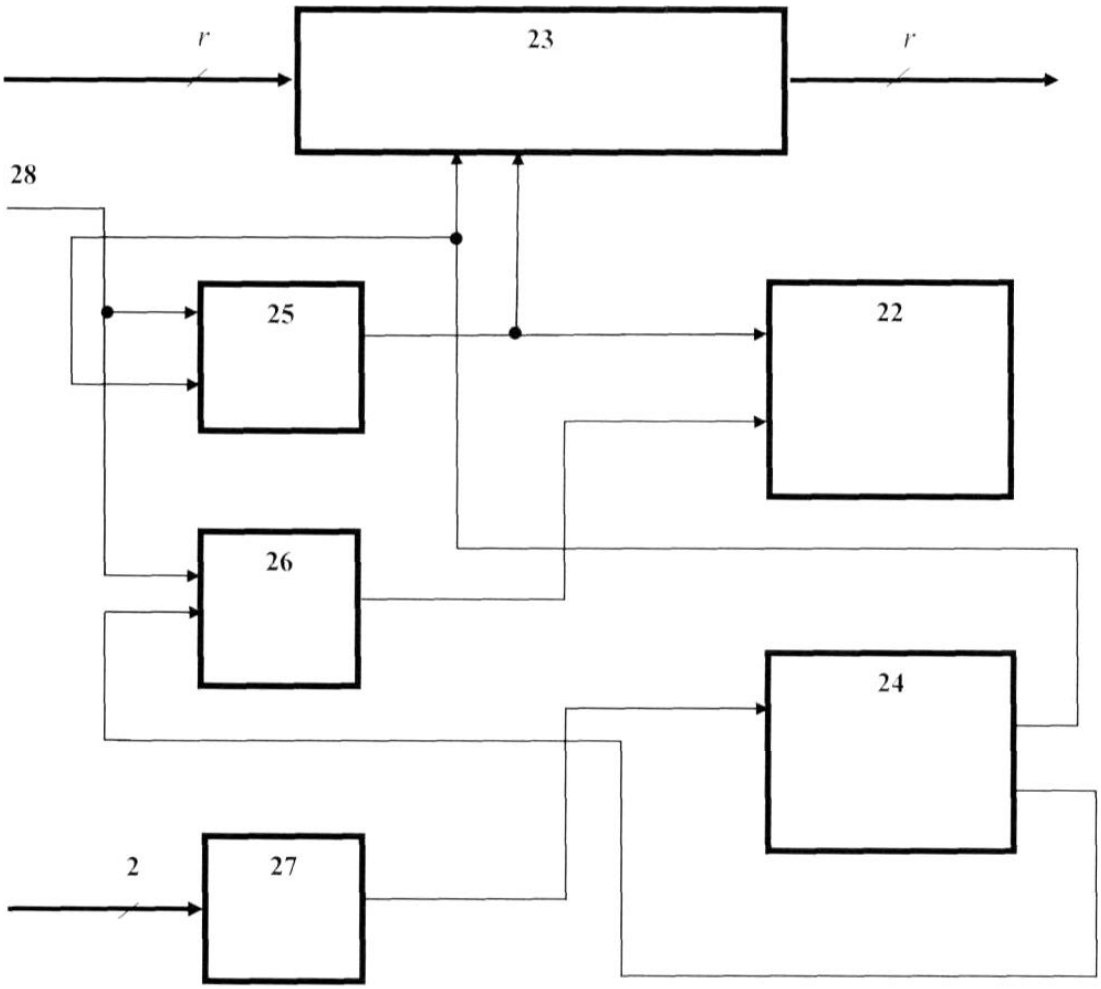
порядку, блок прямої перестановки містить n-розрядний регістр зсуву, причому j-й розряд регістра зв'язаний з i-м входом блока за правилом: j=(2i-l)mod n, n-непарне, а блок оберненої перестановки містить перший лічильник, другий лічильник, n-розрядний кільцевий регістр зсуву, перший елемент І, другий елемент І, елемент АБО та інвертор, вихід якого з'єднаний з першим входом першого елемента І, вихід якого з'єднаний з входом додавання першого лічильника, m-розрядний вихід якого з'єднаний з m-розрядним входом другого лічильника, вихід переносу якого з'єднаний з першим входом елемента АБО, другий вхід та вихід якого з'єднані відповідно з виходом другого елемента І та з входом дозволу паралельного запису в другий лічильник, інформаційний вихід якого з'єднаний з входом зсуву регістра, перший розряд якого з'єднаний з інформаційним входом блока, послідовний вихід якого з'єднаний з n-м розрядом регістра, перший розряд дворозрядного керуючого входу блока з'єднаний з другим входом першого елемента І та з першим входом другого елемента І, а другий розряд дворозрядного керуючого входу блока з'єднаний з входом інвертора та з другим входом другого елемента І.



