**УКРАЇНА** **(19) UA** **(11) 153399** **(13) U**

**(51)** МПК (2023.01)
***G06F 7/58*** (2006.01)
**G07C 15/00**

**НАЦІОНАЛЬНИЙ ОРГАН ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ДЕРЖАВНА ОРГАНІЗАЦІЯ "УКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ОФІС ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ТА ІННОВАЦІЙ"**

# (12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

**(21)** Номер заявки: **u 2022 05118**

**(22)** Дата подання заявки: **29.12.2022**

**(24)** Дата, з якої є чинними права інтелектуальної власності: **29.06.2023**

**(46)** Публікація відомостей про державну реєстрацію: **28.06.2023, Бюл.№ 26**

**(72)** Винахідник(и):
**Торба Алєксандр Алєксєєвіч (UA),**
**Ткачов Віталій Миколайович (UA),**
**Дяченко Владислав Олександрович (UA),**
**Партика Станіслав Олександрович (UA),**
**Єрошенко Ольга Артурівна (UA)**

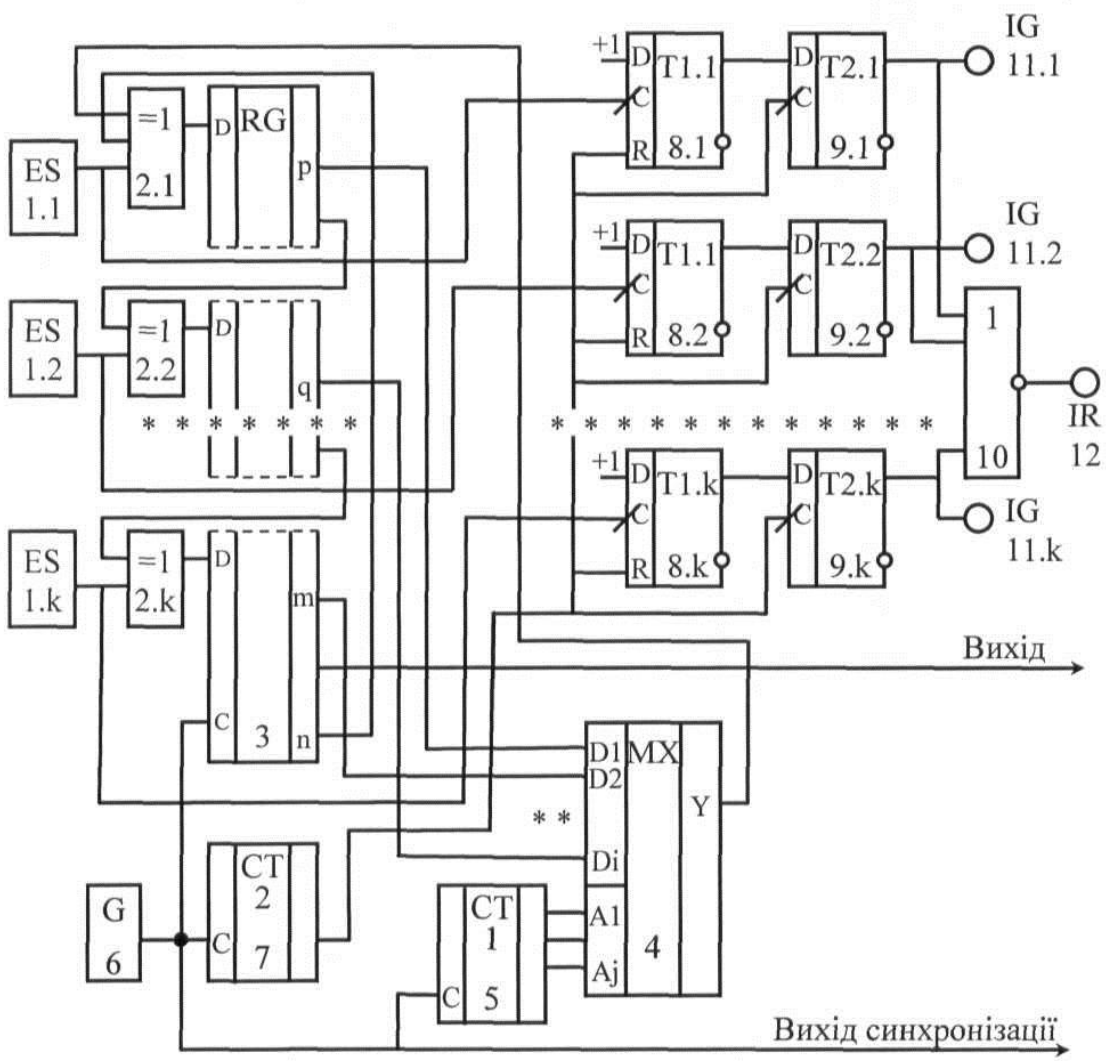
**(73)** Володілець (володільці):
**ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ**,
пр. Науки, 14, м. Харків, 61166 (UA)

