УКРАЇНА

(19) UA (11) 7875 (13) U

(51) 7 H03M13/00

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

ОПИС
ДО ДЕКЛАРАЦІЙНОГО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під відповідальність власника патенту

(54) ПРИСТРІЙ ДЛЯ КОДУВАННЯ І ПЕРЕДАВАННЯ ДИСКРЕТНОЇ ІНФОРМАЦІЇ ІЗ ЗАХИСТОМ

(21) 20041209954
(22) 06.12.2004
(24) 15.07.2005
(46) 15.07.2005, Бюл. № 7, 2005 р.
(72) Купик Анатолій Ярославович
(73) Вінницький національний технічний університет
(57) Пристрій для кодування і передавання дискретної інформації із захистом, який містить персональний комп'ютер у складі центрального процесора, постійного та оперативного запам'ятовувальних пристроїв і носія інформації, а також канал передавання інформації, який відрізняється тим, що до нього введені паралельний інтерфейс, програмований таймер, прямий та інверсний підсилювачі сигналів, генератор опорної частоти, перетворювачі переднього та заднього фронту сигналу на імпульс, схема збігу, а також тригер; причому до каналу передавання інформації підключені вихід суматора та входи перетворювачів переднього та заднього фронту сигналу на імпульс, вхід прямого підсилювача сигналу з'єднаний з першим виходом паралельного інтерфейсу, а вихід - з першим входом суматора, вхід інверсного підсилювача сигналу з'єднаний з другим виходом паралельного інтерфейсу, а вихід - з другим входом суматора, входи схеми збігу підключені відповідно до виходів перетворювачів переднього та заднього фронту сигналу на імпульс, а вихід - до тактового входу С тригера, інформаційний вхід D якого з'єднаний з інверсним виходом, зі входом дозволу роботи G лічильника СТ0 програмованого таймера та з першим входом INT1 програмованого контролера переривань, вхід скидання на нуль R - з третім виходом паралельного інтерфейсу, а прямий вихід - з другим входом INT2 програмованого контролера переривань та з входом дозволу роботи G лічильника СТ1 програмованого таймера, тактові входи С лічильників СТ0 та СТ1 якого підключені до виходу генератора опорної частоти, за допомогою системного каналу центральний процесор зв'язаний з модулями персонального комп'ютера програмованими контролером переривань і таймером, а також паралельним інтерфейсом.

1

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

Відомий пристрій для приймання дискретних сигналів з кореляційним кодуванням по рівню [Авторське свідоцтво СРСР № 1164892, МКІ H03M 13/00, бюлетень "Изобретения стран мира", 1985, № 18], 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 співпадіння та інвертор.

Недоліком даного пристрою є те, що він не захищає інформацію, що передається, від завад у лінії та від несанкціонованого проникнення.

Відомий також пристрій для реєстрації способу кодування і передавання інформації [Авторське свідоцтво СРСР № 1432788, МКІ H03M 13/12, бюлетень "Открытия. Изобретения", 1988, № 39], який вміщує в собі комутатори, блок згорткового кодування, блок модуляції та канал зв'язку.

2

Недоліком даного пристрою є те, що він також не захищає 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 H03M 13/00, бюлетень "Промислова власність", 1998, №4], 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 двунаправленій шині зв'язаний з інформаційним каналом послідовного порту, виходи запитів пере-

(19) UA (11) 7875 (13) U

ривання 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.

