УДК 681.3

А.Мельник[1], докт. техн. наук; Т.Коркішко[2]
[1] *Національний університет "Львівська політехніка"*
[2] *Тернопільська академія народного господарства*

МЕТОДИКА ПРОЕКТУВАННЯ БАГАТОКАНАЛЬНИХ ПРОЦЕСОРІВ СИМЕТРИЧНОГО БЛОКОВОГО ШИФРУВАННЯ

Запропоновано методику проектування багатоканального процесора перетворень симетричного блокового шифрування, структуру багатоканального процесора, до складу якої входять структурно та функціонально спеціалізовані на обслуговування заданих вхідних каналів даних обчислювальні елементи. Формалізація опису кожного етапу проектування створює передумови для побудови засобів автоматизованого проектування багатоканальних процесорів перетворень симетричного блокового шифрування.

Вступ

Сучасні завдання захисту інформації вимагають постійного збільшення продуктивності комп'ютерних засобів для виконання алгоритмів перетворень симетричного блокового шифрування (СБШ), особливо при багатоканальній обробці інтенсивних потоків даних у реальному масштабі часу [1, 2]. Для виконання таких алгоритмів наявні системи захисту інформації використовують універсальні програмовані [3, 4] чи апаратно-орієнтовані процесори [5 – 7], що забезпечують одночасну обробку даних лише з одного каналу, що часто не задовольняє вимог з продуктивності або вимагає використання множини процесорів за числом каналів даних. Попередні дослідження [8] показали, що для побудови багатоканальних систем захисту інформації з мінімальними затратами обладнання доцільно використовувати апаратно-орієнтовані процесори, структура яких орієнтована на одночасну паралельну обробку даних з декількох каналів. У [9] були запропоновані базові структури багатоканальних апаратно-орієнтованих операційних пристроїв, серед яких виділені багато- та однофункціональні.

У рамках продовження робіт на створення багатоканальних процесорів СБШ з мінімальними затратами обладнання пропонується методика їх проектування. Як вихідні дані для проектування використовуються і характеристики каналів даних – їх кількість, частоти надходження даних, режими обробки даних, і параметри базових операційних пристроїв багатоканальних процесорів – час прийому даних, час зміни ключа шифрування, кількість одночасно обслуговуваних каналів, затрати обладнання на побудову операційного пристрою.

1. Архітектура багатоканального процесора СБШ

Багатоканальний процесор СБШ призначений для обробки інтенсивних паралельних потоків даних, що надходять з каналів, які характеризуються множиною:

$$F = \{F_i \mid F_i = [t^{+}_{Bxi}, t^{-}_{Bxi}, t_{Ki}, O_i, M_i]\},$$

де t^{+}_{Bxi} – мінімальний час надходження вхідних даних з i-го каналу для режимів із зворотнім зв'язком, t^{-}_{Bxi} – мінімальний час надходження вхідних даних з i-го каналу для режимів без зворотнього зв'язку, t_{Ki} – мінімальний час зміни ключа шифрування i-го каналу для режимів із зворотнім зв'язком, O_i – виконувана операція над даними i-го каналу, $O_i \in O$, $O = \{E, D\}$, де E – позначення операції зашифрування, D – позначення операції розшифрування, M_i – режим обробки даних i-го каналу, $M_i \in M$, $M = \{ECB, CBC, CFB, OFB\}$, де ECB, CBC, CFB, OFB – відповідно режими обробки даних у режимі простої заміни, зчеплення блоків зашифрованого тексту, зворотнього зв'язку за зашифрованим текстом та зворотнього зв'язку за виходом, i=1,…,H, H=|F| [8].

З метою забезпечення обслуговуваної множини каналів даних у реальному масштабі часу запропонована архітектура багатоканального процесора СБШ [9], що складається з вхідного комутатора каналів (ВхК), багатоканального операційного пристрою та вихідного комутатора каналів (ВихК) (рис. 1а). ВхК подає блоки даних з H вхідних каналів $C_{Вх1}$ – $C_{ВхН}$ у багатоканальний операційний пристрій, що складається з P операційних елементів ОЕ1 – ОЕP. Оброблені дані з виходів ОЕ розподіляються вихідним комутатором між вихідними каналами $C_{Вих1}$ – $C_{ВихН}$.

