



ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

УКРАЇНА

(19) **UA** (11) **88393** (13) **U**
(51) МПК (2014.01)
H04L 9/00

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: u 2013 12760	(72) Винахідник(и): Білан Степан Миколайович (UA), Білан Миколай Миколайович (UA), Пасічник Леонід Павлович (UA), Герцій Олександр Анатолійович (UA), Онофрійчук Ірина Юріївна (UA), Малюк Вікторія Петрівна (UA)
(22) Дата подання заявки: 01.11.2013	
(24) Дата, з якої є чинними права на корисну модель: 11.03.2014	
(46) Публікація відомостей про видачу патенту: 11.03.2014, Бюл.№ 5	(73) Власник(и): ДЕРЖАВНИЙ ЕКОНОМІКО- ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ ТРАНСПОРТУ, вул. Лукашевича, 19, м. Київ-49, 03049 (UA)

(54) ПРИСТРІЙ ДЛЯ ПЕРЕДАЧІ ДАНИХ

(57) Реферат:

Пристрій для передачі даних містить підключені до протилежних сторін лінії зв'язку блок передачі даних та блок прийому даних, блок передачі даних містить скремблер, який містить генератор імпульсів, блок прийому даних містить дескремблер, який містить генератор імпульсів. Пристрій містить у скремблері та дескремблері відповідно перший та другий клітинні автомати, перший та другий лічильники, перший та другий об'єднувачі виходів клітин відповідно першого та другого клітинних автоматів.