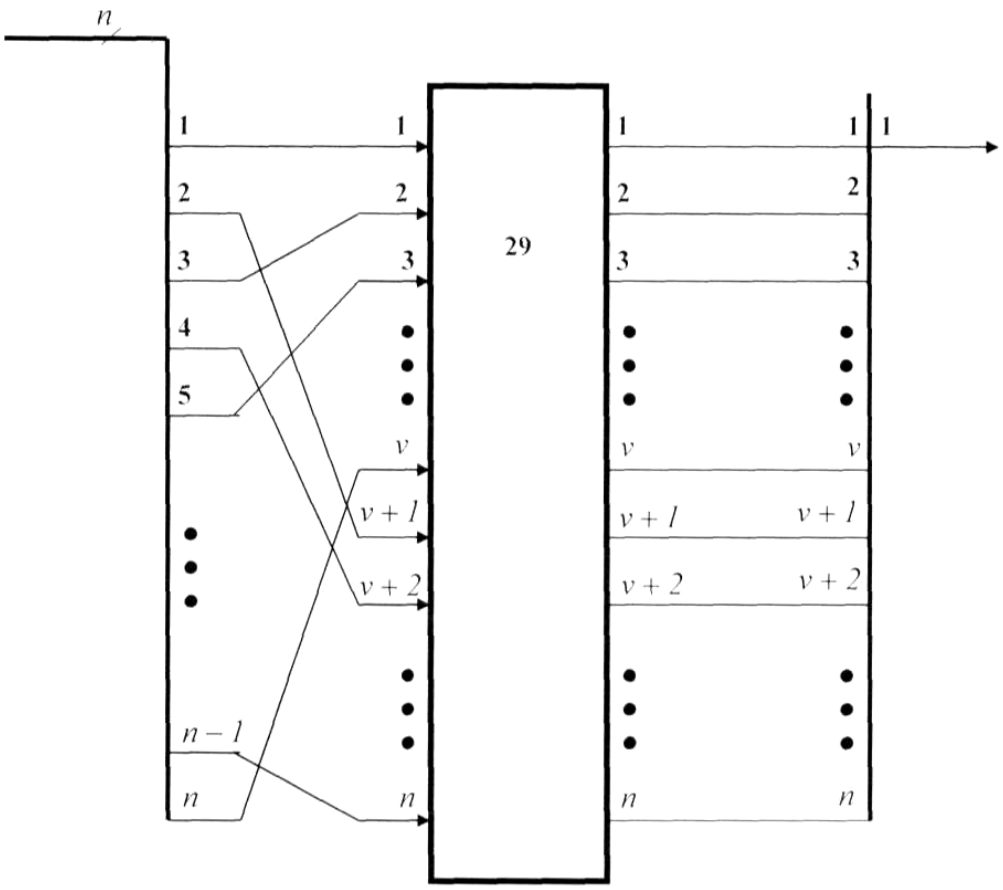
Фіг. 1



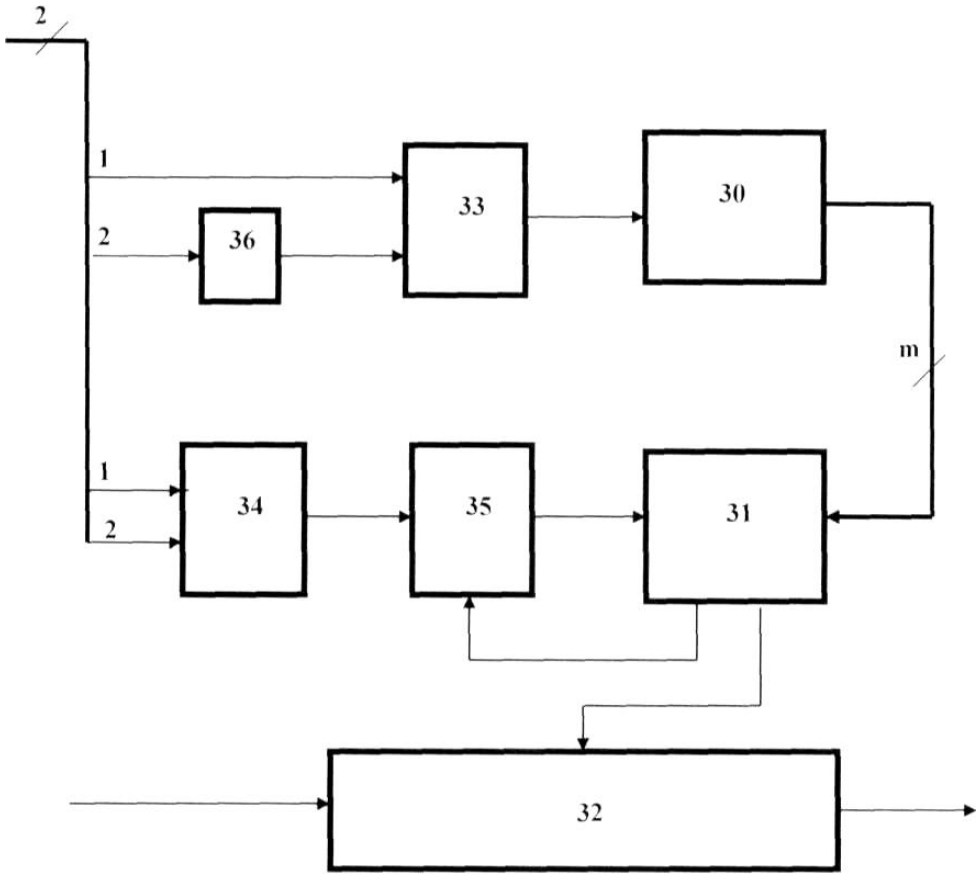
Фіг. 2



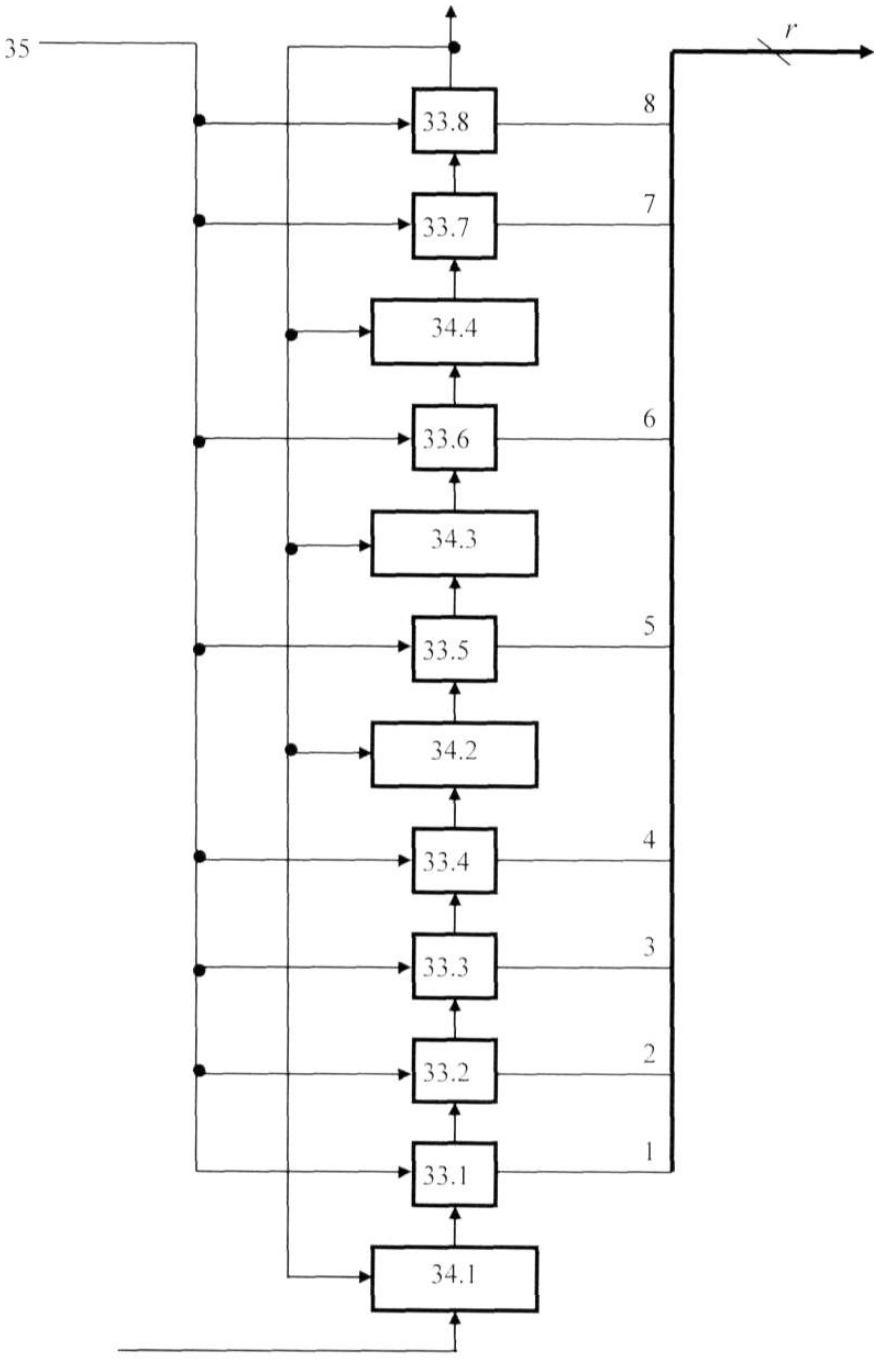
Фіг. 3



