УДК 681.326

# ПОШИРЕННЯ МАТЕМАТИЧНОГО АПАРАТУ СИГНАТУРНОЇ АЛГЕБРИ ДЛЯ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ

В.М. Тупкало[1], О.Л. Харитонов[2], Г.А. Кучук[3]
([1]Інститут управління якістю Держспоживстандарту України, Київ;
[2]Командування Повітряних Сил ЗС України, Вінниця;
[3]Харківський університет Повітряних Сил ім. І. Кожедуба)

*Розроблений математичний апарат сигнатурної алгебри, що дозволяє зводити рішення задачі синтезу до простої процедури композиції функціонально закінчених елементарних комбінаційних вузлів з кінцевого універсального набору з метою функціонального розширення методів боротьби з хакерськими атаками.*

***сигнатурна алгебра, комп'ютерна мережа, хакерська атака***

**Вступ.** На сьогодні серед задач, пов'язаних із управлінням та захистом комп'ютерних мереж (КМ), однією із найбільш актуальних є задача виявлення хакерських атак та відмов у роботі мережевого обладнання та програмного забезпечення [1]. Для вирішення цих задач пропонуються різні методи: сигнатурний аналіз, статистичні методи аналізу, такі як аналіз Фур'є, регресійний аналіз, аналіз сингулярного спектру, а також аналіз, що проводиться на основі нейронних мереж, експертних систем тощо [2, 3]. Однак, лише сигнатурні методи знайшли поки реальне втілення у відповідних системах, завдяки простоті реалізації, причому звичайно використовується відомий математичний апарат синтезу структурної надмірності, заснований на автоматній моделі представлення об'єктів контролю (ОК) [4]. Необхідність в пошуку нового математичного апарату, в першу чергу, пов'язана з питанням вибору рівня формалізації моделі ОК сучасних КМ. З одного боку, рівень повинен бути вибраний найближчим до базисного елементного рівня; з іншого боку, слід забезпечити єдність формалізованого представлення ієрархічних моделей контролю КМ з урахуванням вибраного виду відображення множини реакцій ОК на множину їх контрольних ознак. Правомірність такої вимоги виходить з тенденції розвитку сучасних КМ на принципах глибокої уніфікації, стандартизації структур сигналів і інтерфейсів [5]. Тому стає ***актуальною*** формалізація процесу синтезу надмірності в умовах безперервного зростання складності і ступеня інтеграції сучасних КМ. Одним з напрямів розвитку є уявлення і обробка контрольної інформації у вигляді сигнатур.

В даний час існує ряд робіт, присвячених цьому питанню [6 – 7], але вони вимагають подальшого розвитку і теоретичного узагальнення з метою формування загальної методології сигнатурного контролю у КМ різного призначення, що є ***метою даної статі***.

**1. Завдання вибору аналітичної моделі.** Блок-схема функціонального контролю ФК при використанні входів $X$ і виходів $Y$ об'єкту контролю надана на рис. 1 (ОК – цифровий автомат з передавальною функцією $\psi$; умовний контрольний пристрій (УКП) є комбінаційним і здійснює сюр'єктивне відображення $\psi_k : X \to Y_k$ вхідних двійкових векторів $X$ і вихідних двійкових векторів $Y_k$ таким чином, щоб забезпечувалася задана достовірність контролю; вирішальний орган (ВО) проводить відображення $\psi_{BO} : Y \times Y_k \to \varepsilon = \{0,1\}$ шляхом ідентифікації кожного вектора виходу ОК $y_i \in Y$ з векторами $y_{k_i} \in Y_k$; оператор $S$ необхідний для кодування векторів довжини $n$ у відповідні їм вектори довжини $m\,(n > m)$ ).