U
88393
UA

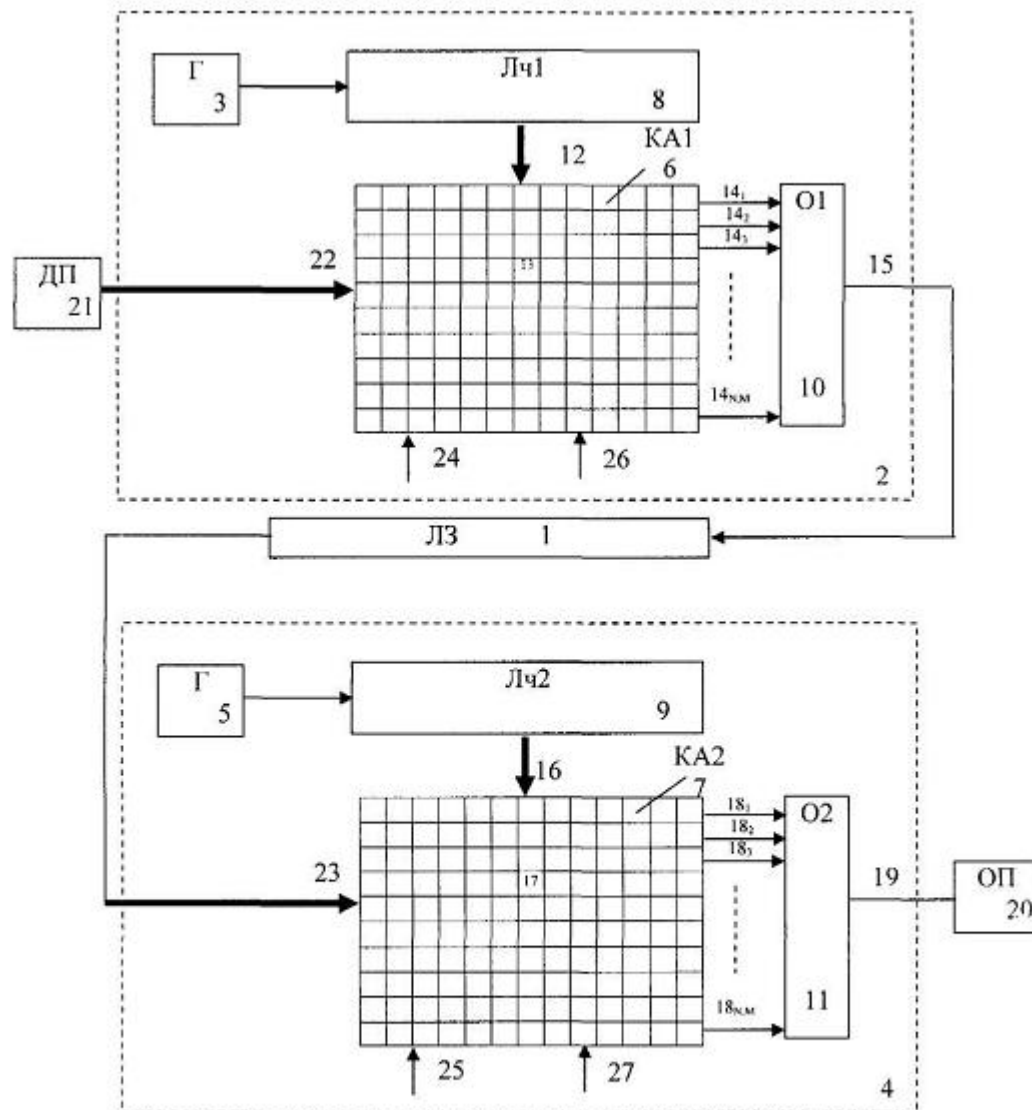


Fig. 1

Корисна модель належить до техніки зв'язку, а саме до схем кодування, декодування та перетворення даних при їх передачі між віддаленими один від одного абонентами.

Відомо пристрій для кодування-декодування даних (Патент Росії № 2260251), який містить лінію зв'язку, з обох сторін якої підключені блоки прийому та передачі даних, генератор псевдовипадкової послідовності бітів, елементи І та Виключне АБО, перший підсилювач, генератор з фазовою автопідстройкою частоти, регістри зсуву, другий підсилювач, дешифратори та тригери.

Недоліком є низька швидкодія та складність побудови генератора псевдовипадкових послідовностей.

Відомо пристрій (Патент США № 5530959) для передачі даних, що містить підключені до протилежних сторін лінії зв'язку блок передачі даних та блок прийому даних, блок передачі даних містить скремблер, який містить генератор псевдовипадкової послідовності бітів, перший елемент Виключне АБО та перший підсилювач, генератор псевдовипадкової послідовності бітів складається з першого регістра зсуву, другого елемента Виключне АБО, входи якого підключені до виходів першого регістра зсуву, а вихід - до першого входу першого елемента Виключне АБО та до входу послідовних даних першого регістра зсуву, вхід синхронізації якого є входом даних скремблера, вихід першого підсилювача підключений до лінії зв'язку, блок прийому даних містить дескремблер, що містить генератор з фазовою автопідстройкою частоти, другий регістр зсуву, третій і четвертий елементи Виключне АБО та другий підсилювач, вхід якого підключений до лінії зв'язку, а вихід - до входу генератора з фазовою автопідстройкою частоти, вихід якого є вихід синхронізації дескремблера, виходи другого регістра зсуву з'єднані зі входами третього елемента Виключне АБО, вихід якого підключений до першого входу четвертого елемента Виключне АБО.

Недоліками даного пристрою є низька швидкодія та низький рівень захисту, який обмежується розрядністю регістра зсуву у генераторі псевдовипадкової послідовності бітів.

Найбільш близьким до пристрою, що заявляється, є пристрій для передачі даних (Патент Росії № 2272360), що містить підключені до протилежних сторін лінії зв'язку блок передачі даних і блок прийому даних, блок передачі даних містить скремблер, що містить генератор псевдовипадкової послідовності бітів, перший елемент виключне АБО і перший підсилювач, генератор псевдовипадкової послідовності бітів містить перший регістр зсуву і другий елемент Виключне АБО, входи якого підключені до виходів першого регістра зсуву, а вихід - до першого входу першого елемента Виключне АБО і до входу послідовних даних першого регістра зсуву, вхід синхронізації якого є входом синхронізації скремблера, другий вхід першого елемента Виключне АБО є входом даних скремблера, вихід першого підсилювача підключений до лінії зв'язку, блок прийому даних містить дескремблер, що містить генератор з фазовим автопідстроюванням частоти, другий регістр зсуву, третій і четвертий елементи Виключне АБО і другий підсилювач, вхід якого підключений до лінії зв'язку, а вихід - до входу генератора з фазовим автопідстроюванням частоти, вихід якого є виходом синхронізації дескремблера, виходи другого регістра зсуву сполучені з входами третього елемента Виключне АБО, вихід якого підключений до першого входу четвертого елемента Виключне АБО, блок передачі даних додатково містить блок перетворення паралельного коду в послідовний, група входів даних якого є групою входів даних пристрою, а вихід байтової синхронізації - першим виходом байтової синхронізації пристрою, скремблер додатково містить третій регістр зсуву, перший дешифратор, перший тригер і перший інвертор, вихід якого підключений до входу синхронізації першого тригера, вхід першого інвертора сполучений з входами синхронізації першого і третього регістрів зсуву, а також з виходом бітової синхронізації блока перетворення паралельного коду в послідовний, управляючий вхід першого регістра зсуву сполучений з виходом першого дешифратора і з входом корекції блока перетворення паралельного коду в послідовний, вихід даних якого сполучений з входом даних скремблера, вхід послідовних даних третього регістра зсуву сполучений з виходом першого елемента Виключне АБО і з входом даних першого тригера, вихід якого сполучений з входом першого підсилювача, входи паралельних даних першого регістра зсуву сполучені з виходами першого дешифратора, входи якого сполучені з виходами третього регістра зсуву, блок прийому даних додатково містить блок перетворення послідовного коду в паралельний, група виходів даних якого є групою виходів даних пристрою, а вихід байтової синхронізації - другим виходом байтової синхронізації пристрою, дескремблер додатково містить четвертий регістр зсуву, другий дешифратор, другий і третій тригери і другий інвертор, вихід якого підключений до входу синхронізації другого тригера і до входів синхронізації другого і четвертого регістрів зсуву, управляючий вхід другого регістра зсуву сполучений з виходом другого дешифратора і з входом корекції блока перетворення послідовного коду в паралельний, вхід даних якого сполучений з виходом