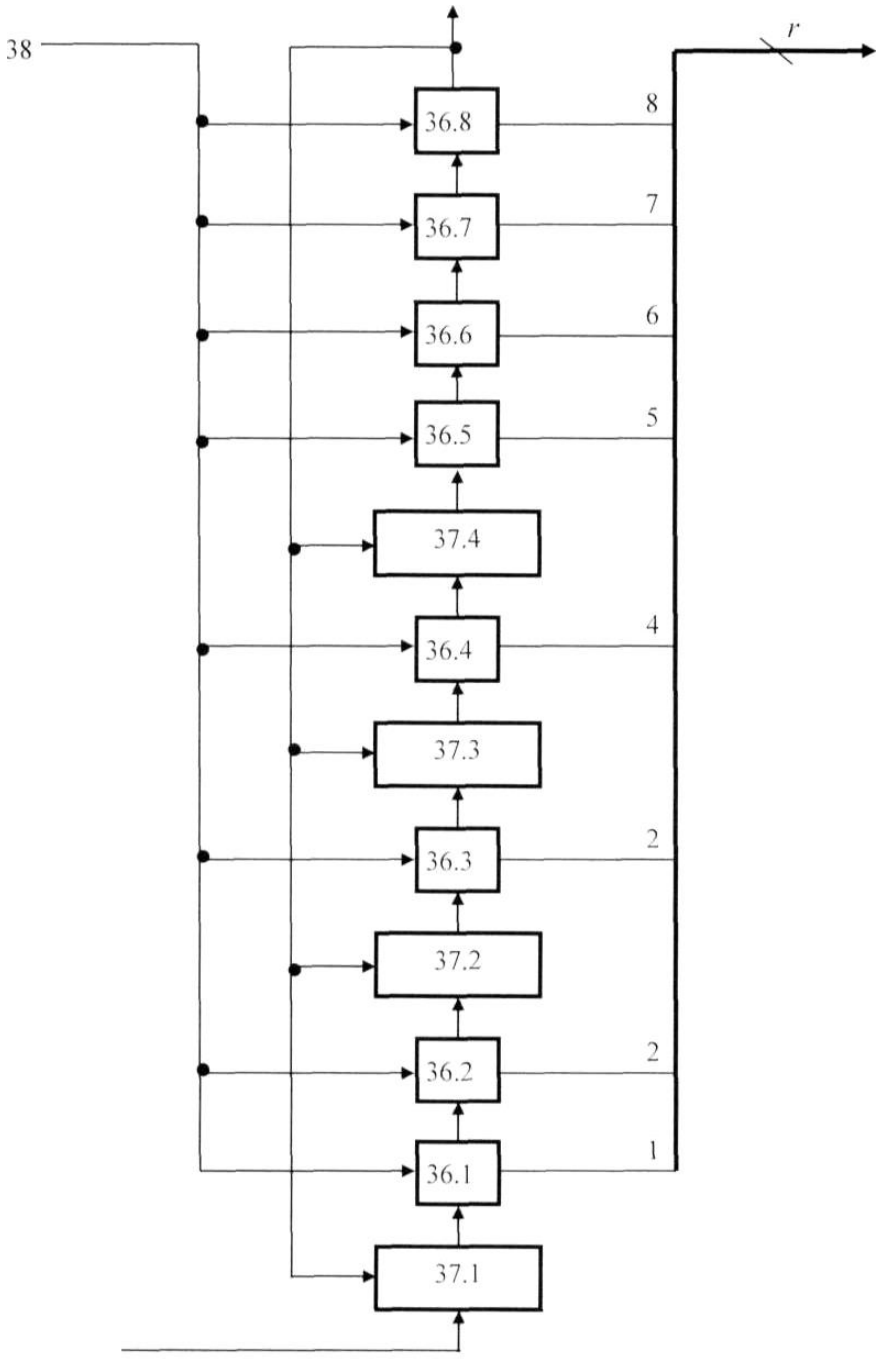
Фіг. 4



Фіг. 5



Фіг. 6



Фіг. 7

Комп'ютерна верстка А. Крулевський

Міністерство розвитку економіки, торгівлі та сільського господарства України,
вул. М. Грушевського, 12/2, м. Київ, 01008, Україна

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