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

$d \geq r+s+1$ (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 корисної моделі 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, програмований контролер переривань та персональний комп'ютер у складі центрального процесора, оперативного та постійного запам'ятовувальних пристроїв та носія інформації додатково введені паралельний інтерфейс, програмований таймер, прямий та інверсний підсилювачі сигналів, генератор опорної частоти, перетворювачі переднього та заднього фронту сигналу на імпульс, схема співпадіння, а також тригер; причому до каналу передавання інформації підключені вихід суматора та входи перетворювачів переднього та заднього фронту сигналу на імпульс, вхід прямого підсилювача сигналу з'єднаний з першим виходом паралельного інтерфейсу, а вихід - з першим входом суматора, вхід інверсного підсилювача сигналу з'єднаний з другим виходом паралельного інтерфейсу, а вихід - з другим входом суматора, входи схеми співпадіння підключені відповідно до виходів перетворювачів переднього та заднього фронту сигналу на імпульс, а вихід - до тактового входу С тригера, інформаційний вхід D якого з'єднаний з інверсним виходом, зі входом дозволу роботи G лічильника СТ0 програмованого таймера та з першим входом INT1 програмованого контролера переривань, вхід скидання на нуль R - з третім виходу паралельного інтерфейсу, а прямий вихід - з другим входом INT2 програмованого контролера переривань та з входом дозволу роботи G лічильника СТ1 програмованого таймера, тактові входи С лічильників СТ0 та СТ1 якого підключені до виходу генератора опорної частоти, за допомогою системного каналу центральний процесор зв'язаний з модулями персонального комп'ютера програмованими контролером переривань і таймером, а також паралельним інтерфейсом,

Введення до складу пристрою паралельного інтерфейсу, програмованого таймера, генератора опорної частоти, суматора, прямого та інверсного підсилювачів сигналів, перетворювачів переднього та заднього фронту на імпульс, схеми співпадіння та тригера з відповідними зв'язками та програмним забезпеченням дозволяє суттєво підвищити ефективність передавання інформації за рахунок збільшення завадоза-хищеності без порушення захисту від несанкціонованого проникнення.

На фіг. 1 наведена схема пристрою для реалізації способу кодування і передавання дискретної інформації із захистом, на фіг. 2 - часові діаграми роботи пристрою, на фіг. 3 - схема роботи пристрою в режимі передавання інформації, а на фіг. 4 - схема роботи пристрою в режимі приймання інформації.

Пристрій для кодування дискретної інформації із захистом вміщує канал передавання інформації 1, прямий 2 та інверсний 3 підсилювачі сигналів, виходи яких підключені відповідно до першого та другого входів суматора 4, вихід якого з'єднаний з каналом передавання інформації 1, до якого також підключені входи перетворювачів переднього 5 та заднього 6 фронтів на імпульс, виходи яких з'єднані відповідно з першим та другим входами схеми співпадіння 7, вихід якої підключений до тактового входу С тригера 8, генератор опорної частоти 9, паралельний інтерфейс 10, перші два виходи якого з'єднані відповідно зі входами прямого 2 та інверсного 3 підсилювачів сигналу, а третій - зі входом скидання на нуль R тригера 8, інформаційний вхід D якого підключений до його інверсного виходу, до першого входу INT1 програмованого контролера переривань 11 і до входу дозволу роботи G нульового СТ0 лічильника програмованого таймера 12, а прямий вихід - до другого входу INT2 програмованого контролера переривань 11 і до входу дозволу роботи G першого СТ1 лічильника програмованого таймера 12, тактові входи С лічильників СТ0 та СТ1 якого з'єднані з виходом генератора опорної частоти 9, за допомогою системного каналу 13 персонального комп'ютера 14 центральний процесор 15 зв'язаний з оперативним 16 та постійним 17 запам'ятовувальними пристроями, а також носієм інформації 18, що входять до складу персонального комп'ютера 14, а крім цього

- з паралельним інтерфейсом 10 і програмованими контролером переривань 11 і таймером 12.

Функції Хаара природно мають кодову відстань, яка дорівнює 4. Виходячи з виразу (1), це означає, що їх використання без усяких додаткових заходів дозволяє не лише виявляти, але й виправляти помилки, Крім цього, вони реалізуються біполярним сигналом, що само собою виключає наявність постійної складової у канальному сигналі і, як наслідок, виключення між символьних завад першого та другого роду.

У відповідності із правилами побудови складається матриця Хаара, яка має вигляд (2).

$$H_8 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & -1 & -1 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix} \quad (2)$$

Здійснивши циклічний зсув рівнів сигналів, можна отримати додаткову матрицю (3):

$$\overline{H_8} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & -1 & -1 & -1 \\ 0 & 0 & -1 & -1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & -1 & -1 \\ 0 & -1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & -1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & -1 \end{bmatrix} \quad (3)$$

Об'єднавши ці дві матриці, можна отримати шістнадцять кодових комбінацій із кодовою відстанню d=4. Їм у відповідність можна поставити шістнадцять інформаційних кодових комбінацій, 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).