третього тригера, а вхід бітової синхронізації - з виходом синхронізації дескремблера, вхід послідовних даних четвертого регістра зсуву сполучений з другим входом четвертого елемента Виключне АБО і з виходом другого тригера, вхід даних якого сполучений з виходом другого підсилювача, входи паралельних даних другого регістра зсуву сполучені з виходами другого дешифратора, входи якого сполучені з виходами четвертого регістра зсуву, вхід послідовних даних другого регістра зсуву сполучений з першим входом четвертого елемента Виключне АБО, вихід якого сполучений з входом даних третього тригера, вхід синхронізації якого сполучений з виходом синхронізації дескремблера і з входом другого інвертора. Блок перетворення паралельного коду в послідовний містить тригер, постійний запам'ятовуючий пристрій, паралельний регістр, регістр зсуву, генератор імпульсів і інвертування, група входів даних блока сполучена з входами паралельних даних регістра зсуву, вихід послідовних даних якого є виходом даних блока, а вхід синхронізації сполучений з виходом генератора імпульсів і з входом Інвертування і є виходом бітової синхронізації блока, вхід корекції блока сполучений з входом даних тригера, вхід синхронізації якого сполучений з виходом інвертування і з входом синхронізації паралельного регістра, виходи якого сполучені з входом управління регістра зсуву, з виходом байтової синхронізації блока і з входами адреси постійного пристрою, що запам'ятовує, виходи якого сполучені з входами даних паралельного регістра, вихід тригера сполучений з входом адреси постійного запам'ятовуючого пристрою. Блок перетворення послідовного коду в паралельний містить перший і другий регістри зсуву, інвертор, постійний запам'ятовуючий пристрій, перший і другий паралельні регістри, вхід даних другого паралельного регістра сполучений з входом даних першого регістра зсуву і є входом даних блока, вхід синхронізації першого регістра зсуву сполучений з входом інвертора і є входом бітової синхронізації блока, вхід даних другого регістра зсуву є входом корекції блока, група виходів другого паралельного регістра є групою виходів даних блока, вхід синхронізації другого паралельного регістра сполучений з виходом першого паралельного регістра і є виходом байтової синхронізації блока, вихід інвертора сполучений з входами синхронізації другого регістра зсуву і першого паралельного регістра, виходи постійного запам'ятовуючого пристрою, сполучені з входами першого паралельного регістра, а адресні входи - з виходом другого регістра зсуву і з виходами першого паралельного регістра.

Недоліком даного пристрою є низька швидкодія та низька надійність функціонування за рахунок використання генераторів псевдовипадкових послідовностей бітів на регістрах зсуву та застосування перетворювачів паралельних кодів у послідовні.

В основу корисної моделі поставлена задача підвищення швидкодії, надійності функціонування та криптостійкості. Висока швидкодія, надійність та криптостійкість досягається за рахунок використання клітинного автомату із заданою організацією функціонування.

Поставлена задача вирішується тим, що пристрій для передачі даних, що містить підключені до протилежних сторін лінії зв'язку блок передачі даних та блок прийому даних, блок передачі даних містить скремблер, який містить генератор імпульсів, блок прийому даних містить дескремблер, який містить генератор імпульсів, також пристрій містить у скремблері та дескремблері відповідно перший та другий клітинні автомати, перший та другий лічильники, перший та другий об'єднувачі виходів клітин відповідно першого та другого клітинних автоматів, причому вихід першого генератора імпульсів скремблера підключений до лічильного входу першого лічильника імпульсів, виходи якого підключені до відповідних входів клітин першого клітинного автомату, виходи кожної клітини якого підключені до відповідних входів першого об'єднувача виходів клітин, вихід якого підключений до першого кінця лінії зв'язку, а другий генератор імпульсів дескремблера підключений до лічильного входу другого лічильника імпульсів, виходи якого підключені до відповідних входів клітин другого клітинного автомату, виходи кожної клітини якого підключені до відповідних входів другого об'єднувача виходів, вихід якого підключений до входу одержувача повідомлень, вихід джерела повідомлень підключений до входів установки клітин першого клітинного автомата, а другий вивід ліній зв'язку підключений до входів установки клітин другого клітинного автомату, крім того кожна клітина першого та другого клітинних автоматів підключені до входу початкової установки та входу обнуління.

