

М.Ю. Лосєв

*Харківський національний економічний університет ім. С. Кузнеця, Харків*

## МЕТОДИКА СИНТЕЗУ ПРИСТРОЇВ КОНТРОЛЮ І ТЕСТОВОЇ ДІАГНОСТИКИ РОЗПОДІЛЕНИХ СИСТЕМ

*В роботі розглянута методика синтезу універсальних, швидкодіючих багатоканальних пристроїв, яка реалізована на основі метода сигнатурного аналізу. Приведений приклад синтезу пристрою, який дозволяє аналізувати результати тестових реакцій в розподілених системах. Практична реалізація запропонованого підходу дозволяє створювати пристрої, в яких досягнуто суттєвого зменшення апаратних витрат та спрощення технічної реалізації сигнатурних аналізаторів, за рахунок автоматичного формування службової інформації.*

**Ключові слова:** *тестовий контроль, технічна діагностика, поліном, що не приводиться, примітивний поліном, реєстри зсуву, сигнатурний аналіз, перешкодозахищений код, інформаційних послідовність.*

### Вступ

Характерною рисою розподілених систем, яка відрізняє їх від одиничних машин, є можливість часткової відмови. Часткова відмова відбувається при збої в одному з компонентів розподіленої системи. Ця відмова може порушити нормальну роботу деяких компонентів, тоді як інші компоненти це ніяк не торкнеться [1]. На протигагу відмови в розподіленої системі така відмова завжди є глобальною, в тому сенсі, що вона чіпає всі її компоненти і легко може привести до повної втрати працездатності. Тому завдання виявлення в мережі розподілених систем помилок, не збільшуючи при цьому обсягу службової інформації, в кожній одиниці даних є актуальною.

Цієї мети можна досягти шляхом розробки універсальних програмних, апаратних або програмно-апаратних засобів контролю повідомлень і апаратурних розподілених систем. При цьому, в основі таких розробок лежать методи і алгоритми завадостійкого кодування [2]. Найбільшого поширення набули засоби контролю інформації з використанням циклічних надлишкових кодів, програмна і апаратна реалізація яких не викликає особливих труднощів [3].

Циклічний надлишковий код особливо спрощує виявлення наступних категорій помилок. Одним з таких напрямків використання циклічних кодів є сигнатурний аналіз, який успішно застосовується не тільки для контролю передачі інформації, але і для перевірки на працездатність електронного цифрового обладнання [4].

З метою підвищення швидкодії і розширення функціональних можливостей сигнатурних аналізаторів в сучасних розробках [5–8] пропонуються багатоканальні сигнатурні аналізатори. Однак поліпшення їх можливостей щодо виявлення та локалізації помилок у даних призводить до значного збільшення інформаційної або апаратною надмірності. В умовах зростаючих вимог до достовірності інформації, що передається між різноманітними

об'єктами, а також зменшення часу доставки даних є актуальною задачею розроблення простих і ефективних засобів контролю як процесу передачі інформації, так і обладнання в розподілених системах.

Тому основна **мета цього дослідження** є удосконалення методики синтезу універсальних, швидкодіючих багатоканальних пристроїв на основі методу сигнатурного аналізу, які дозволяють локалізувати помилки в інформаційних пакетах повідомлень і діагностувати обладнання

### Основний матеріал

Розглянемо принцип роботи сигнатурного аналізатора. Матриця станів сигнатурного аналізатора, може бути побудована на підставі характеристичного полінома над полем Галуа GF(2) [9]. При цьому кожний стовбець цієї матриці можна визначити відповідно виразу [1]:

$$h_i = S^i \cdot h_0, i = 0, 1, \dots, z, \quad (1)$$

де  $h_i$  –  $i$ -й стовбець матриці станів  $H$ ;  $z$  – кількість стовбців матриці станів;  $h_0 = \|10\dots0\|^T$  – нульовий стовбець матриці станів;  $S$  – супроводжуюча матриця, яка однозначно описує характеристичний поліном [3]:

$$P(x) = a_n x^n \oplus a_{n-1} x^{n-1} \oplus \dots \oplus a_1 x^1 \oplus 1, \quad (2)$$

де  $a_i \in \{0, 1\}$  – коефіцієнти характеристичного поліному. Відповідно (1) матриця станів для характеристичного поліному  $P(x) = x^4 \oplus x^3 \oplus 1$  має вигляд, який наведений в табл. 1.