## (54) НЕДЕТЕРМІНОВАНИЙ ГЕНЕРАТОР ВИПАДКОВИХ БІТІВ

**(57)** Реферат:

Недетермінований генератор випадкових бітів, що містить k джерел ентропії, виходи яких підключені до перших входів k елементів "ВИКЛЮЧНЕ АБО", а їх виходи з'єднані з проміжними входами регістра зсуву, поділеного на k частин, останні виходи кожної частини регістра зсуву підключені до других входів наступних елементів "ВИКЛЮЧНЕ АБО", другий вхід першого елемента "ВИКЛЮЧНЕ АБО" з'єднаний з останнім виходом регістра зсуву, а третій вхід першого елемента "ВИКЛЮЧНЕ АБО" з'єднаний з виходом мультиплексора, інформаційні входи якого підключені до проміжних виходів регістра зсуву у довільному порядку, і лічильника імпульсів, останні виходи якого підключені до адресних входів мультиплексора, а також тактовий генератор, вихід якого з'єднаний з синхровходом регістра зсуву і лічильника імпульсів, а вихід пристрою є одним з виходів регістра зсуву, згідно з корисною моделлю, додатково введені k каналів контролю справності джерел ентропії, кожен канал включає перший D-тригер, що тактується фронтом, у якому вхід D підключений до постійної напруги з рівнем "логічної одиниці", синхровхід з'єднаний з виходом відповідного джерела ентропії, а вихід першого тригера підключений до входу D другого тригера, вихід якого з'єднаний з світлодіодним індикатором, а також виходи усіх других тригерів підключені до входів додаткового логічного елемента АБО-НІ, вихід якого з'єднаний з світлодіодним індикатором "Аварія", а також додатково введений другий лічильник імпульсів, вхід якого з'єднаний з виходом тактового генератора, а вихід другого лічильника імпульсів підключений до входів скидання усіх перших тригерів в кожному каналі контролю справності джерел ентропії і до синхровходів усіх других тригерів в кожному каналі контролю справності джерел ентропії і вихід тактового генератора є виходом синхронізації всього пристрою.

UA 153399 U


ES 1.1
ES 1.2
ES 1.k
=1 2.1
=1 2.2
=1 2.k
D RG p
D q
D m n
C 3
G 6
CT 2
C 7
CT 1
C 5
+1
D T1.1
C
R 8.1
D T2.1
C 9.1
IG 11.1
R 8.2
D T2.2
C 9.2
IG 11.2
1
10
IR 12
T1.k
R 8.k
T2.k
9.k
IG 11.k
Вихід
D1 MX
D2
Y
Di
A1
Aj
4
Вихід синхронізації

Корисна модель належить до області обчислювальної техніки і може бути використана в системах захисту інформації обчислювальних систем, наприклад при генерації параметрів алгоритмів криптографічного перетворення, в протоколах аутентифікації, в засобах імовірнісного кодування та ін.