На фіг. 1 подано структурну схему пристрою для передачі даних, на фіг. 2 представлена функціональна схема клітини першого клітинного автомату, на фіг. 3 - функціональна схема клітини другого клітинного автомату, а на фіг. 4 - приклад функціонування першого та другого клітинних автоматів.

Пристрій для передачі даних (фіг. 1) містить, підключені до протилежних сторін лінії 1 зв'язку (ЛЗ), блок передачі даних та блок прийому даних, блок передачі даних містить скремблер 2, який містить перший генератор 3 імпульсів (Г), блок прийому даних містить дескремблер 4, який

містить другий генератор 5 імпульсів, скремблер 2 та дескремблер 4 містять, відповідно, перший та другий клітинні автомати (КА1 КА2) 6,7, перший та другий лічильники (Лч1, Лч2) 8,9, перший та другий об'єднувачі (О1, О2) 10,11 виходів клітин відповідно першого та другого клітинних автоматів КА1 6, КА2 7, причому вихід першого генератора 3 імпульсів скремблера 2 підключений до лічильного входу першого ЛЧ1 8 імпульсів, виходи якого підключені до відповідних входів 12 клітин 13 КА1 6, виходи 14 кожної клітини якого підключені до відповідних входів 01 10, вихід 15 якого підключений до першого кінця ЛЗ 1, а другий генератор 5 імпульсів дескремблера 4 підключений до лічильного входу другого лічильника Лч2 9 імпульсів, виходи якого підключені до відповідних входів 02 11, вихід 19 якого підключений до входу одержувача 20 повідомлень (ОП), вихід джерела 21 повідомлень (ДП) підключений до входів 22 установки клітин КА1 6, а другий вивід ЛЗ 1 підключений до входів 23 установки клітин 17 КА2 7, крім того кожна клітина 13, 17 КА1 6 та КА2 7 підключені до входів 24, 25 початкової установки та до входів 26, 27 обнуління.

Клітина 13 КА1 6 (фіг. 2) містить тригер 28 (Т), комбінаційну схему 29 (КС) та диз'юнктор 30, вихід якого підключений до входу 31 установки тригера Т 28, вхід 32 обнуління підключений до входу 26 обнуління КА1 6, другий вхід диз'юнктора 30 підключений до входу 24 установки КА1 6, перший вхід диз'юнктора 30 підключений до виходу КС 29, перші вісім входів 33₁.....33₈ підключені до виходів 14 сусідніх клітин 13, розташованих по вертикалі, горизонталі та діагоналях, дев'ятий вхід КС 29 підключений до входу 22 КА1 6, вихід Т 28 підключений до виходу 14, десятій вхід КС 29 підключений до входу 12 клітини 13.

Клітина 17 КА2 7 (фіг. 3) містить тригер 34 (Т), диз'юнктор 35 та комбінаційну схему 36 (КС), вихід якої підключений до виходу 18, перші вісім входів 37₁.....37₈ до виходів 38 сусідніх клітин 17, розташованих по вертикалі, горизонталі та діагоналях, дев'ятий вхід КС 36 підключений до виходу 38 власної клітини та до прямого виходу Т 34, вхід 39 установки підключений до виходу диз'юнктора 35, перший вхід якого підключений до входу 23 клітини, а другий вхід диз'юнктора 35 підключений до входу 25 установки клітини 17, вхід 27 обнуління якої підключений до входу 40 обнуління Т 34, десятій вхід КС 36 підключений до входу 16 клітини 17.

Пристрій функціонує в такий спосіб.

У початковий момент часу на входи 26 та 27 обнуління КА1 6 та КА2 7 подаються одиничні сигнали, які обнулюють усі клітини 13, 17 обох клітинних автоматів 6, 7. ДП 21 починає формувати послідовність бітів, які подаються у вигляді сигналів логічних "1" та "0".

Вихідна послідовність подається на входи 22 усіх клітин 13 КА1 6. Одночасно з початком вихідної інформаційної послідовності Г 3 генерує імпульси, що лічаються Лч1 8.

