March 29, 2024;
Cambridge, United Kingdom

SECTION 22.
INFORMATION TECHNOLOGIES AND SYSTEMS

DOI 10.36074/logos-29.03.2024.067

ПІДВИЩЕННЯ НАДІЙНОСТІ НЕДЕРМІНОВАНИХ ГЕНЕРАТОРІВ ВИПАДКОВИХ БІТІВ

Торба Алєксандр Алєксєєвіч[1], Рибалка Антоніна Іванівна[2], Мегель Юрій Євгенович[3]

1. канд. техн. наук, доцент, професор кафедри ЕОМ
Харківський національний університет радіоелектроніки, м. Харків, УКРАЇНА
ORCID ID: 0000-0003-2993-2955

2. канд. фіз.- мат. наук, доцент кафедри фізики
Харківський національний університет радіоелектроніки, м. Харків, УКРАЇНА
ORCID ID: 0000-0002-4148-2443

3. доктор техн. наук, старший науковий співробітник
кафедри інтелектуальних технологій та систем, професор
Харківський національний університет радіоелектроніки, м. Харків, УКРАЇНА
ORCID ID: 0000-0003-0072-0756

Вступ

Граничні характеристики стійкості систем криптографічного захисту інформації (КЗІ) досягаються в разі, якщо для формування ключів, параметрів і синхромаркерів використовується генератор випадкових бітів – ГВБ (або випадкових послідовностей – ГВП) на основі фізичних датчиків шуму з найкращими параметрами рівноймовірності, незалежності і некорельованості.

Ще в XIX сторіччі голландець А. Керкгоффс сформулював головні вимоги до криптографічних систем, які залишається актуальними і понині, – друга та третя вимоги А. Керкгоффса до криптосистем [1]: 2. Потрібно, щоб не було потреби збереження системи в таємниці; потрапляння системи в руки ворога не повинно завдавати незручностей; 3. Зберігання і передача ключа повинні бути здійсненні без допомоги паперових записів; кореспонденти повинні мати можливість змінювати ключ на свій розсуд.

Тобто – секретність шифрів повинна бути заснована не на секретності алгоритму, а на секретності ключа (параметра алгоритму), який можливо змінювати.

Шеннон сформулював цей принцип (ймовірно, незалежно від А. Керкгоффса) таким чином: «Ворог знає систему».

Але і надійність систем КЗІ значною мірою визначається надійністю генераторів випадкових бітів (випадкових послідовностей). Несправність генератора випадкових бітів унеможливлює нормальну (штатну) роботу системи КЗІ.

1. Вимоги до генераторів випадкових бітів

Міжнародний стандарт ISO/IEC 18031:2005 – Information technology – Security techniques – Random bit generation (Інформаційні технології – Методи захисту – Генерація випадкових бітів) [2] встановлює обов'язкові вимоги, яких необхідно дотримуватися при розробці генераторів випадкових бітів для криптографічних застосувань.

Ці криптографічні застосування включають наступне [3]:

– випадкові ключі і значення ініціалізації для шифрування;
– випадкові особові ключі для алгоритмів цифрового підпису;
– випадкові значення, які використовуються в механізмах аутентифікації об'єктів;
– генерація випадкових PIN, паролів та ін.

Стандарт ISO/IEC 18031:2005 визначає два типи генераторів: недерміновані і детерміновані генератори випадкових бітів [2, 3].

Недетермінований генератор випадкових бітів – НГВБ (non deterministic random bit generator – NRBG) – це механізм генерації випадкових бітів, який використовує джерело ентропії (джерело невизначеності) для генерації випадкового потоку бітів (випадкових послідовностей).

Детермінований генератор випадкових бітів – ДГВБ (deterministic random bit generator – DRBG) – це механізм генерації бітів, який використовує детерміновані алгоритми, такі як криптографічні алгоритми, на джерелі ентропії для генерації випадкового потоку бітів (випадкових послідовностей). У цьому типі генерації бітів використовується особливі вхідні дані (початкові значення) і, можливо, деякі необов'язкові вхідні дані, які можуть (чи не можуть) бути загальнодоступними.