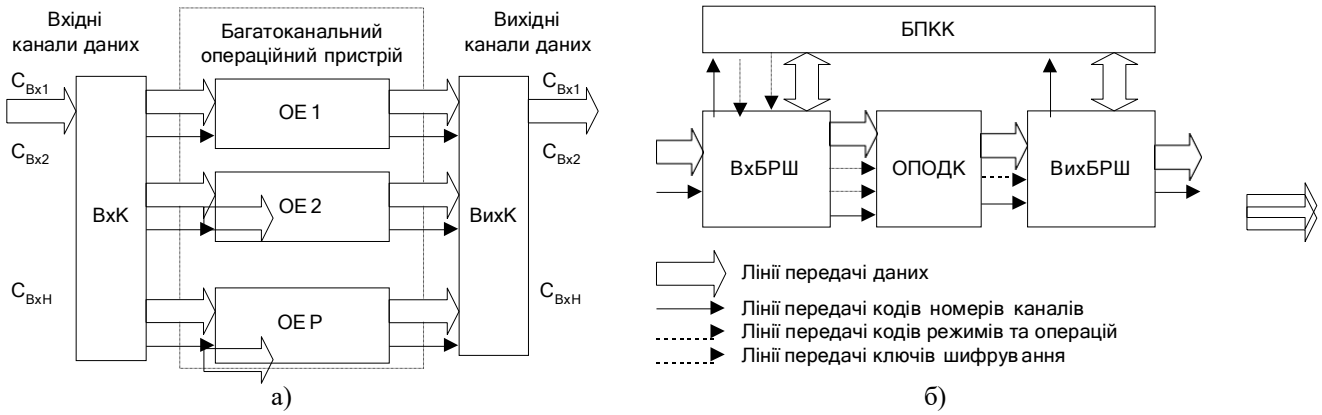

Рис. 1. Багатоканальний процесор СБШ: а) структура процесора, б) структура ОЕ.

ОЕ (рис. 1б) обробляє вхідні блоки згідно з алгоритмомо СБШ, який апаратно відображений в операційному пристрої обробки даних та ключа (ОПОДК). Структури ОПОДК орієнтовані на багатоканальну обробку даних. Блок пам'яті контекстів каналів (БПКК) містить інформацію про параметри каналів даних – коди режимів шифрування, коди операції, ключі шифрування, вектори ініціалізації та проміжні дані, що утворюють контекст каналу даних. Вхідний та вихідний блоки режимів шифрування, ВхБРШ та ВихБРШ відповідно перетворюють вхідні та вихідні дані ОПОДК згідно з кодами режимів шифрування з використанням проміжних даних, які зчитуються з БПКК. При цьому взаємодія складових частин ОЕ організована так, що блоки з різних каналів обробляються паралельно, а кількість таких блоків визначається як алгоритмом СБШ, так і структурою ОПОДК і лежить у межах від одного до Nr, де Nr – кількість раундів в алгоритмі СБШ [9].

Оскільки значення параметрів каналів даних наперед відомі, це дозволяє значно спростити алгоритми роботи комутаторів каналів та організувати статичний розподіл каналів між ОЕ багатоканального процесора СБШ. При цьому канали об'єднуються у групи за співмірною швидкістю надходження даних. Кожній групі виділяється окремий

комутатор та приєднаний до нього ОЕ. Це дозволяє спростити структуру багатоканального процесора внаслідок утворення паралельних незалежних ОЕ, структура яких оптимізована на обробку даних у режимах, перелік яких визначається характеристиками групи каналів, що обробляється даним ОЕ.