Перед початком передавання інформаційної послідовності обидва КА1 6 та КА2 7 встановлюються у заданий користувачем стан. Початкове встановлення КА1 6 та КА2 7 здійснюється по входах 24, 25 початкової установки, відповідно. Таким чином, на початку передавання клітини 13, 17 обох КА1, 2 6 та 7 встановлюються у стани логічних "0" та "1". На фіг. 4 приклад такого стану поданий на нульовому такті.

З приходом першого біта на вхід 22 Лч1 8 має на виході код одиниці, який подається на входи 12 клітин 13. Такий код указує на номер клітини 13 КА1 6. Отже біт вхідної послідовності подається на вхід 22 тієї клітини 13, на яку указує код Лч1 8 на входах 12. На виході 14 відповідної клітини 13 формується сигнал, який є результатом додавання за модулем 2 значень на виходах сусідніх клітин околиці власної клітини та значення на вході 22.

Отриманий сигнал з відповідного виходу 14 подається на відповідний вхід О1 10. Перший об'єднувач 10 також як і другий об'єднувач 11 функціонують як багатовходові диз'юнктори. На виході 15 О1 10 формується сигнал, що сформований на відповідному виході 14 клітини 14. Отриманий бітовий сигнал подається у ЛЗ 1 від скремблера 2.

Аналогічним чином формуються усі біти шифрограми, що сформовані на виході скремблера 2.

Імпульси з другого виводу ЛЗ 1 подаються у дескремблер 4 на входи 23 усіх клітин 17 КА2 7. Другий генератор Г 5 імпульсів формує імпульси, в такт бітам шифрограми, які подаються на лічильний вхід Лч2 9. Код з виходів Лч2 9 подається на входи 16 клітин 17 КА2 7, який указує на відповідну клітину 17.

Клітина 17, на яку указав код Лч2 9, встановлюється у стан, на який указує відповідний біт. Якщо на вході 23 присутня логічна "1", то клітина встановлюється у стан логічної "1", а якщо інформаційний біт має значення логічного "0", то клітина встановлюється у стан логічної "1", а якщо інформаційний біт має значення логічного "0", то клітина встановлюється у логічний "0". На відповідному виході 18 даної клітини 17 формується сигнал, величина якого дорівнюється сумі за модулем 2 сигналів, що відповідають станам клітин околиці для обраної клітини та значення інформаційного біта у даний момент часу. Отриманий сигнал через 02 11 формується

на його виході 19, від якого він у вигляді відповідного інформаційного біта початкової послідовності подається до ОП 20.

На фіг. 4 подано приклад формування станів КА1 6 та КА2 7. На фіг. 4 на кожному такті зліва показано біт інформаційної початкової послідовності, зліва направо подано стани КА1 6, біт шифрограми, отриманий на даному такті, стани КА2 7 та біт на виході дескремблера 4. Індеси навколо бітів указують номер часового такту. Пунктиром окреслено клітини околиці заданої клітини на даному часовому такті.

Для визначення стану заданої клітини під КА1 6 подана формула, яка враховує стани клітин околиці, стан заданої клітини та стан інформаційного біту. Значення стану клітини 13 КА1 6 та значення біту шифрограми визначається додаванням за модулем 2 станів клітин околиці, стану заданої клітини та стану інформаційного біту.

Стан заданої клітини 17 КА2 7 встановлюється значенням біту шифрограми на заданому часовому такті, а значення біту на виході дескремблера 4 шляхом додавання за модулем 2 значень станів усіх клітин окресленої околиці.

Таким чином, початковий стан КА1 6 та КА2 7, а також послідовність перебору клітин 13 та 17 визначають основні параметри ключових параметрів для проведення подальшого потокового шифрування. Дані параметри не відомі супротивнику. Вони визначають стійкість шифру.

Клітина 13 КА1 6 функціонує в такий спосіб (фіг. 2).

Перші вісім входів $33_1, \dots, 33_8$ КС 29 підключені до виходів 14 відповідних клітин 13 околиці, верхньої, нижньої, лівої, правої та клітин по обох діагоналях. Від цих клітин 13 на входи 33 подаються значення відповідних станів. Якщо на вході 12 присутній сигнал логічної "1", то КС 29 додає за модулем 2 значення сигналів на входах 33 та 22. Результат роботи КС 29 подається на перший вхід диз'юнктора 30, сигнал з виходу якого подається на вхід 31 установки Т 28. Т 28 встановлюється на виході 14 у стан, що відповідає сигналу на вході 31 установки.

Початкова установка Т 28 здійснюється по входу 24, сигнал від якого подається на другий вхід диз'юнктора 30. Обнуління Т 28 здійснюється сигналом від входу 26 обнуління, який подається на вхід 32 обнуління Т 28.