Обов'язковою вимогою при проектуванні НГВБ є наявність джерела (або джерел) ентропії (entropy source – ES) у вигляді фізичного генератора шуму. З урахуванням кінцевої надійності (тобто імовірність безвідмовної роботи менш одиниці) аналогових фізичних генераторів шуму (джерел ентропії) в стандарті ISO/IEC 18031:2005 введена вимога продовження роботи недетермінованого генератора випадкових бітів (НГВБ) способом, не менш захищеним, ніж детермінований генератор випадкових бітів (ДГВБ), у разі повного збою джерела (або усіх джерел) ентропії [2].

Стандарт ISO/IEC 18031:2005 не накладає жорсткі обмеження на параметри джерела 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.

У обчислювальній техніці джерела ентропії найчастіше реалізують на основі генераторів шуму на кремнієвих діодах із Зенерівським пробоєм (стабілітронах) [3].

2. Генератори випадкових бітових послідовностей

Значною мірою вимогам стандарту ISO/IEC 18031:2005 задовольняє генератор рівномірно розподілених випадкових бітових послідовностей, описаний в деклараційному патенті України № 36108А [6]. Спрощена схема цього генератора наведена на рисунку 1.

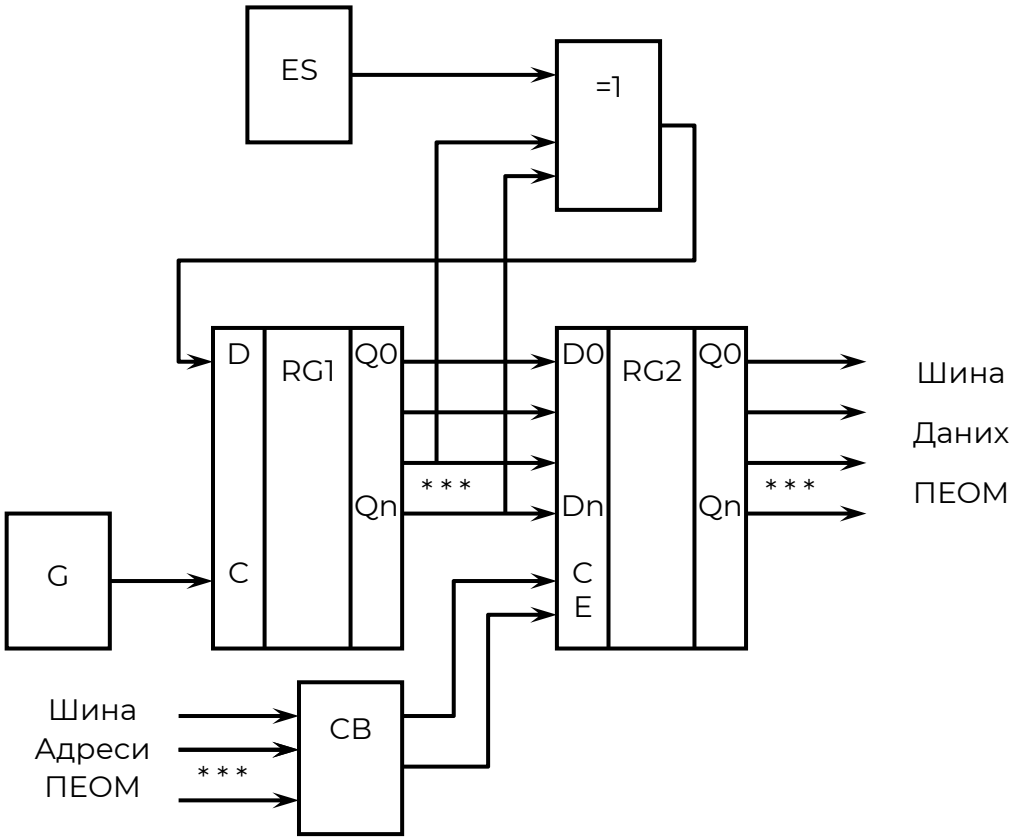

Рис. 1 **Генератор рівномірно розподілених випадкових послідовностей**

Основу генератора складає послідовний регістр зсуву RG1 зі зворотним зв'язком – лінійний рекурентний регістр (ЛРР). Логічні сигнали з виходу

джерела ентропії ES у випадкові моменти часу інвертують сигнал зворотного зв'язку через елемент «ВИКЛЮЧНЕ АБО», і тим самим руйнують лінійні параметри рекурентного регістру, що робить його стан непередбачуваним (випадковим).