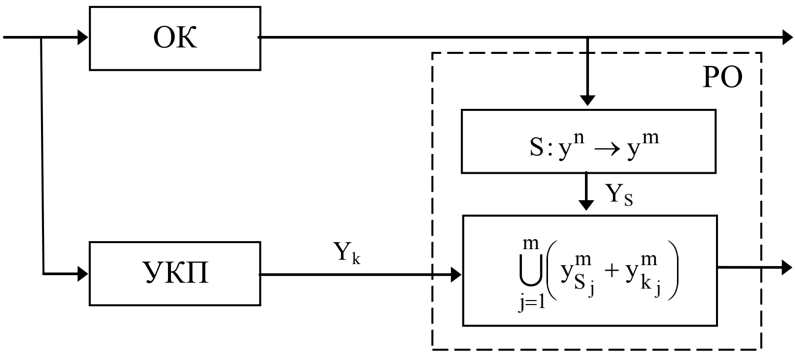


Рис. 1. Блок-схема функціонального контролю

Залежність між функціями $\psi(X)$ і $\psi_k(X)$ визначимо у вигляді

$$\psi_k = S(\psi(X)) = S(\psi_1 * \psi_2 * \ldots * \psi_q) = S\psi_1 * S\psi_2 * \ldots * S\psi_q\,, \tag{1}$$

де $\psi_j$ і «*» – відповідно булева функція $j$-го елементарного контрольного вузла з шуканого кінцевого (стандартного) набору і булева операція суперпозиції (комутації).

При цьому рівень абстракції ОК (опис функції $\psi(X)$ ) обмежимо детермінованими арифметичними функціями, оскільки єдиною (універсальною) основою всіх арифметичних і логічних операцій КМ є елементарна операція арифметичного складання [8]. Зокрема, приклади даного уявлення для булевих операцій розглянуті в роботі [5].

Тоді завдання вибору аналітичної моделі ОК з урахуванням прийнятих початкових посилок сформулюємо наступним чином.

Нехай задано ОК з доступними для контролю його входами і виходами. Знайти для цього ОК опис його УКП у вигляді (1) такий, щоб детермінована арифметична функція $\psi(X)$ була представлена еквівалентною булевою функцією

$$\left(\psi_1 * \psi_2 * \ldots * \psi_q\right).$$

**2. Основний результат.** Оскільки (1) припускає незалежність вибору оператора $S$ від функції $\psi(X)$, то основою синтезу УКП служить таке твердження.

***Твердження 1.*** Детермінованій арифметичній функції $\psi(X)$ може бути поставлено у відповідність S-перетворення її булевого еквівалента в інфіксному вигляді (1), якщо кожна з функцій $\psi_j$ унітарна або бінарна, оператор $S$ є лінійним, а операція * – складання по модулю два.

*Доказ.* Оскільки умовою виконання рівності (1) є незалежність вибору оператора $S$ від функції $\psi$, то існування для детермінованої арифметичної функції булевого еквівалента у принципі не виключає його інфіксного уявлення

$$\psi = \left(\psi_1 * \psi_2 * \ldots * \psi_q\right). \qquad (2)$$

У свою чергу, оскільки розглядається безперервний в часі (безперервний по тактах роботи цифрової системи) контроль, то з рішення 13-й проблеми Гильберта відомо, що всяка безперервна функція $N$ змінних представима у вигляді суперпозиції безперервних функцій двох змінних [9]. Тоді принцип суперпозиції $S\left(\psi_1 * \psi_2 * \ldots * \psi_q\right) = S\psi_1 * S\psi_2 * \ldots * S\psi_q$ реалізується, якщо має місце лінійне S-перетворення лінійної булевої функції. Лінійність булевого еквівалента (2) можлива тільки у тому випадку, коли всі функції $\psi_j$ є функціями однієї і(або) двох змінних за умови уявлення $\psi_j$ та * сумою по модулю два або еквівалентністю [10].