Клітина 17 КА2 7 функціонує в такий спосіб (фіг. 3).

Сигнали з виходів клітин 17 околиці подаються на відповідні входи 37 КС 36, яка починає функціонувати у момент часу коли на вході 16 присутній одиничний сигнал. Початкова установка Т 34 здійснюється сигналом з входу 25, який подається на вхід 39 установки Т 34. На виході 38 з'являється значення, відповідне сигналу установки.

Т 34 також встановлюється сигналом з входу 23, який подається на перший вхід диз'юнктора 35. Коли на вході 16 з'являється одиничний сигнал КС 36 реалізує функцію додавання за модулем 2 значень сигналів на входах 37 та сигналу з виходу 38 Т 34. Результат з виходу КС 36 подається на вихід 18 клітини 17.

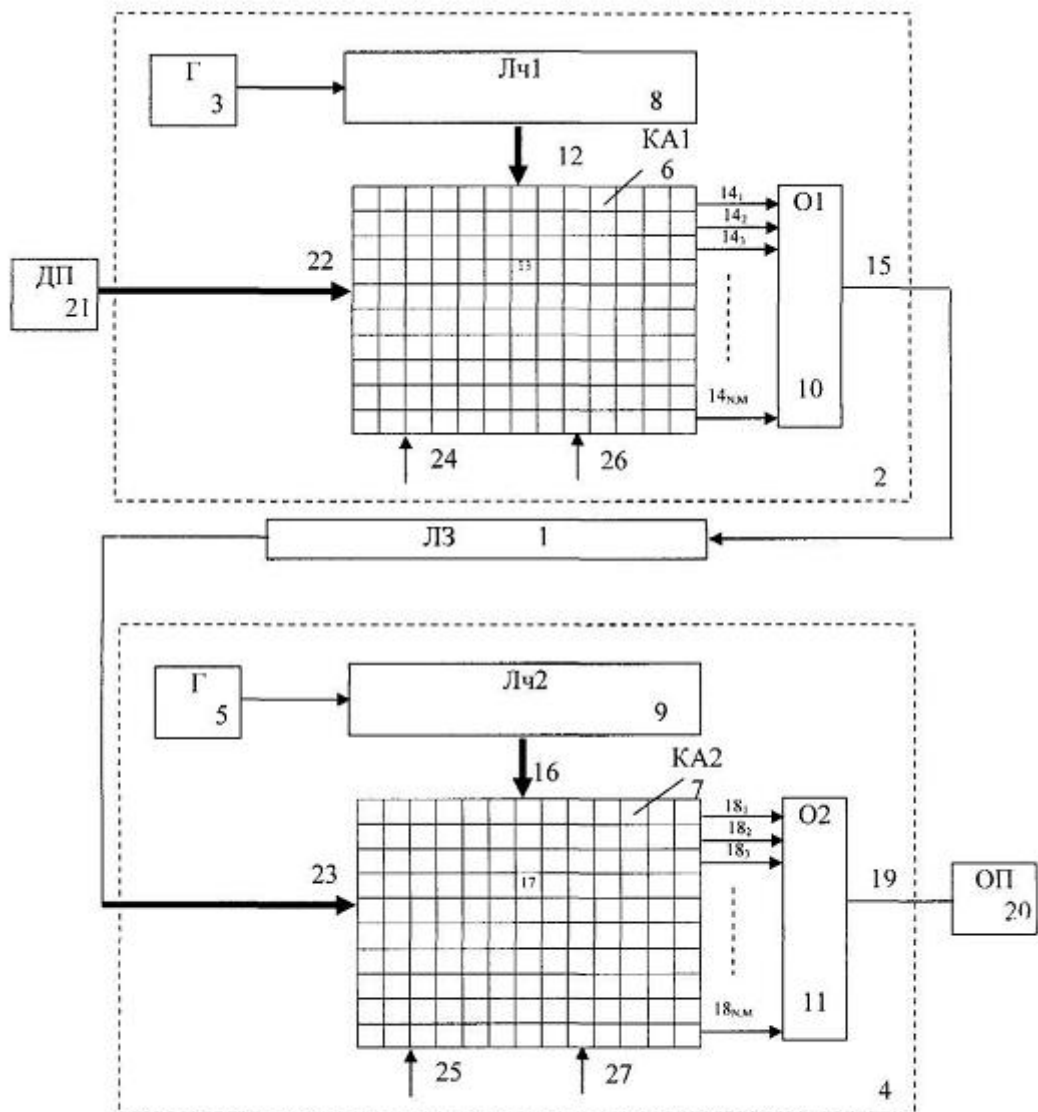
Обнуління Т 34 здійснюється сигналом з входу 27, який подається на вхід 40 обнуління Т 34.