Відомий генератор рівномірно розподілених випадкових послідовностей (див. деклараційний патент України № 50386 А, МПК6 G06F 7/58, G07C 15/00, опублікований 15.10.2002, Бюл. №10), що містить n джерел ентропії, які складаються з послідовно з'єднаних генератора шуму, підсилювача-обмежувача та лічильного тригера, виходи джерел ентропії підключені до перших входів n елементів "ВИКЛЮЧНЕ АБО", виходи яких з'єднані з входами регістра зсуву, поділеного на n частин, а останні виходи кожної частини регістра зсуву підключені до других входів наступних елементів "ВИКЛЮЧНЕ АБО", входи першого елемента "ВИКЛЮЧНЕ АБО" з'єднані з останнім виходом регістра зсуву та проміжним виходом цього регістра, виходи регістра зсуву підключені до входів вихідного паралельного регістру, а його виходи підключені до шини даних ПЕОМ, тактовий генератор, вихід якого з'єднаний з синхровходами регістра зсуву і входом лічильника імпульсів, вихід якого під'єднай до синхровходу вихідного паралельного регістра та входу тригера "прапора", а його вихід з'єднаний з входом запиту переривання ПЕОМ і через буферний елемент "І" з шиною даних ПЕОМ, та дешифратор адреси, включений входами до шини адреси ПЕОМ, а першим виходом до входу дозволу вихідного регістра і входу скидання тригера "прапора", і другим виходом до буферного елемента "І".

Недоліком цього генератора є його недостатня крипостійкість у випадку повного збою усіх джерел ентропії.

Як найближчий аналог вибрано генератор випадкових бітових послідовностей на основі ЛРР зі змінами параметрів рекуренти (див. рисунок 6.4 в монографії: Торба А.А. Методы и средства генерации случайных битовых последовательностей: Под ред. д.т.н., проф. Горбенко И.Д. / А.А.Торба, А.А. Бобкова, Ю.И. Горбенко, В.А. Бобух. - Харьков: Изд-во "Форт", 2012. - 232 с.), що містить k джерел ентропії, підключених до перших входів елементів "ВИКЛЮЧНЕ АБО", виходи яких з'єднані з проміжними входами регістра зсуву, поділеного на k частин, а останні виходи кожної частини регістра зсуву підключені до других входів наступних елементів "ВИКЛЮЧНЕ АБО", другий вхід першого елемента "ВИКЛЮЧНЕ АБО" з'єднаний з останнім виходом регістра зсуву, а третій вхід першого елемента "ВИКЛЮЧНЕ АБО" з'єднаний з виходом мультиплексора, інформаційні входи якого підключені до проміжних виходів регістра зсуву у довільному порядку, тактовий генератор, вихід якого з'єднаний з синхровходами регістра зсуву і лічильника імпульсів, останні виходи якого підключені до адресних входів мультиплексора.

Цей генератор рівномірно розподілених випадкових бітових послідовностей має високу надійність роботи за рахунок гарячого резервування джерел ентропії, а також високу крипостійкість у випадку повного збою усіх джерел ентропії згідно з Міжнародним стандартом ISO/EEC 18031:2005.

Але при проведенні регламентних робіт оператору треба знати, які джерела ентропії є справними, а які втратили роботоспроможність і потребують заміни.

В основу корисної моделі поставлена задача підвищити надійність роботи за рахунок створення такого недетермінованого генератора випадкових бітів, в якому додавання нових схемних елементів і зв'язків дозволило б контролювати справність джерел ентропії і виводити на індикатори стан параметрів, які контролюються.

Поставлена задача може бути вирішена, якщо у недетермінований генератор випадкових бітів, що містить k джерел ентропії, виходи яких підключені до перших входів k елементів "ВИКЛЮЧНЕ АБО", а їх виходи з'єднані з проміжними входами регістра зсуву, поділеного на k частин, останні виходи кожної частини регістра зсуву підключені до других входів наступних елементів "ВИКЛЮЧНЕ АБО", другий вхід першого елемента "ВИКЛЮЧНЕ АБО" з'єднаний з останнім виходом регістра зсуву, а третій вхід першого елемента "ВИКЛЮЧНЕ АБО" з'єднаний з виходом мультиплексора, інформаційні входи якого підключені до проміжних виходів регістра зсуву у довільному порядку, і лічильника імпульсів, останні виходи якого підключені до адресних входів мультиплексора, а також тактовий генератор, вихід якого з'єднаний з синхровходом регістра зсуву і лічильника імпульсів, а вихід пристрою є одним з виходів регістра зсуву, згідно з корисною моделлю, додатково введені k каналів контролю справності джерел ентропії, кожен канал включає перший D-тригер, що тактується фронтом, у якому вхід D підключений до постійної напруги з рівнем "логічної одиниці", синхровхід з'єднаний з виходом відповідного джерела ентропії, а вихід першого тригера підключений до входу D другого тригера, вихід якого з'єднаний з світлодіодним індикатором, а також виходи усіх других тригерів підключені до входів додаткового логічного елемента АБО-НІ, вихід якого з'єднаний з світлодіодним індикатором