Процес отримання сигнатури для вхідної послідовності  $v(t)$  можна представити з допомогою виразу:

$$\text{sig}v(t) = \sum S^i v_i h_0, i = 0, 1, \dots, z, \quad (3)$$

де  $\sum$  – сума за модулем два;  $v_i$  –  $i$ -й елемент вхідної послідовності;  $z$  – кількість елементів вхідної послідовності.

Вираз (3) можна перетворити до наступного вигляду:

$$\text{sigv}(t) = \sum h_i v_i, i = 0, 1 \dots z. \quad (4)$$

Таблиця 1

Матриця станів для характеристичного поліному  
 $P(x) = x^4 \oplus x^3 \oplus 1$

Номер рядка	Номер стовбця											
	1	2	3	4	5	6	7	8	9	10	11	12
1	1	0	0	1	1	0	1	0	1	1	1	1
2	0	1	0	0	1	1	0	1	0	1	1	1
3	0	0	1	0	0	1	1	0	1	0	1	1
4	0	0	0	1	0	0	1	1	0	1	0	1

Створення нового обладнання переслідує мету розширення функціональних можливостей, підвищення його швидкодії в процесі збору і обробки інформації або зменшення його складності (об'єму пам'яті тощо).

Розглянемо як можна зменшити складність пристроїв [1; 4–5; 10–12], який має високу швидкодію. Для визначення суми (5) у пристрої [1] необхідно зберігати матрицю станів з кількістю стовбців відповідно кількості входів сигнатурного аналізатора. При цьому необхідно використовувати запам'ятовуючий пристрій та регістри для зберігання інформації у процесі роботи пристрою [2].

У загальному випадку для пристрою, який має k входів та n ступінь утворюючого поліному необхідно зберігати k\*n розрядів. У пристрої [2] декілька зменшена кількість розрядів за рахунок того, що частка розрядів перших n-1 стовбців матриці станів сигнатурного аналізатора має заздалегідь нульові значення. Кількість розрядів N<sub>n-1</sub> для зберігання перших n-1 стовбців матриці станів можна визначити за формулою:

$$N_{n-1} = \sum_{i=0}^{n-1} i. \quad (5)$$

Для зберігання перших k стовбців матриці станів (k >= n-1) необхідно N<sub>k</sub> розрядів, які визначаються за формулою:

$$N_k = \sum_{i=0}^{n-1} i + (k - n + 1)n. \quad (6)$$

Пристрій [2] може збирати інформацію з декілька входів (але не більше k). При цьому, для кожної кількості входів пристрою [2], які використовуються в процесі збирання даних необхідно зберігати нову кодову комбінацію. Тоді, загальна кількість розрядів, які необхідні для забезпечення роботи пристрою [2], що здатен збирати дані з будь-якої кількості входів (але не більше k), обчислюється за формулою:

$$N_k = k \left( \sum_{i=0}^{n-1} i + (k - n + 1)n \right). \quad (7)$$

Пристрій [2] може функціонувати з різними поліномами. Тоді загальна кількість розрядів N<sub>p</sub>, які необхідно зберігати дорівнює:

$$N_p = pk \left( \sum_{i=0}^{n-1} i + (k - n + 1)n \right), \quad (8)$$

де p – кількість поліномів, які використовує сигнатурний аналізатор.

Припустимо, що пристрій [2] має p'ять (вісім) входів і використовує любий з двох утворюючих поліномів четвертого ступеню (P(x)=x<sup>4</sup> ⊕ x<sup>3</sup> ⊕ 1, P(x)=x<sup>4</sup> ⊕ x ⊕ 1, n=4), які забезпечують найбільший період генерації [3]. У табл. 2 приведено результати визначення кількості розрядів що необхідно зберігати для забезпечення роботи пристрою [2].

Таблиця 2

Кількість розрядів для забезпечення роботи пристрою [2]

n	p	k	Np
4	2	5	140
4	2	8	416
16	4	16	9728
16	6	16	14592

Для спрощення технічної реалізації пристрою необхідно формувати матрицю станів сигнатурного аналізатора відповідно утворюючого поліному. Для виконання цієї функції можна використати класичний генератор псевдовипадкової послідовності [10], який формує стовбці матриці станів шляхом зсуву коду 1000. Відповідно генератору псевдовипадкової послідовності побудовані пристрої [2]. У процесі формування псевдовипадкової послідовності генератор зберігає лише один стовпчик матриці станів. Якщо кількість розрядів регістра буде більше ступеню полінома n, то це дозволить зберігати більше стовбців. Наприклад, на рис.1 приведений генератор псевдовипадкової послідовності, побудований відповідно поліному P(x)=x<sup>4</sup> ⊕ x<sup>3</sup> ⊕ 1, який дозволяє зберігати вісім стовбців матриці станів.