Таблиця 1

Приклад таблиці відповідності між кодовими комбінаціями та інформаційними повідомленнями

Інформаційне повідомлення	Кодова комбінація
0000	11111111
0001	1-1000000
0010	11110-111
0011	111 100-1-1
0100	11-1-10000
0101	1111-1-1-1-1
0110	0000-1-1-1-1
0111	110-11111
1000	000011-1-1
1001	10101010
1010	00-1-11111
1011	00000000
1100	1111110-1
1101	0-1111111
1110	001-10000
1111	0000001-1

$N_k - k_k!$ (4)

де k_k - кількість кодових комбінацій.

$N_n = C_8^4 N$ (5)

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

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 чотири двійкові розряди. Кількість можливих варіантів таких сполучень буде визначатися формулою (5).

Після перекодування інформаційних повідомлень центральним процесором 15 персонального комп'ютера 14, він налаштовує паралельний інтерфейс 10 на просте виведення інформації. Необхідні рівні сигналу формуються за допомогою перших двох виводів порту. Якщо в каналі зв'язку потрібно сформувати 1, то одиниця записується у перший розряд на необхідний проміжок часу, який визначається за формулою:

$$\tau = \frac{1}{v_n} \quad (6)$$

де V_n - швидкість передавання інформації.

Лічильник часу організовується в програмному режимі за допомогою персонального комп'ютера 14. Таким чином в послідовному коді формуються кодові комбінації, які за допомогою прямого 2 та інверсного підсилювачів сигналів, а також сумматора 4 перетворюються на канальний сигнал і передаються до приймача каналом передавання інформації 1. Процес продовжується, поки всі кодові комбінації не будуть переслані до приймача.

На приймальному боці ініціалізація пристроїв полягає у налаштовуванні лічильників програмованого таймера 12 на роботу у режимі термінального рахування, а програмованого контролера переривань 11 - на режим циклічного зсуву пріоритету. Процес ініціалізації завершується завантаженням лічильників СТ0 та СТ1 програмованого таймера 12 і скиданням тригера 8 за допомогою паралельного інтерфейсу 10.

Надходження з каналу передавання інформації 1 інформаційних імпульсів викликає їх перетворення пристроями 5 та 6, як це подано на фіг. 2 і формування коротких імпульсів, які відповідають фронтам сигналів. За допомогою схеми співпадіння 7 і тригера 8, який працює в лічильному режимі, з них утворюються контрольовані часові інтервали, вимірювання яких здійснюється лічильниками СТ0 та СТ1 програмованого таймера 12. При цьому після завершення квантування часових інтер-

валів у лічильниках CT0 та CT1 програмованого таймера 12 будуть зафіксовані числа

$$N_i = \frac{\tau_i}{T_0} = \tau_i \ f_0 \qquad (7)$$

де T_0 та f_0 - відповідно період та частота сигналу генератора опорної частоти 9

Завершення квантування кожного часового інтервалу визначається зупинкою роботи відповідного лічильника програмованого таймера 12 і формуванням сигналу переривання за відповідним вектором INT1 чи INT2 програмованим контролером 11 За цим сигналом, центральний процесор здійснює зчитування зафіксованого значення тривалості імпульсу з лічильника програмованого таймера 12 до оперативного запам'ятовувального пристрою 16 персонального комп'ютера 14 і пере завантаження лічильника Після отримання всієї кодової комбінації з каналу передавання інформації 1, вона відновлюється центральним процесором 15 персонального комп'ютера 14, У випадку відсутності помилок вона перетворюється на початкову у відповідності з таблицею перекодування і записується на носій інформації 18 персонального комп'ютера 14

Наявність помилок контролюється за тривалістю кожного імпульсу кодової комбінації, яка є фіксованою для даної швидкості передавання, а також за послідовністю надходження імпульсів, яка визначається формою функцій Хаара Якщо під час приймання була сприйнята помилка, як це подано на фіг 3, то вона легко визначається за обома показниками і легко вилучається з кодової комбінації Після цього її перетворюють на початкову у відповідності з таблицею перекодування і записують на носій інформації 18 персонального комп'ютера 14