Стан ЛРР через визначені моменти часу запам'ятовується у паралельному регістрі RG2 і по запиту ПЕОМ зчитується через паралельний інтерфейс в ЕОМ.

Більшість елементів генератора рівномірно розподілених випадкових послідовностей реалізовано на основі Програмованої Логічної Інтегральної Схеми (ПЛІС), і тільки елементи джерела ентропії ES реалізовані на дискретних елементах, що знижує надійність всього пристрою.

Для підвищення надійності в генератор випадкових бітових послідовностей згідно з деклараативним патентом України № 50386 А [7] введені декілька джерел ентропії (рисунок 2). Для цього регістр зсуву RG розбитий на *k* частин (необов'язково рівних) і на входи кожної частини регістра зсуву подаються сигнали з виходів попередніх частин цього регістра через елементи «ВИКЛЮЧНЕ АБО». Другі входи елементів «XOR» підключені до виходів додаткових джерел ентропії (ES 2...ES k).

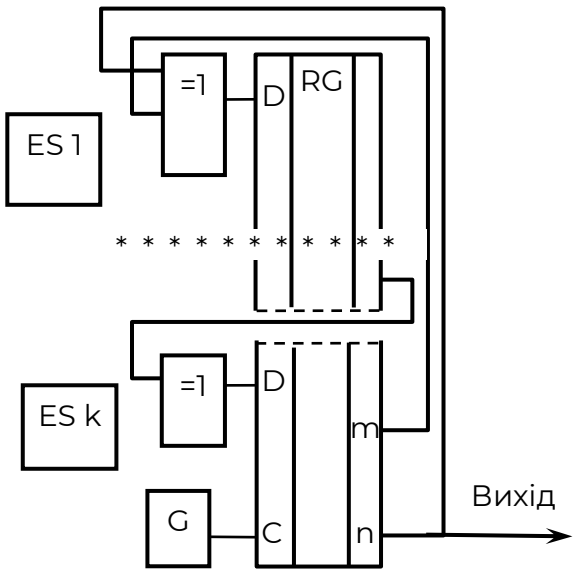

Рис. 2 **Недетермінований генератор випадкових бітів**

Таке рішення дозволяє реалізувати «гаряче резервування» джерел ентропії (ES1...ES k), тобто їх паралельну роботу. Вихідні біти НГВБ залишаються випадковими (непередбачуваними) при справній роботі хоча б одного

джерела ентропії (на виходах інших несправних джерел може бути «логічний нуль» або «логічна одиниця», тобто ентропія несправних джерел дорівнює нулю). Імовірність одночасної несправності усіх джерел ентропії в цій схемі дуже мала і дорівнює добутку імовірностей збою кожного окремого джерела ентропії.

Швидкість формування випадкових бітів визначається частотою тактового генератора (G) і для сучасних ПЛІС може бути від 10 до 1000 МГц.

У разі повного збою усіх джерел ентропії такий генератор (згідно зі стандартом ISO/IEC 18031:2005) продовжує працювати як лінійний рекурентний регістр (ЛРР), тобто детермінований генератор псевдовипадкових послідовностей, який проходить усі тести на випадковість [3].

Самі по собі ЛРР є хорошими генераторами псевдовипадкових послідовностей, але вони мають деякі небажані невипадкові властивості [3, 4]. Відомі математичні алгоритми (наприклад, алгоритм Берлекемпа-Месі) дозволяють розрахувати основні параметри рекуренти ЛРР – «m» і «n» за результатами спостереження вихідної бітової послідовності, тривалість якої в 2 рази перевищує розрядність регістра зсуву «n». Тому криптостійкість такого генератора (тобто стійкість проти хакерських атак) при повному збої усіх джерел ентропії є недостатньою.

Існує декілька методів проектування детермінованих генераторів випадкових бітів, які руйнують лінійні властивості ЛРР і тим самим роблять такі системи криптографічно стійкішими [3, 4, 5]:

– використання нелінійної функції, що об'єднує виходи декількох ЛРР (генератор Геффа та ін.);

– використання виходу одного ЛРР для управління синхросигналами іншого (чи декількох) ЛРР (алгоритм А5 та ін.);

– динамічна зміна параметрів рекуренти ЛРР (довжини регістра «n» і номерів відводів «m») в процесі формування випадкових бітів, – так звані динамічні лінійні рекурентні регістри (ДЛРР) [4, 5].