Висока швидкодія досягається тим, що усі клітини клітинних автоматів функціонують паралельно. Використання КА дозволяє підвищити випадковість формування бітів шифрограми. За рахунок початкової установки карти станів клітин клітинних автоматів та початкового завдання послідовності перебору клітин, підвищується стійкість до зламу шифрограми, що формується. Однорідність та простота структури КА дозволяє підвищити надійність функціонування.

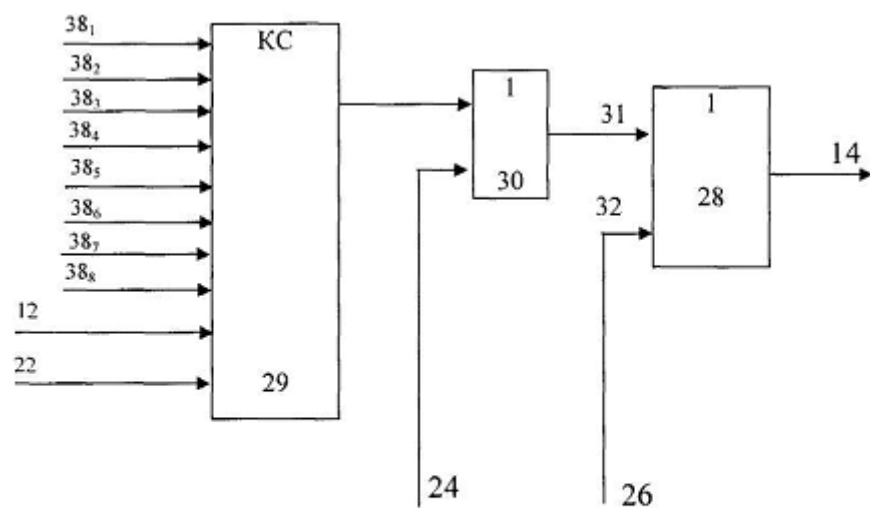
45 ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Пристрій для передачі даних, що містить підключені до протилежних сторін лінії зв'язку блок передачі даних та блок прийому даних, блок передачі даних містить скремблер, який містить генератор імпульсів, блок прийому даних містить дескремблер, який містить генератор імпульсів, який **відрізняється** тим, що пристрій містить у скремблері та дескремблері відповідно перший та другий клітинні автомати, перший та другий лічильники, перший та другий об'єднувачі виходів клітин відповідно першого та другого клітинних автоматів, причому вихід першого генератора імпульсів скремблера підключений до лічильного входу першого лічильника імпульсів, виходи якого підключені до відповідних входів клітин першого клітинного автомату, виходи кожної клітини якого підключені до відповідних входів першого об'єднувача виходів клітин, вихід якого підключений до першого кінця лінії зв'язку, а другий генератор імпульсів дескремблера підключений до лічильного входу другого лічильника імпульсів, виходи якого підключені до відповідних входів клітин другого клітинного автомату, виходи кожної клітини якого підключені до відповідних входів другого об'єднувача виходів, вихід якого підключений до входу одержувача повідомлень, вихід джерела повідомлень підключений до

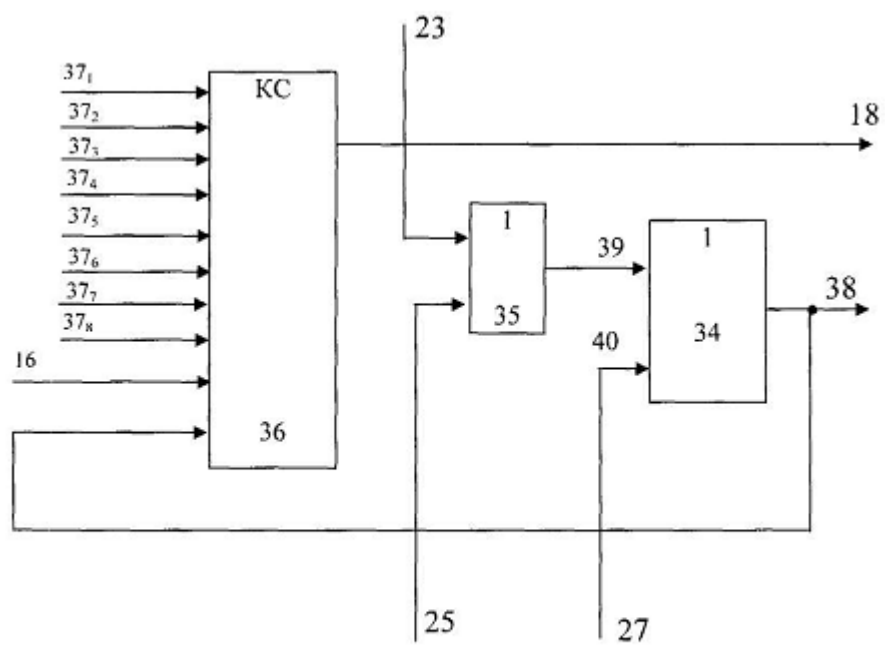
входів установки клітин першого клітинного автомата, а другий вивід ліній зв'язку підключений до входів установки клітин другого клітинного автомата, крім того кожна клітина першого та другого клітинних автоматів підключені до входу початкової установки та входу обнуління.