Припустимо, що $S$ несюр'єктивне відображення. Тоді повинен бути хоч би один такий вектор $y_i^k \in Y_k$ на вході УКП, що для всіх $y_i$ $S(y_i) \neq y_i^k$. Проте перехід безпомилково працюючого КО в працездатний стан з таким $y_i^k$ суперечить суті організації ФК і тому $S: Y \rightarrow S(\leftarrow Y)$ є сюр'єктивне відображення, що і було потрібно довести.

З урахуванням твердження 1 булевий еквівалент арифметичної функції складання має вигляд

$$A+B=(A\oplus B)\oplus H(A\oplus B)=A\oplus B\oplus H(A+B), \tag{3}$$

де $H(A+B)$ – число, код якого характеризує перехід одиниць перенесення при складанні чисел A і B. Оскільки $H(A+B)$ встановлює взаємний зв'язок між A і B, то $H(A+B)$ визначимо як взаємну характеристику двох чисел, вступаючих в операцію арифметичного складання.

Аналогічно використання суперпозиції по модулю два контрольних характеристик у відомому методі тестового контролю – сигнатурному аналізі, як оператора S вибираємо векторну інтеграцію $(\mathrm{sig})$ оператора утворення сигнатур двійкової послідовності довжини $n$. У [11] показано, що при загальному виді створюючого (що породжує) полінома

$$P(x)=\delta_m x^m+\delta_{m-1}x^{m-1}+\ldots+\delta_1 x+1$$

синтез формувача сигнатур двійкових векторів $A=a_n a_{n-1}..a_1$ (вага розрядів зростає справа наліво) зводиться до тривіального синтезу комбінаційної схеми згортки по модулю два $(\mathrm{sig}\,A=g_m g_{m-1}..g_1)$ на основі алгоритму зрушення регістра із зворотними зв'язками:

$$\begin{cases} g_{1(j)}=\sum\limits_{i=1}^{m}\delta_i g_{i(j-1)}\oplus a_j, & j=\overline{1,n}; \\ g_{r(j)}=g_{r-1(j-1)}, & r=\overline{2,m}. \end{cases} \tag{4}$$

Покажемо, що щодо множини $R$ аналітичних модулів ОК у вигляді детермінованих арифметичних функцій існує кінцева множина $W$ операцій інфіксного уявлення (1). З цією метою необхідно довести, що для всіх чотирьох елементарних арифметичних функцій умова сформульованої теореми виконується.

Враховуючи (3), для функції складання

$$\mathrm{sig}\,(A+B)=\mathrm{sig}\,(A\oplus B)\oplus \mathrm{sig}\,H(A\oplus B)=\mathrm{sig}\,A\oplus \mathrm{sig}\,B\oplus \mathrm{sig}\,H(A+B) \tag{5}$$

і, отже, $\mathrm{sig},\oplus,H(\ldots)\in W$.

***Визначення 1.*** $\breve{H}(A+B)$ – є усічена зліва (відкинутий старший розряд) взаємна характеристика $H(A+B)$.

Функція віднімання $F^{(-)}=A-B=A+(-B)$. В результаті перетворення n-розрядного прямого коду негативного числа $(-B)$ в його додатковий код $(-B)_{\text{дод}}$ одержуємо

$$\left(-B\right)_{дод} = B \oplus d_{[n]} \oplus f_{[n]} \oplus \breve{H}\left[\left(B \oplus d_{[n]}\right) + f_{[n]}\right];$$

$$\begin{gathered} sig\left(A - B\right) = sig\,A \oplus sig\,b \oplus sig\left(d_{[n]} \oplus f_{[n]}\right) \oplus sig\breve{H}\left[\left(B \oplus d_{[n]}\right) + f_{[n]}\right] \oplus \\ \oplus\, sig\,\breve{H}\left\{A + \left[B \oplus d_{[n]} \oplus f_{[n]} \oplus \breve{H}\left[\left(B \oplus d_{[n]}\right) + f_{[n]}\right]\right]\right\}, \end{gathered} \tag{6}$$

де $d_{[n]}, f_{[n]}$ – n-розрядні числа (константи) відповідно з одиницями у всіх та тільки в молодших розрядах.