Процес продовжується до тих пір, поки все повідомлення не буде прийняте

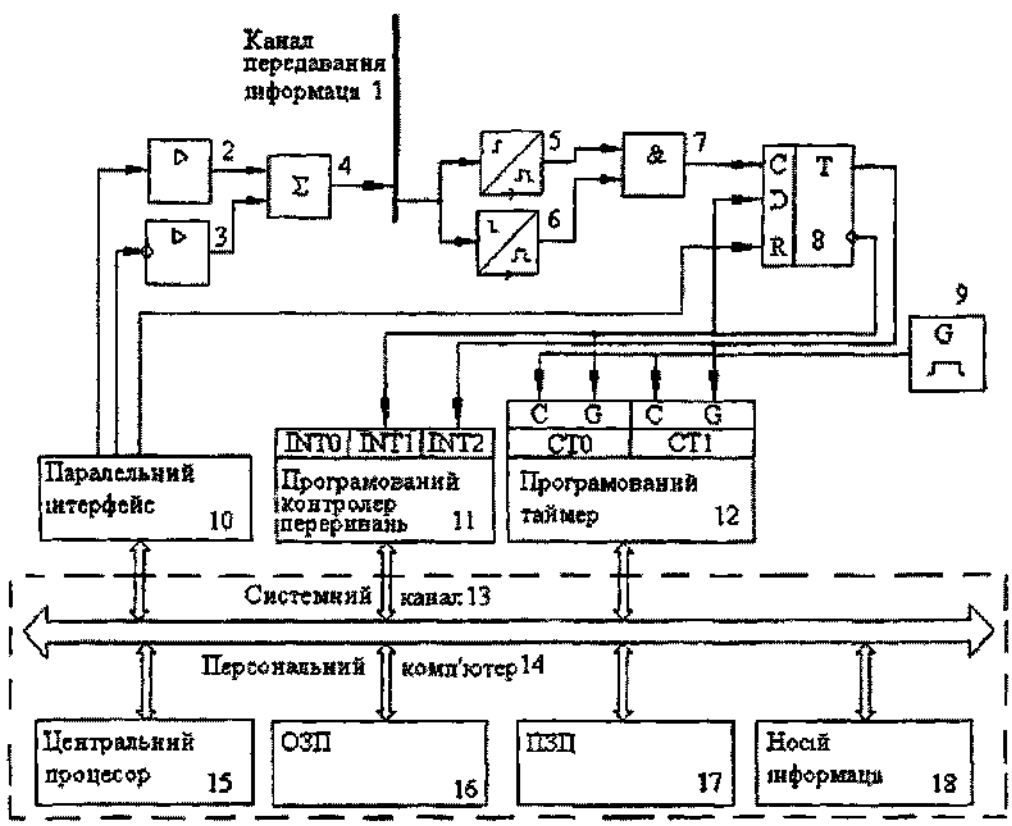
Оскільки для передавання інформації використано код із кодовою відстанню 4, то він може виправлять одну помилку у кожній кодовій комбінації Отже завадозахищеність обміну інформацією підвищується