Таке технічне рішення запропоноване в патенті України на корисну модель № 52380 [8]. На рисунку 3 наведена спрощена структурна схема цього пристрою.

Номери усіх відводів регістра зсуву «m_k» повинні задовольняти відомій умові для ЛЛР [3, 4]: поліном, який обчислюється на коефіцієнтах : $1 + x^m + x^n$ – має бути примітивним і неприведеним над полем Галуа. Відводи регістра зсуву RG перемикаються до входу елемента «ВИКЛЮЧНЕ АБО» мультиплексором MX. На адресні входи мультиплексора (A1...Aj) подаються вихідні сигнали старших розрядів двійкового лічильника (СТ). Кількість

молодших розрядів лічильника визначає інтервал часу між змінами параметрів рекуренти.

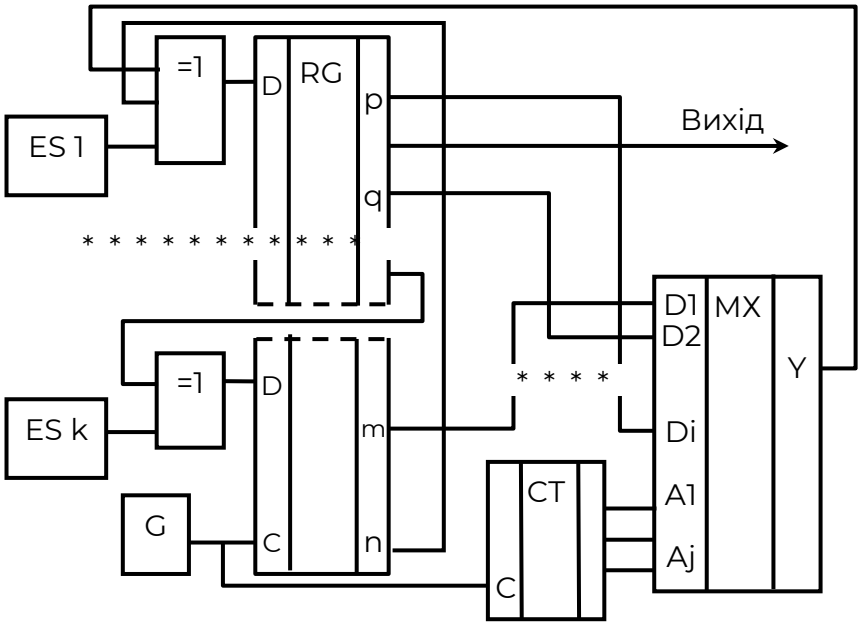

Рис. 3 **Недетермінований генератор випадкових бітів зі зміною параметрів рекуренти**

За час генерації $2n$ вихідних випадкових бітів кілька разів змінюється параметр «m_k» рекуренти ЛРР. Це робить безглуздим застосування алгоритму Берлекемпа-Мессі для розрахунку параметра рекуренти ЛРР.

Технічне рішення, запропоноване в патенті України на корисну модель № 52410 [9], дозволяє робити зміну параметрів «m_k» рекуренти ЛРР у псевдовипадковому порядку. Для цього псевдовипадкові коди з проміжних виходів регістра зсуву RG запам'ятовуються в додатковому паралельному регістрі, а виходи цього регістру підключені до адресних входів мультиплексора. Інтервал між змінами параметрів рекуренти визначається додатковим лічильником

У недетермінованому генераторі випадкових послідовностей, який запропонований в патенті України на винахід № 99017 [10], змінюються параметри рекуренти не тільки в псевдовипадковому порядку, а й через псевдовипадкові інтервали часу. Для цього на керуючи входи дільника з програмованим коефіцієнтом ділення (ДПКД), який визначає інтервали часу

між змінами параметрів рекуренти, подаються псевдовипадкові коди з виходів регістра зсуву ЛРР.

В патенті України на винахід № 96654 [10] запропоновано недетермінований генератор випадкових послідовностей, в якому два мультиплексори перемикають відводи ЛРР до входів елемента «ВИКЛЮЧНЕ АБО» в псевдовипадковому порядку. Це дозволяє змінювати не тільки номери відводів «m_k», а й довжину «n» регістра зсуву ЛРР.