Із зіставлення (5) і (6) слідує $\breve{H}(\ldots), d, f \in W$.

Функція множення $F^{(\times)} = A \times B$. З урахуванням староєгіпетського способу множення [8] і представлення вагів розрядів множника:

$$B(x) = b_n x^n + b_{n-1} x^{n-1} + \ldots + b_2 x^2 + b_1 x;$$

$$A \times B = A \sum_{i=1}^{n} b_i 2^{i-1}.$$

Тоді на підставі (3) для випадку позитивних співмножників

$$\begin{gathered} sig\left(A \times B\right) = b_1 sig\,A \oplus b_2 sig\,H\left(A + A\right) \oplus b_{n-1} sig\,A\,2^{n-2} \oplus \\ \oplus\, b_n sig\,A\,2^{n-1} \oplus b_1 b_2 sig\,H\left[A + H\left(A + A\right)\right] \oplus \ldots \oplus b_{n-1} sig\,H\left[\left(Ab_1 \oplus\right.\right. \\ \left.\left. \oplus\, b_2 H\left(A + A\right) \oplus b_1 b_2 H\left[A + H\left(A + A\right)\right] \oplus \ldots\right) + A\,2^{n-2}\right] \oplus \\ \oplus\, b_n sig\,H\left\{Ab_1 \oplus b_2 H\left(A + A\right) \oplus \ldots \oplus Ab_{n-1} 2^{n-2} \oplus Ab_n 2^{n-1} \oplus\right. \\ \oplus\, b_1 b_2 H\left[A + H\left(A + A\right)\right] \oplus \ldots \oplus b_{n-1} H\left[\left(Ab_1 \oplus b_2 H\left(A + A\right) \oplus\right.\right. \\ \left.\left.\left. \oplus\, b_1 b_2 H\left[A + H\left(A + A\right)\right] \oplus \ldots\right) + A\,2^{n-2}\right]\right] + A 2^{n-1}\right\}. \end{gathered} \tag{7}$$

Випадки різних знакових розрядів співмножників розглянуті у [6]. При цьому загальне представлення результатів множення як суперпозиції по модулю два має вигляд

$$F^{(\times)} = \left(|A| \times |B|\right) + k_{[2n+1]} = \left(|A| \times |B|\right) \oplus k_{[2n+1]} \oplus H\left[\left(|A| \times |B|\right) + k_{[2n+1]}\right],$$

де $k_{[2n-1]}$ – (2n+1)-розрядне число (константа з одиницею тільки в старшому розряді) представлення знакового розряду за умови його розташування зліва від старшого розряду мантиси.

Із зіставлення (5), (6) з (7) витікає, що $k \in W$.

Функція ділення $F^{(:)} = A / B$. Подібно до множення, ділення двійкових чисел може бути виконано у вигляді чергування простих операцій віднімання і зрушення [8]. Щодо операції зрушення інтерес представляє випадок співвідношення

$$B = 2^{-r} A \quad \left(r = 1, 2, \ldots\right).$$

***Визначення 2.*** Якщо число A описується приведеним поліномом

$A(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, то відповідне йому транспоноване число $A^T$ описується поліномом

$$A^T(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n,$$

де T – операція транспонування кодів двійкових чисел (логічна операція).

З урахуванням даного визначення

$$2^{-1} A = A - B = B = \left[\breve{H}\left(A^T + A^T\right)\right] = \breve{H}^T\left(A^T + A^T\right). \tag{9}$$

Тоді

$$\operatorname{sig} B = \operatorname{sig}\left(2^{-1} 2^{-(r-1)} A\right) = \operatorname{sig}\left(2^{-(r-1)} \breve{H}^T\left(A^T + A^T\right)\right). \tag{10}$$

Із зіставлення (5) – (8) з (9) витікає, що $T \in W$.