Фиг. 1



Фиг. 2



Фиг. 3

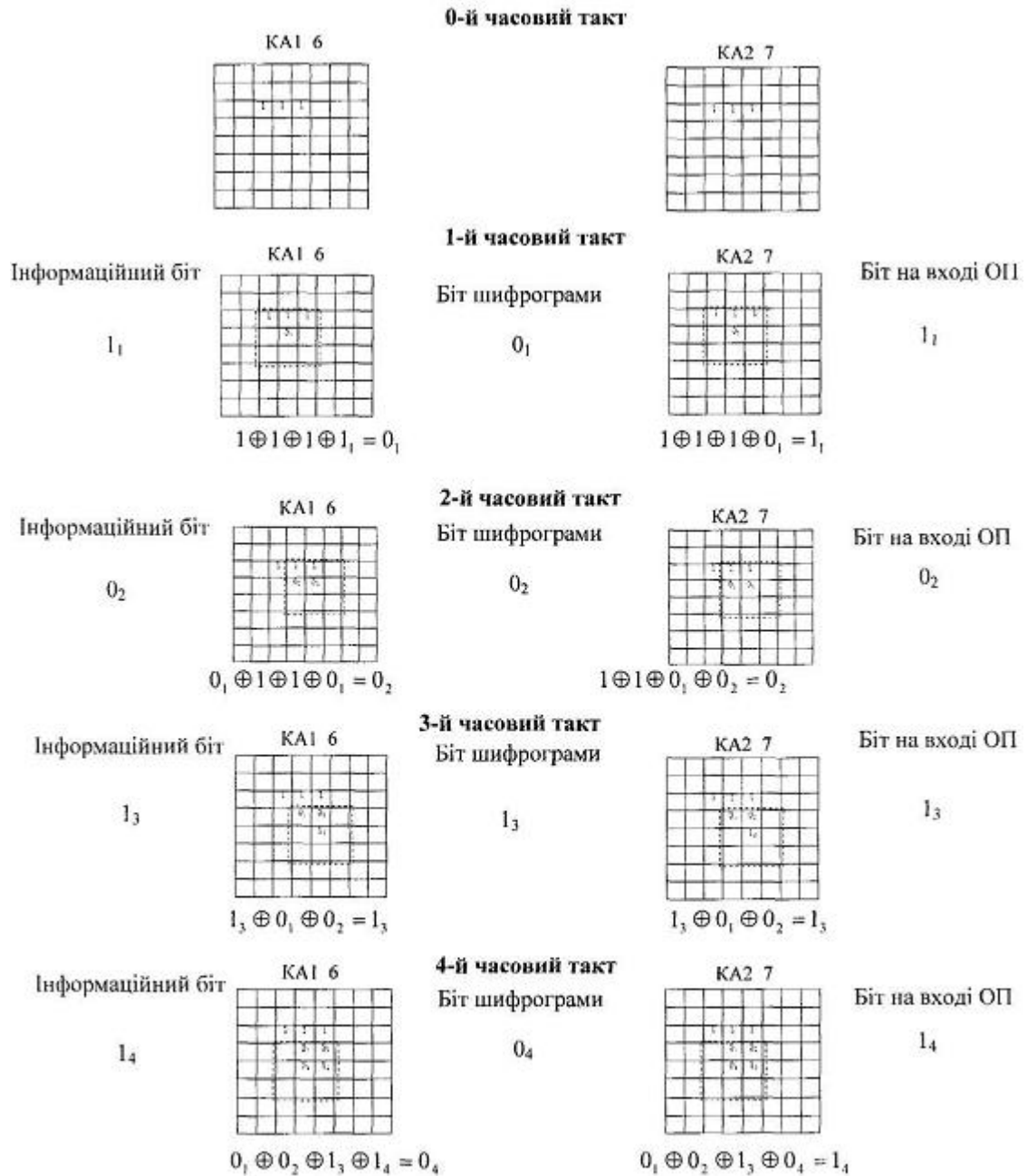


Fig. 4