В недетермінованому генераторі випадкових послідовностей, який запропоновано в патенті України на винахід № 103097 [12], два мультиплесори змінюють параметри рекуренти – «m_k» і «n» не тільки в псевдовипадковому порядку, а й через псевдовипадкові інтервали часу.

3. Особливості експлуатації генераторів випадкових послідовностей

Гаряче резервування джерел ентропії хоча й підвищує імовірність безвідмовної роботи всього НГВП, але не дає можливості контролювати стан цих джерел ентропії. При проведені регламентних робіт оператору треба знати, які джерела ентропії є справними, а які втратили роботоспроможність і потребують заміни.

В патенті України на корисну модель № 153399 [13] запропоновано недетермінований генератор випадкових послідовностей з контролем справності усіх джерел ентропії і з індикацією їх стану (рисунок 4).

Процедура контролю справності джерел ентропії враховує той факт, що стандарт ISO/IEC 18031 : 2005 (Information technology – Security techniques – Random bit generation) [2] не накладає жорсткі обмеження на параметри джерела (джерел) ентропії. 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 кожного джерела ентропії фіксують факт переходу вихідного сигналу кожного джерела із «логічного нуля» в «логічну одиницю» за період часу, що у тисячі разів більше періоду вихідних імпульсів справного джерела ентропії. робіт.

Справність конкретного джерела ентропії висвітлюється відповідним зеленим світлодіодним індикатором IG. А несправність усіх джерел ентропії висвітлюється червоним світлодіодним індикатором IR – «Аварія». Джерела