Таким чином, $W = \left(\operatorname{sig}, \oplus, H, \breve{H}, T, f, d, k\right)$ – є множина операцій інфіксного представлення виду (1) множини R і згідно відомому визначенню [10] система $(R; W)$ – є алгебра (R – основна множина, W – сигнатура алгебри) з двома бінарними логічними операціями: $\oplus, H$; трьома унарними логічними операціями: $\breve{H}, T, \operatorname{sig}$; константами: $f, d, k$. Алгебру $(R; W)$ назвемо сигнатурною алгеброю.

***Твердження 2.*** Сигнатурна алгебра $(R; W)$ є лінійною комутативною.

*Доказ.* Відносно (1) відображення

$$\operatorname{sig}\left(\psi_1 * \psi_2 * \ldots * \psi_q\right) \to \operatorname{sig}(Y)$$

лінійно, оскільки воно зберігає лінійну структуру в наступному сенсі [12]:

1) є адитивним, тобто з (1) слідує

$$\operatorname{sig}\left(\psi_1 \oplus \psi_2 \oplus \ldots \oplus \psi_q\right) = \operatorname{sig} \psi_1 \oplus \operatorname{sig} \psi_2 \oplus \ldots \oplus \operatorname{sig} \psi_q;$$

2) є однорідним першого ступеня, тобто $\operatorname{sig}\left(\psi_j\right) = \operatorname{sig} \psi_j$, де $\chi = \{0, 1\}$ – скаляр поля $GF(2)$, а $\psi_j$ – будь-який n-розрядний вектор з розширення $GF(2^n)$.

Відомо [12], що алгебра називається комутативною, якщо основна множина R наділена комутативним законом композиції. З твердження 1 витікає, що у разі булевого інфіксного уявлення (1) таким законом є сума по модулю два.

**3. Приклад і аналіз результату.** Оскільки операції з множини W є логічними, то проведемо порівняльну оцінку синтезу УКП в базисах сигнатурної алгебри $(R; W)$ і відомої булевої алгебри. Розглянемо приклад: необхідно здійснити контроль зрушуючого регістра управо (у бік молодших розрядів) з циклічним перенесенням з молодшого розряду в старший за умови, що початковий вміст регістра може бути будь-яким, кількість розрядів $n = 9$.

На основі апарату булевої алгебри відомий метод контролю цифрових автоматів шляхом прогнозу парності одиниць в коді результату [13]. Можливості методу істотно обмежені, оскільки вузол контролю, що реалізовує функцію парності, є ініциальним автоматом і, отже, для початку і відновлення процесу контролю обов'язково потрібна установка його початкового стану. Крім того, достовірність контролю за даним методом у принципі не може перевищувати величину $D = 0{,}5$ (реалізується кодовий контроль по модулю два). У разі пропонованого підходу до рішення задачі ФК при даному виді зрушення (i+1)-й результат $A_{i+1}$ визначається арифметичною сумою

$$A_{i+1} = 2^{-1}\left(A_i - a_1 f_{[n]}\right) + a_1 k\,.$$

З урахуванням (9) інфіксним представленням булевого еквівалента даної суми є

$$A_{i+1} = \breve{H}^T\left(A^T{}_i + A^T{}_i\right) \oplus a_1 k_{[n]}\,.$$

Відповідно до (1) правило сигнатурного контролю n-розрядного регістра зрушення з циклічним перенесенням з молодшого розряду в старший має вигляд

$$\begin{aligned} \operatorname{sig} A_{i+1} &= \operatorname{sig}\left[\breve{H}^T\left(A^T + A^T\right) \oplus a_1 k_{[n]}\right] = \\ &= \operatorname{sig} \breve{H}^T\left(A^T + A^T\right) \oplus a_1 \operatorname{sig} k_{[n]} \end{aligned} \tag{11}$$

і дозволяє організувати контроль шляхом прогнозу сигнатури кожного подальшого результату зрушення.