"Аварія", а також додатково введений другий лічильник імпульсів, вхід якого з'єднаний з виходом тактового генератора, а вихід другого лічильника імпульсів підключений до входів скидання усіх перших тригерів в кожному каналі контролю справності джерел ентропії і до синхровходів усіх других тригерів в кожному каналі контролю справності джерел ентропії і вихід тактового генератора є виходом синхронізації всього пристрою.

На кресленні зображена структурна схема недетермінованого генератора випадкових бітів. На кресленні використані наступні міжнародні позначення: ES - джерело ентропії, RG - регістр, MS - мультиплексор, G - генератор, CT - лічильник T - тригер, IG - індикатор зелений, IR - індикатор червоний.

Недетермінований генератор випадкових бітів містить k джерел 1.1…1.k ентропії, виходи яких підключені до перших входів елементів 2.1…2.k "ВИКЛЮЧНЕ АБО", а їх виходи з'єднані з проміжними входами регістра 3 зсуву, поділеного на k частин (необов'язково рівних), останні виходи кожної частини регістра 3 зсуву підключені до других входів наступних елементів 2.2…2.k "ВИКЛЮЧНЕ АБО", другий вхід першого елемента 2.1 "ВИКЛЮЧНЕ АБО" з'єднаний з останнім виходом регістра 3 зсуву, а третій вхід першого елемента 2.1 "ВИКЛЮЧНЕ АБО" з'єднаний з виходом мультиплексора 4, інформаційні входи якого підключені до проміжних виходів регістра 3 зсуву у довільному порядку, і перший лічильник 5 імпульсів, останні виходи якого підключені до адресних входів мультиплексора 4, а також тактовий генератор 6, вихід якого з'єднаний з синхровходом регістра 3 зсуву і синхровходами першого 5 та другого 6 лічильників імпульсів. Вихід цього тактового генератора 6 є виходом синхронізації всього пристрою. Кожен канал контролю справності джерел 1.1….1.k ентропії включає перший D-тригер 8.1…8.k, що тактується фронтом, у якому вхід D підключений до постійної напруги з рівнем "логічної одиниці", синхровхід з'єднаний з виходом відповідного джерела 1.1…1.k ентропії, а вихід першого тригера 8.1…8.k підключений до входу D другого тригера 9.1…9.k, вихід якого з'єднаний з світлодіодним індикатором 11.1…11.k, а також виходи усіх других тригерів 9.1…9.k підключені до входів додаткового логічного елемента 10 АБО-НІ, вихід якого з'єднаний з світлодіодним індикатором 12 "Аварія", а також додатково введений другий лічильник 7 імпульсів, вхід якого з'єднаний з виходом тактового генератора, а вихід другого лічильника 7 імпульсів підключений до входів скидання усіх перших тригерів 8.1…8.k в кожному каналі контролю справності джерел ентропії і до синхровходів усіх других тригерів 9.1…9.k в кожному каналі контролю справності джерел ентропії і вихід тактового генератора 6 є виходом синхронізації всього пристрою.

Недетермінований генератора випадкових бітів працює наступним чином.

На виходах джерел 1.1…1.k ентропії формуються логічні рівні, які з рівною імовірністю приймають значення нуля або одиниці в випадкові моменти часу. Ці випадкові логічні рівні перемикають на протилежні значення логічні рівні, що подаються з останніх виходів частин регістра 3 зсуву до входів наступних частин цього регістра, в випадкові моменти часу за допомогою елементів 2.1…2.k "ВИКЛЮЧНЕ АБО". Тактовий генератор 6 визначає частоту зсуву випадкових бітів в регістрі 3 зсуву і таким чином визначає швидкість формування випадкових бітів, які за рахунок дії джерел 1.1…1.k ентропії стають непередбачуваними, недетермінованими.