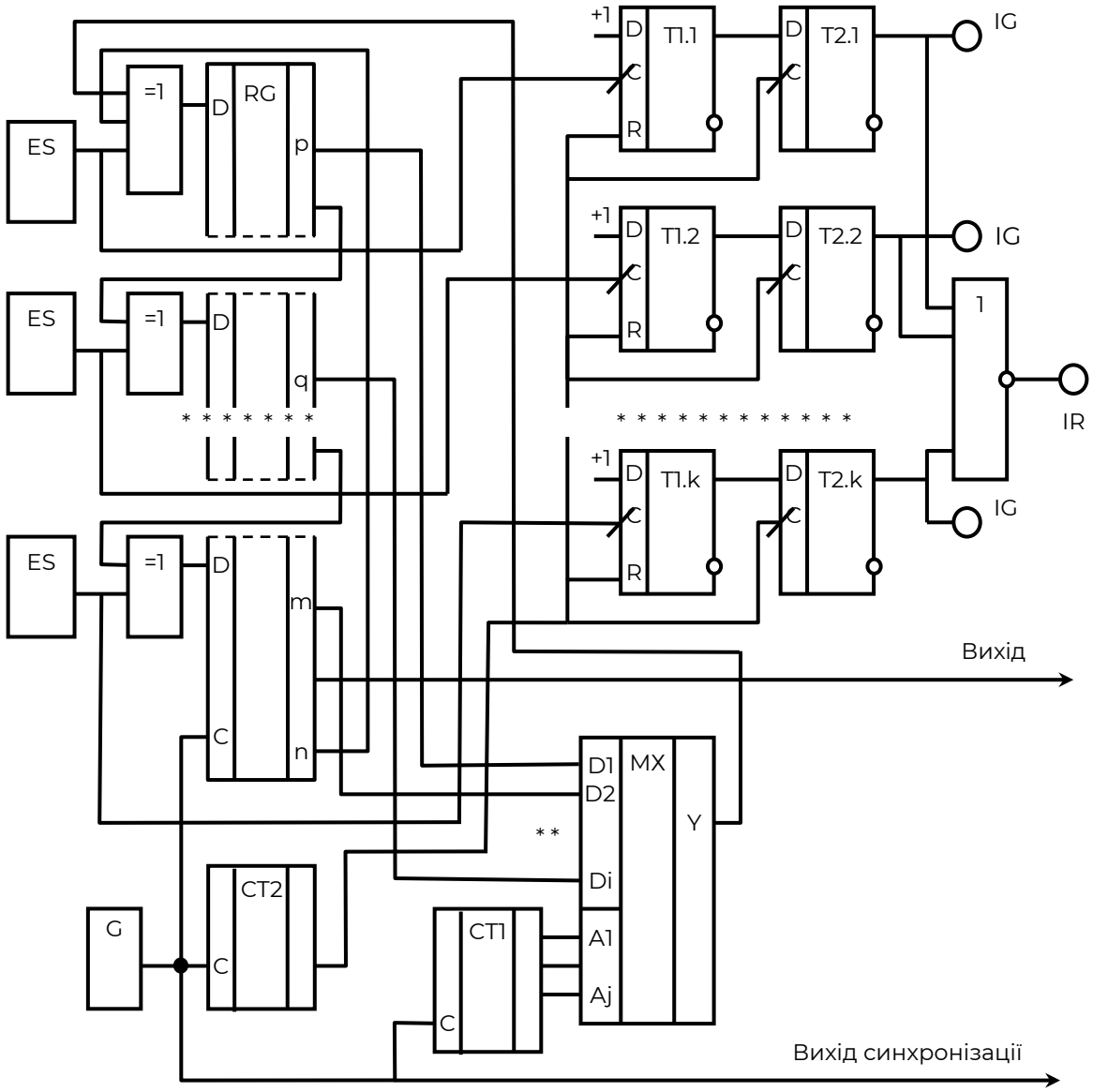

Рис. 4 **Генератор випадкових послідовностей з контролем стану джерел ентропії**

ентропії виконуються у вигляді окремих модулів на розніманнях з можливістю їх заміни при проведенні регламентних робіт.

В необслуговуваних НГВП для підвищення надійності запропоновано використовувати гаряче резервування не тільки джерел ентропії, а й усіх цифрових каналів перетворення сигналів джерел ентропії в вихідні випадкові послідовності (рисунок 5) [13].