У стовбці 1 (рис. 1) другий, третій та четвертий розряди не можуть мати друге значення крім нульового. Тому, нульові розряди першого стовпчика можна відкинути. В результаті отримаємо регістр, який містить тільки вісім розрядів і здатний зберігати вісім стовпчиків матриці станів, при цьому у старшому розряді регістра завжди буде записано 1.

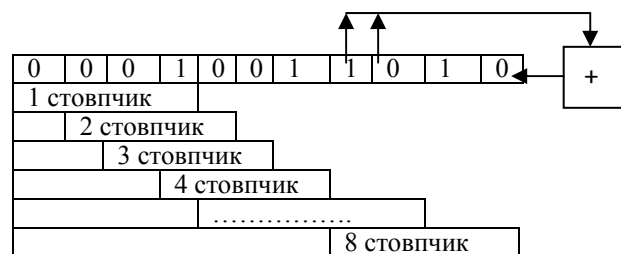


Рис. 1. Генератор псевдовипадкової послідовності побудови матриці станів аналізатора

Аналогічно створюється пристрій на підставі любого характеристичного полінома. При цьому регістр для зберігання матриці станів буде мати стільки розрядів, скільки сигнатурний аналізатор

має інформаційних входів. Хай вхідна послідовність вводиться в сигнатурний аналізатор по групах, по  $m$  розрядів в кожній. Тоді формулу (4) можна перетворити до виразу:

$$\text{sigv}(t) = \sum_{i=1}^{r-1} S^{m(i-1)} \sum_{j=0}^{m-1} S^j v_j, \quad (9)$$

де  $r$  – кількість тактів роботи приладу при перевірці вхідної послідовності по  $m$  розрядів за один такт. Для того, щоб результат відповідав виразу (9), необхідно сигнатуру першої групи розрядів помножити на матрицю  $S^{m(r-1)}$ , а результат скласти за модулем два з сигнатурою другої групи розрядів вхідної послідовності, яку необхідно помножити на матрицю  $S^{m(r-2)}$ . Такі дії повторюються доки не закінчується перевірка даних і буде введена остання група розрядів. Для виконання цих функцій у приладах [1–2] використовуються  $n$  груп по  $n$  суматорів. При цьому, до входів подається матриця  $S^m$ , яка має ступінь що відповідає кількості входів  $m$ .

Припустимо, що функціональна схема аналізатора відповідає утворюючому поліному  $P(x)=x^4 \oplus x^3 \oplus 1$  для випадку  $k=5$ . Покажемо процес отримання однакових сигнатур на одноканальному та багатоканальному аналізаторах на наступному прикладі. Припустимо сигнатурний аналізатор обробляє послідовність  $v(t) = 101011$  по три розряди (старший розряд вводиться першим), на першому такті вводиться послідовність  $v(t=1)=101$ , а на другому –  $v(t=2)=011$ . В регістрі (рис. 1) формується код 10011, відповідний першим п'яти стовбцям матриці станів сигнатурного аналізатора.

Процес отримання сигнатури для послідовності  $v(t)= 01011$  на одноканальному сигнатурному аналізаторі наведений в табл. 3.

Таблиця 3

Процес отримання сигнатури

Виходи регістра	Матриця станів регістра зсуву						Сигнатура
1	1	0	0	1	1	0	0
2	0	1	0	0	1	1	0
3	0	0	1	0	0	1	1
4	0	0	0	1	0	0	1
$v(t)$	1	1	0	1	0	1	

Таким чином, багатоканальний аналізатор сигнатур здатний достовірно обробляти інформацію, яка може передаватися по групах довжиною не більше кількості інформаційних входів пристрою та одержувати сигнатуру, яка дорівнює сигнатурі од-

ноканального аналізатора при використанні одного й того утворюючого поліному.

При цьому, пристрій що пропонується потребує тільки  $n$  розрядів вхідних даних, а для зберігання початкової інформації використовуються два додаткових регістра загальною довжиною  $n+k$  розрядів. Тоді, при використанні  $p$  поліномів, кількість розрядів, що необхідно зберігати визначається відповідно формулі:

$$N_p = p(k + n). \quad (10)$$

У табл. 4 приведено результати визначення кількості розрядів що необхідно зберігати для забезпечення роботи пристрою, який пропонується.