Хай в якості створюючим вибраний поліном $P(x) = x^4 + x^3 + 1$.

Тоді, використовуючи алгоритм синтезу (4) і логічне представлення коду $\breve{H}^T\left(A^T + A^T\right) = 0, a_n a_{n-1} .. a_3 a_2$, безпосередньо з формули правила (10) виходить, що УКП повинне реалізувати систему булевих функцій $\left(Y_k = y_{k4} y_{k3} y_{k2} y_{k1}\right)$ :

$$y_{k4} = a_9 \oplus a_8 \oplus a_5; \qquad y_{k2} = a_9 \oplus a_7 \oplus a_6 \oplus a_3;$$
$$y_{k3} = a_8 \oplus a_7 \oplus a_4 \oplus a_1; \qquad y_{k1} = a_8 \oplus a_6 \oplus a_5 \oplus a_1 \oplus a_1,$$

яка щодо вибраного полінома $P(X)$ за кількістю необхідних бінарних операцій є мінімальною.

У контексті правила (11) УКП може бути реалізовано і за допомогою відомого прямого методу синтезу комбінаційних систем на основі представлення булевих функцій у вигляді довершеної диз'юнктивної нормальної форми (ДДНФ) [14]. Проте опис функцій $y_{kj}$ в ДДНФ вимагає знання початкового стану регістра $A_0$ для попереднього складання таблиці істинності. Порушимо умову прикладу і встановимо $A_0 = 110100100$. Тоді при $P(x) = x^4 + x^3 + 1$:

$$
\begin{aligned}
y_{k4} &= a_9\bar{a}_8\bar{a}_7a_6\bar{a}_5\bar{a}_4a_3a_2\bar{a}_1 \vee a_9\bar{a}_8a_7\bar{a}_6\bar{a}_5a_4\bar{a}_3\bar{a}_2a_1;\\
y_{k3} &= a_9a_8\bar{a}_7a_6\bar{a}_5\bar{a}_4a_3\bar{a}_2\bar{a}_1 \vee \bar{a}_9\bar{a}_8a_7a_6\bar{a}_5a_4\bar{a}_3\bar{a}_2a_1 \vee\\
&\vee \bar{a}_9\bar{a}_8a_7\bar{a}_6\bar{a}_5a_4a_3\bar{a}_2a_1 \vee a_9\bar{a}_8a_7\bar{a}_6\bar{a}_5a_4\bar{a}_3\bar{a}_2a_1;\\
y_{k2} &= a_9a_8\bar{a}_7a_6\bar{a}_5\bar{a}_4a_3\bar{a}_2\bar{a}_1 \vee \bar{a}_9a_8a_7\bar{a}_6a_5\bar{a}_4\bar{a}_3a_2\bar{a}_1 \vee\\
&\vee a_9\bar{a}_8\bar{a}_7a_6a_5\bar{a}_4a_3\bar{a}_2a_1 \vee a_9\bar{a}_8\bar{a}_7a_6\bar{a}_5\bar{a}_4a_3a_2\bar{a}_1;\\
y_{k1} &= \bar{a}_9a_8a_7\bar{a}_6a_5\bar{a}_4\bar{a}_3a_2\bar{a}_1 \vee \bar{a}_9a_8\bar{a}_7\bar{a}_6a_5a_4\bar{a}_3a_2\bar{a}_1 \vee\\
&\vee \bar{a}_9\bar{a}_8a_7\bar{a}_6\bar{a}_5a_4a_3\bar{a}_2a_1 \vee a_9\bar{a}_8a_7\bar{a}_6\bar{a}_5a_4\bar{a}_3\bar{a}_2a_1.
\end{aligned}
$$

Легко відмітити, що зменшити складність реалізації одержаних функцій шляхом використання операції склеювання термів ДДНФ не вдається, тобто ДДНФ відразу є тупиковою ДНФ [14]. Кількість елементарних кон'юнкцій може бути зменшена трохи, якщо при переборі варіантів представлення функцій $y_{kj}$ використовувати сполучну і розподільну властивості кон'юнкції і диз'юнкції.