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

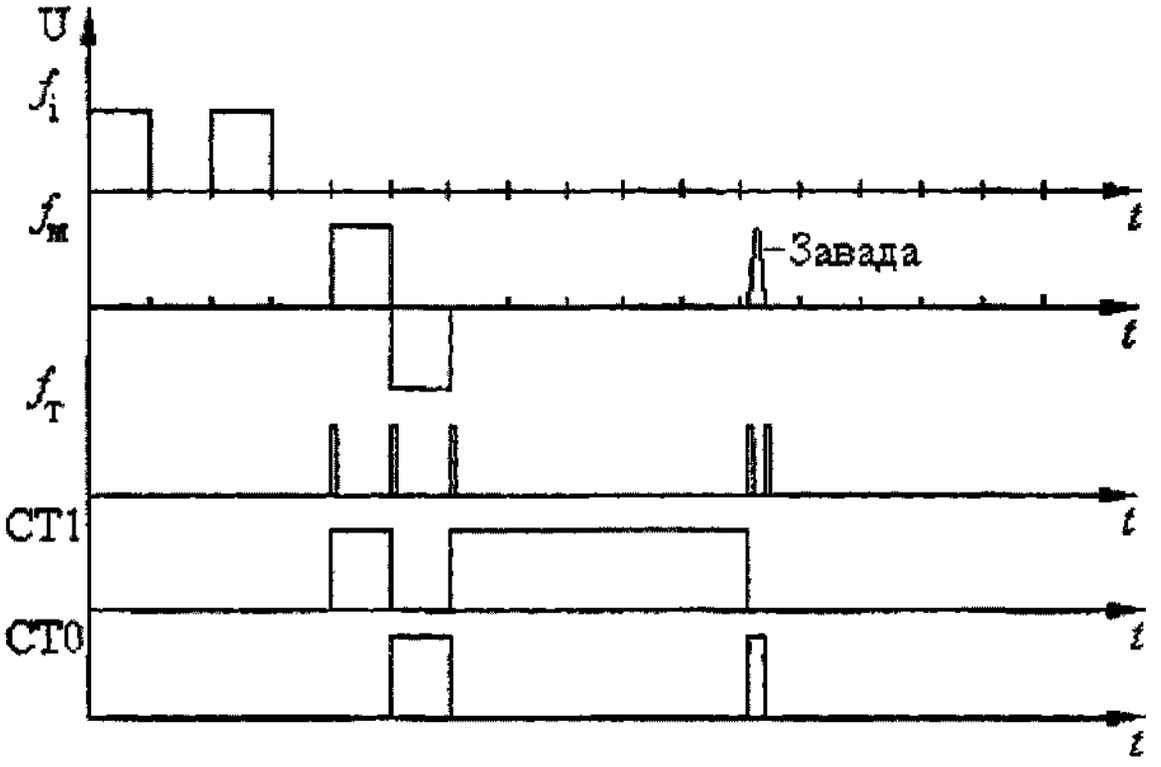
$$N_\Sigma = N_k \ N_n = k_k! C_{8\,N}^4 = \frac{k_k!(8\ N)!}{4!(8\ N-4)!} \qquad (8)$$

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

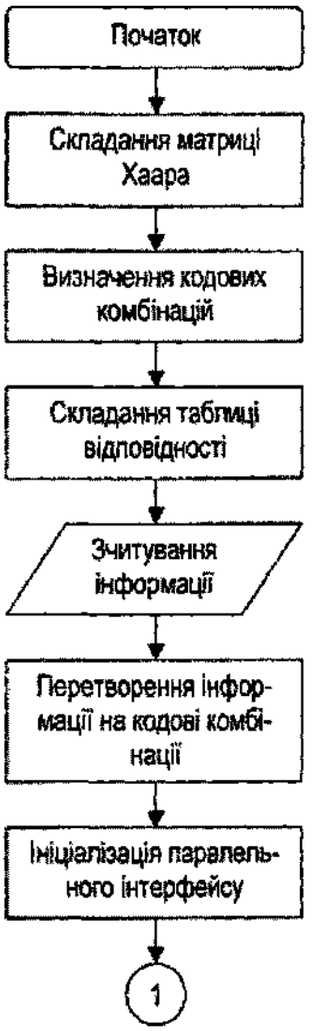
Пропоновані спосіб та пристрій для його реалізації доцільно будувати на базі персонального комп'ютера IBM PC Інтерфейси, програмовані таймери, програмовані контролери переривань та інші блоки випускаються серійно, або легко реалізуються на інтегральних схемах