З табл. 2 та 4 видно, що об'єм пам'яті, який необхідний для функціонування сигнатурного аналізатора в декілька разів менше ніж у приладі [2].

Таким чином, досягнуто зменшення апаратних витрат та спрощення технічної реалізації сигнатурного аналізатора, що потребує зберігання вхідної інформації, яка забезпечує можливість використання різних характеристичних поліномів, за рахунок автоматичного формування цієї інформації у пристрої.

Таблиця 4

Кількість розрядів для забезпечення роботи нового пристрою

$n$	$p$	$k$	$N_p$
4	2	5	18
4	2	8	24
16	4	16	128
16	6	16	192

## Висновки

У проведеному дослідженні виконана формалізація процесу обробки інформації на основі сигнатурного аналізу та удосконалено методику синтезу багатоканальних пристроїв тестового контролю. Багатоканальний сигнатурний аналізатор дозволяє оперативно змінювати кількість активно працюючих входів відповідно до кількості розрядів, що вимагають обробки за один такт генератора імпульсів.

Практична реалізація запропонованого підходу дозволяє створювати пристрої, які спроможні використовувати різні поліноми при перевірці тестових послідовностей, при цьому можливе досягнути суттєвого зменшення апаратних витрат та спрощення технічної реалізації сигнатурних аналізаторів, за рахунок автоматичного формування службової інформації у пристроях.

## Список літератури

1. Информационные технологии и защита информации в информационно-коммуникационных системах: моногр. / под ред. В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2015. – 486 с.
2. Информационные системы в управлении, образовании, промышленности: моногр. / под ред. В.С. Пономаренко. – Х.: Вид-во ТОВ «Щедра садиба плюс», 2014. – 278 с.
3. Автоматизация в сетях с коммутацией пакетов: моногр. / под ред. Ю.И. Лосева. – К: Техніка, 1994. – 499 с.
4. Информационные технологии и системы в управлении, образовании, науке: моногр. / под ред. В.С. Пономаренко. – Х.: Вид-во ТОВ «Цифрова друкарня № 1», 2013. – 278 с.
5. Информационные технологии: проблемы та перспективи: моногр.: за заг. ред. В.С. Пономаренка. – Х.: Вид-во. Рожко С.Г., 2017. – 446 с.

6. Камер Дуглас Э. Сети TCP/IP, том 1. Принципы, протоколы и структура / Э. Камер Дуглас. – М.: Издательский дом "Вильямс", 2003. – 445 с.
7. Филимонов А.Ю. Протоколы Интернета / А.Ю. Филимонов. – СПб.: БХВ-Петербург, 2013. – 528 с.
8. Бернард Р. Цифровая связь. Теоретические основы и практическое применение / Р. Бернард, С. Скляр. – М.: Вильямс, 2013. – 1104 с.
9. Блейхут Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут. – М.: Мир, 1986. – 576 с.
10. Гордон Г. Локализация неисправностей в микропроцессорных системах при помощи шестнадцатеричных ключевых кодов / Г. Гордон, Х. Надич // Электроника. – 1977. – № 5. – С. 23-33.
11. Петров А.А. Компьютерная безопасность. Криптографические методы защиты информации / А.А. Петров. – М.: ДМК, 2000. – 448 с.
12. Різник В.В. Синтез оптимальних комбінаторних схем / В.В. Різник. – Львів: Вища школа, 1989. – 165 с.