Відомі переборні методи мінімізації логічних функцій, які використовують довизначення таблиці істинності забороненими наборами. Проте їх застосування з метою отримання мінімальної ДНФ вимагає оцінку числа $(\tau(n))$ можливих тупикових ДНФ, рівного [14]:

$$5^{2^{n-4}} \le \tau(n) < \left( \frac{2^{n+0,5}}{\sqrt{\pi n}} \right)^{2^n},$$

тобто вже при $n = 9$ процес знаходження мінімальної ДНФ малоефективний. При цьому слід вказати, що кожному початковому стану $A_0$ утворення циклічного коду повинна бути синтезована своя логічна структура УКП (різні таблиці істинності).

**Висновки.** Отже, перевагою синтезованої сигнатурної алгебри $(R; W)$ є можливість переходу від формул алгебри до реалізації їх УКП безпосередньо без застосування додаткових інтерпретуючих і мінімізуючих процедур шляхом простої логічної композиції (комутації) функціонально закінчених елементарних структур з кінцевої множини (стандартного набору). Це дасть змогу розширити використання сигнатурного аналізу для виявлення хакерських атак та відмов у роботі мережевого обладнання та програмного забезпечення. ***Метою подальших досліджень*** є розробка практичних рекомендацій до застосування наведеного апарату при виявленні хакерських атак

## ЛІТЕРАТУРА


1. *Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999. – 328 с.*
2. *Домарев В.В. Безопасность информационных технологий. – К.: Диасофт, 2002. – 688 с.*
3. *Pinus A., Zhurkov S, The scales of computability potentials //F&P Mathematics. – 2003. – Vol. 9, no. 3. – P. 145-164.*
4. *Щербаков Н.С., Подкопаев Б.П. структурная теория аппаратного контроля цифровых автоматов. – М.: Машиностроение, 1982. – 191 с.*
5. *Гуляев В.А., Чаплыга В.Н., Кедровский И.В. Методы и средства обработки диагностической информации в реальном времени. – К.: Наукова думка, 1986. – 224 с.*
6. *Тупкало В.Н. Сигнатурный контроль выполнения регистровых операций // Электронное моделирование. – 1992. – № 1. – С. 64-67.*
7. *Тупкало В.Н. Обеспечение контролепригодности хода программ по критерию минимальной периодичности контроля // Кибернетика и системный анализ. – 1993. – № 1. – С. 34-37.*
8. *Прикладная теория цифровых автоматов / К.Г. Самофалов и др. – К.: Вища школа, 1987. – 375 с.*
9. *Проблемы Гильберта / Под ред. П.С. Александрова. – М.: Наука, 1969. – 56 с.*
10. *Кузнецов А.П., Адельсон-Вельский Г.М. Дискретная математика для инженера. – М.: Энергия, 1980. – 344 с.*
11. *Тупкало В.Н. Сигнатуры как элементы конечного поля в задачах технической диагностики // Автоматизированные системы управления и приборы автоматики. – 1990. – Вып. 93. – С. 30-35.*
12. *Функциональный анализ / Под ред. С.Г. Крейна. – М.: Наука, 1972. – 544 с.*
13. *Селлерс Ф. Методы обнаружения ошибок в работе ЭЦВМ. – М.: Мир, 1972. – 312 с.*
14. *Поспелов Д.А. Логические методы анализа и синтеза схем. – М.: Энергия, 1974. – 368 с.*



*Надійшла 20.03.2006*


**Рецензент:** доктор технічних наук, професор С.В. Козелков,
Національна академія оборони України, Київ.