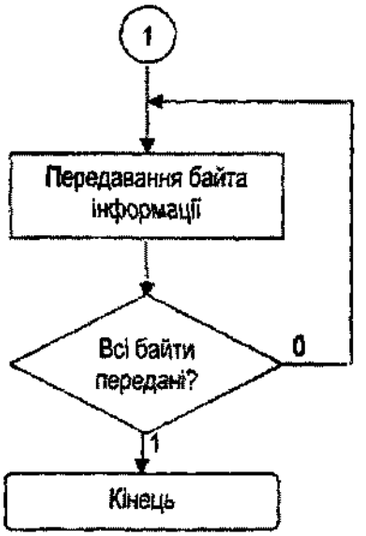
Фіг. 1



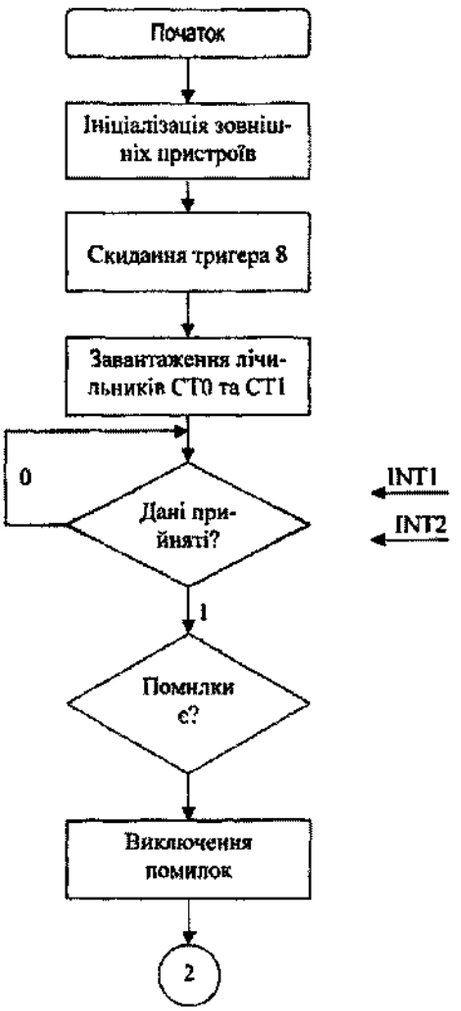
Фіг. 2



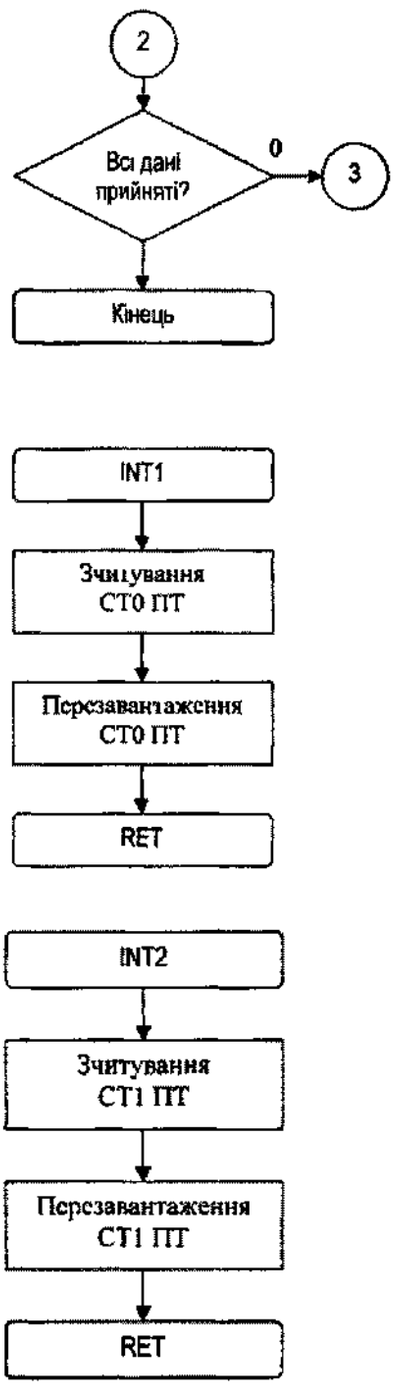
Фіг. 3



Продовження Фіг.3



Фіг. 4



Продовження Фіг.4

Комп'ютерна верстка Г. Паяльніков Підписне Тираж 28 прим.

Міністерство освіти і науки України

Державний департамент інтелектуальної власності, вул Урицького, 45, м Київ, МСП, 03680, Україна

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