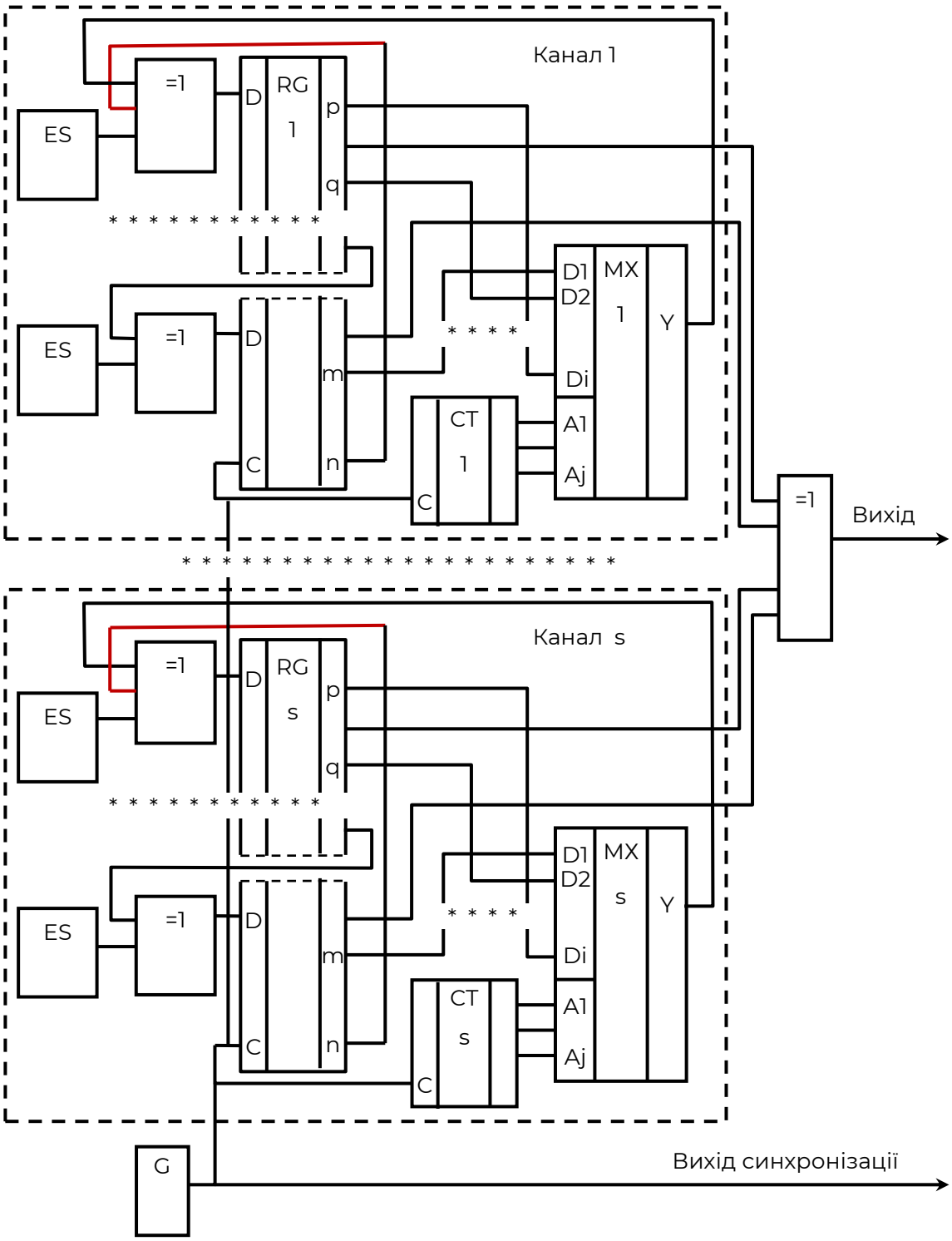

Рис. 5 **НГВП з гарячим резервуванням цифрових каналів перетворення сигналів джерел ентропії в вихідні випадкові послідовності**

Для об'єднання випадкових послідовностей різних каналів введено ще один елемент «ВИКЛЮЧНЕ АБО», на входи якого подаються сигнали з декількох проміжних виходів регістрів зсуву у кожному каналі, а вихід цього елементу XOR є виходом всього пристрою

Вихідні випадкові послідовності будуть проходити усі тести на випадковість при справності хоча б одного каналу перетворення сигналів джерел ентропії в вихідні випадкові послідовності і роботоспроможності хоча б одного джерела ентропії в цьому каналі.

Висновки

Головним методом підвищення надійності НГВП є гаряче резервування аналогових елементів джерел ентропії, які мають найменшу надійність, а також гаряче резервування усіх каналів перетворення сигналів джерел ентропії в вихідні випадкові послідовності.

Враховуючи на те, що в стандарті ISO/IEC 18031:2005 введена вимога продовження роботи недетермінованого генератора випадкових бітів (НГВБ) способом, не менш захищеним, ніж детермінований генератор випадкових бітів (ДГВБ), у разі повного збою джерела (або усіх джерел) ентропії [2], – необхідно забезпечити крипостійкість алгоритмів використовуваних ДГВП. Наприклад, використовувати замість ЛРР – Динамічні Лінійні Рекурентні Регістри.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

[1] Auguste Kerckhoffs La Cryptographie Militaire, – 1883.
[2] ISO/IEC 18031:2005. Information technology – Security techniques – Random bit generation (Інформаційні технології – Методи захисту – Генерація випадкових бітів).
[3] Методы и средства генерации случайных битовых последовательностей [Текст] : 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.
[4] Торба А., Д'яченко В., Партика С., Пушкар О. Недетерміновані генератори випадкових бітів на основі стандарту ISO/IEC 18031: 2005 / Improvement of scientific approaches to the development of engineering: collective monograph / Boston. – 2022. – p.232-241.
[5] Торба А., Мегель Ю., Науменко М. Алгоритми потокового шифрування. / Polish scince journal. ISSUE 10 (66). Warsaw. Poland. – 2023. p. 61 – 72 с.
[6] Деклараційний патент України № 36108 А, опубл. Бюл. № 3, 2001р.
[7] Деклараційний патент України № 50386 А, опубл. Бюл. № 10, 2002р.
[8] Патент України на корисну модель № 52380, опубл. Бюл. № 16, 2010р.
[9] Патент України на корисну модель № 52410, опубл. Бюл. № 16, 2010р.
[10] Патент України на винахід № 99017, опубл. Бюл. № 13, 2012р.
[11] Патент України на винахід № 96654, опубл. Бюл. № 22, 2011р.
[12] Патент України на винахід № 103097, опубл. Бюл. № 17, 2013р.
[13] Патент України на корисну модель № 153399, опубл. Бюл. № 26, 2023р.
[14] Патент України на корисну модель № 153398, опубл. Бюл. № 26, 2023р.