Для зміни параметрів рекуренти регістра 3 зсуву логічні сигнали з його проміжних виходів подаються на інформаційні входи мультиплексора 4, вихід якого підключено до третього входу першого елемента 2.1 "ВИКЛЮЧНЕ АБО". Адресні входи мультиплексора 4 підключені до останніх виходів першого лічильників 5 імпульсів.

Процедура контролю справності джерел 1.1…1.k ентропії враховує той факт, що стандарт ISO/IEC 18031: 2005 (Information technology-Security techniques-Random bit generation) не накладає жорсткі обмеження на параметри джерела (джерел) ентропії. Це джерело може бути зміщеним (тобто імовірність появи нулів і одиниць на виході не обов'язково має бути рівною) і вихідні біти можуть навіть залежати один від одного. Єдина обов'язкова вимога - джерело ентропії повинне генерувати біти з ненульовою ентропією.

Згідно з формулою Шенона ентропія для бінарних сигналів дорівнює:

$H(X) = - (P(0) * \log_2(P0) + P(1) * \log_2(P(1))$.

Тому нульовій ентропії відповідають:

або імовірність P (0) = 0, (при цьому P (1) =1);

або імовірність P (1) = 0, (при цьому P (0) =1),

тобто сигнал на виході джерела ентропії постійно дорівнює "логічному нулю" або "логічній одиниці" і не переходить з одного логічного стану в інший.

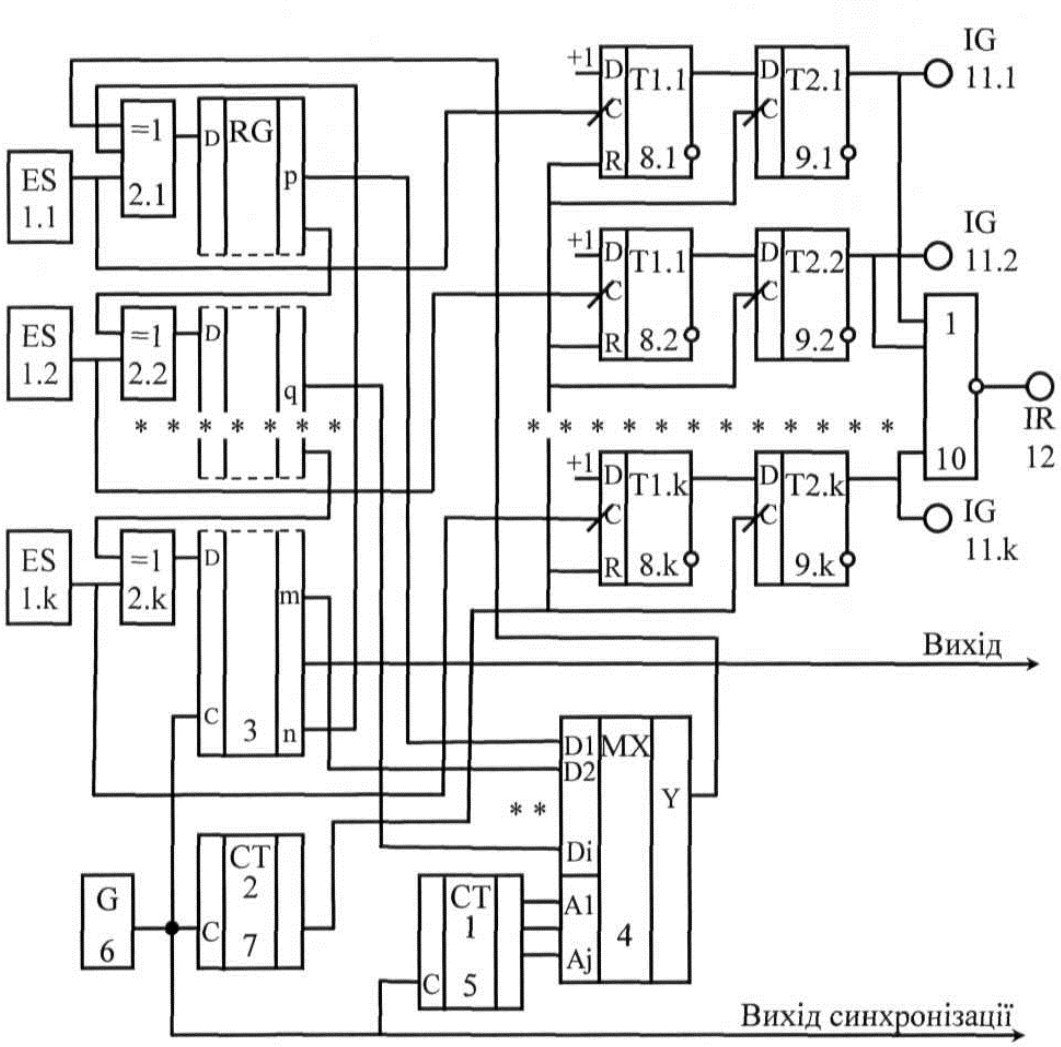
Схеми контролю справності джерел ентропії 1.1…1.1c перевіряють факт переходу вихідного стану із "логічного нуля" в "логічну одиницю" за період часу, що у тисячі разів більше періоду