## References

1. Ponomarenko, V.S. (2015), "Ynformatsyonnyy tekhnolohyy y zashchyta ynformatsyy v ynformatsyonno-kommunikatsyonnykh systemakh: monohrafiia" [Information technologies and information protection in information and communication systems], Shchedra sadyba, Kharkiv, 486 p.
2. Ponomarenko, V.S. (2014), "Ynformatsyonnyy systemy v upravlenyy, obrazovany, promyshlennosty: monohrafiia" [Information systems in management, education, industry], Shchedra sadyba plius, Kharkiv, 278 p.
3. Losev, Yu.I (1994), "Avtomatyzatsiya v setiakh s kommutatsyei paketov: monohrafiia" [Automation in networks with packet switching], Tekhnika, Kyiv, 499 p.
4. Ponomarenko, V.S. (2013), "Ynformatsyonnyy tekhnolohyy y systemy v upravlenyy, obrazovany, nauke: monohrafiia" [Information technologies and systems in management, education, science], Tsyfrova drukarnia No. 1, Kharkiv, 278 p.
5. Ponomarenko, V.S. (2017), "Informatsiini tekhnolohii: problemy ta perspektyvy: monohrafiia" [Information technologies: problems and prospects], Rozhko S.H., Kharkiv, 446 p.
6. Chamber Douglas, E. (2003), "Sety TCP/IP, tom 1. Prynitsypy, protokoly y struktura" [TCP / IP networks, volume 1. Principles, protocols and structure], Yzdatelskiy dom "Vyliams", Moscow, 445 p.
7. Filimonov, A.Yu. (2013), "Protokoly Ynterneta" [Internet protocols], SPb.: BKhV-Peterburh, St. Petersburg, 528 p.
8. Bernard, R. and Skliar, S. (2013), "Tsyfrovaia sviaz. Teoretycheskiye osnovy y praktycheskoe pryumenenye" [Digital communication. Theoretical bases and practical application], Vyliams, Moscow, 1104 p.
9. Bleikhut, R. (1986), "Teoriya y praktyka kodov, kontrolyruuiushchykh oshybyky" [Theory and practice of codes that control errors], Mir, Moscow, 576 p.
10. Gordon, G. and Nadic, H. (1977), "Lokalyzatsiya nespravnoitei v mykroprotsessornykh systemakh pry pomoshchy shestnadsatyrichnykh kliuchevykh kodov" [Localization of irregularities in microprocessor systems using hexadecimal key codes], *Electronics*, No. 2(27), pp. 75-78.
11. Petrov, A.A. (2000), "Computernaya bezopasnost. Criptograficheskie metody zashity informacyy" [Computer security. Cryptographic methods of information protection], DМК, Moscow, 448 p.
12. Riznyk, V.V. (1989), "Syntez optymalnykh kombinatorynykh skhem" [Synthesis of optimal combinatorial circuits], Vyshya shkola, Lviv, 165 p.

Надійшла до редколегії 23.03.2018

Схвалена до друку 15.05.2018

### Відомості про автора:

#### Лосев Михайло Юрійович

кандидат технічних наук доцент  
доцент кафедри Харківського національного  
економічного університету ім. С. Кузнеця,  
Харків, Україна  
orcid.org/0000-0002-2393-3490

### Information about the author:

#### Mihailo Losev

Candidate of Technical Sciences Associate Professor  
Senior Lecturer of Department of Simon Kuznets  
Kharkiv National University of Economics,  
Kharkiv, Ukraine  
orcid.org/0000-0002-2393-3490

## МЕТОДИКА СИНТЕЗА УСТРОЙСТВ КОНТРОЛЯ И ТЕСТОВОЙ ДИАГНОСТИКИ РАСПРЕДЕЛЕННЫХ СИСТЕМ

М.Ю. Лосев

Рассмотрена методика синтеза универсальных, быстродействующих многоканальных устройств, реализованная на основе метода сигнатурного анализа. Приведен пример синтеза устройства, которое позволяет анализировать результаты тестовых реакций в распределенных системах. Практическая реализация предлагаемого подхода позволяет создавать устройства, в которых достигнуто существенное уменьшение аппаратных затрат и упрощение технической реализации сигнатурных анализаторов, за счет автоматического формирования служебной информации.

**Ключевые слова:** тестовый контроль, техническая диагностика, неприводимые и примитивные полиномы, регистры сдвига, сигнатурный анализ, помехозащищенный код, информационная последовательность.

## THE METHOD OF SYNTHESIS OF CONTROL DEVICES AND TEST DIAGNOSTICS OF DISTRIBUTED SYSTEMS

M. Losev

The formalization of the process of information processing on the basis of signature analysis was completed and the method of synthesis of multichannel devices of test control was improved in the conducted research. In this case, the algorithm of data processing in the multichannel signature analyzer is proposed, and its architecture, which is aimed at verifying the objects of distributed systems. Architecture of the signature analyzer allows you to control the data by groups is considered in the work. At the same time reception of the information sequence can be carried out in one cycle of the clock generator, if it allows the bit of the analyzer. In that case, if the bit size of the analyzer is less than the length of the group of discharges, then its processing can be carried out over several cycles of the clock generator. Multichannel signature analyzer allows you to quickly change the number of active inputs in accordance with the number of discharges that require processing in one cycle pulse generator. The practical implementation of the proposed approach allows you to create devices that are able to use different polynomials when testing the test sequences. It is possible to achieve a significant reduction of hardware costs and simplify the technical implementation of signature analyzers, due to the automatic generation of service information in devices.

**Keywords:** test control, technical diagnostics, irreducible and primitive polynomials, shift registers, signature analysis, interference-protected code, information sequence.