вихідних імпульсів справного джерела ентропії 1.1…1.k. Справність конкретного джерела ентропії висвітлюється відповідним світлодіодним індикатором 11.1…11.k. А несправність усіх джерел ентропії 1.1…1.k висвітлюється світлодіодним індикатором 12 "Аварія".

Таким чином, вирішена задача підвищення надійності роботи за рахунок створення такого недетермінованого генератора випадкових бітів, в якому додавання нових схемних елементів і зв'язків дозволило контролювати справність джерел ентропії і виводити на індикатори стан параметрів, які контролюються.

## ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Недетермінований генератор випадкових бітів, що містить k джерел ентропії, виходи яких підключені до перших входів k елементів "ВИКЛЮЧНЕ АБО", а їх виходи з'єднані з проміжними входами регістра зсуву, поділеного на k частин, останні виходи кожної частини регістра зсуву підключені до других входів наступних елементів "ВИКЛЮЧНЕ АБО", другий вхід першого елемента "ВИКЛЮЧНЕ АБО" з'єднаний з останнім виходом регістра зсуву, а третій вхід першого елемента "ВИКЛЮЧНЕ АБО" з'єднаний з виходом мультиплексора, інформаційні входи якого підключені до проміжних виходів регістра зсуву у довільному порядку, і лічильника імпульсів, останні виходи якого підключені до адресних входів мультиплексора, а також тактовий генератор, вихід якого з'єднаний з синхровходом регістра зсуву і лічильника імпульсів, а вихід пристрою є одним з виходів регістра зсуву, який **відрізняється** тим, що додатково введені k каналів контролю справності джерел ентропії, кожен канал включає перший D-тригер, що тактується фронтом, у якому вхід D підключений до постійної напруги з рівнем "логічної одиниці", синхровхід з'єднаний з виходом відповідного джерела ентропії, а вихід першого тригера підключений до входу D другого тригера, вихід якого з'єднаний з світлодіодним індикатором, а також виходи усіх других тригерів підключені до входів додаткового логічного елемента "АБО-НІ", вихід якого з'єднаний з світлодіодним індикатором "Аварія", а також додатково введений другий лічильник імпульсів, вхід якого з'єднаний з виходом тактового генератора, а вихід другого лічильника імпульсів підключений до входів скидання усіх перших тригерів в кожному каналі контролю справності джерел ентропії і до синхровходів усіх других тригерів в кожному каналі контролю справності джерел ентропії і вихід тактового генератора є виходом синхронізації всього пристрою.




Комп'ютерна верстка Л.Бурлак

ДО "Український національний офіс інтелектуальної власності та інновацій", вул. Глазунова, 1, м. Київ – 42, 01601