2. Технічні характеристики багатоканальних процесорів СБШ

У [8] досліджено базові архітектури ОПОДК та їх параметри (апаратні затрати, часові параметри). До переліку варіантів базових архітектур за структурними особливостями належать: ітераційна, конвеєрна та ітераційно-конвеєрна, за функціональним призначенням: багато- та однофункціональна. Багатоканальна реалізація ОПОДК передбачає апаратну реалізацію ярусів потокового графу алгоритму СБШ [10]. Тут під ярусом потокового графу алгоритму розуміємо такий набір функціональних операторів та операторів передачі даних, що забезпечує виконання одного раунду обробки даних та ключа алгоритму СБШ для виконання операцій зашифрування або розшифрування. Основні параметри базових архітектур ОПОДК визначаються їх структурними та функціональними особливостями: (1) затрати обладнання $W_{\text{ОПДК}}$, що залежать від обраного варіанту реалізації проекції потокового графу алгоритму СБШ, (2) час прийому даних ОПОДК при обробці даних у режимах із зворотнім зв'язком $t^{+}_{\text{ОПОДК}}$, час прийому даних при роботі у режимах без зворотнього зв'язку $t^{-}_{\text{ОПОДК}}$, (3) кількість каналів, які одночасно обслуговуються в ОПОДК $h_{\text{ОПОДК}}$, (4) час зміни ключа шифрування $t_{\text{К}}$, що залежить від способу виконання розпису ключа [11] – однократного чи паралельного, (5) множина режимів обробки даних O', $O' \subset O$, та множина операцій обробки даних M', $M' \subset M$.

Структури БРШ орієнтовані на виконання режимів шифрування та операцій, що належать множинам O' і M'. Структури і параметри БРШ залежать від функціональної орієнтації ОПОДК і не залежать від структурних особливостей ОПОДК. Основними параметрами БРШ є: (1) затрати обладнання $W_{\text{ВхБРШ}}$ на реалізацію ВхБРШ, (2) затримка обробки вхідних даних ВхБРШ $t^{\text{ВхБРШ}}{}_{\text{Д}}$, (3) затрати обладнання $W_{\text{ВихБРШ}}$ на реалізацію ВихБРШ, (4) затримка обробки вхідних даних ВихБРШ $t^{\text{ВихБРШ}}{}_{\text{Д}}$.

При багатоканальній обробці даних БРШ обмінюються інформацією через спільні поля БПКК. Тому для організації такої роботи у БПКК використана багатопортова пам'ять, принципи побудови якої подані у [10]. Основними характеристиками БПКК є: (1) затрати обладнання $W_{\text{БПКК}}$, що залежать від місткості БПКК, (2) час читання даних $t^{\text{БПКК}}{}_{\text{R}}$, (3) час запису даних $t^{\text{БПКК}}{}_{\text{W}}$.

Співвідношення часових параметрів БПКК залежить від обраної структури багатопортової пам'яті. Наприклад, при реалізації БПКК на базі двопортової пам'яті $t^{\text{БПКК}}{}_{\text{R}} = t^{\text{БПКК}}{}_{\text{W}}$.

Параметри ОЕ залежать від параметрів його складових та утворюють множину:

$$A = \{A_i \mid A_i = [W^A{}_i,\ t^{A+}{}_i,\ t^{A-}{}_i,\ t^A{}_{Ki},\ h^A{}_i,\ O'_i,\ M'_i]\}, \qquad (2.1)$$

де $W^A{}_i = W_{\text{ОПДК}} + W_{\text{ВхБРШ}} + W_{\text{ВихБРШ}} + W_{\text{БПКК}}$, $t^A{}_i$ – апаратні затрати на реалізацію ОЕ з i-ю архітектурою ОПОДК, $t^{A+}{}_i = t^{\text{БПКК}}{}_{\text{R}} + t^{\text{ВхБРШ}}{}_{\text{Д}} + t^{+}_{\text{ОПОДК}} + t^{\text{ВихБРШ}}{}_{\text{Д}}$, $t^{A-}{}_i$ – час прийому даних для режиму обробки із зворотнім зв'язком, $t^{A-}{}_i = t^{\text{БПКК}}{}_{\text{R}} + t^{\text{ВхБРШ}}{}_{\text{Д}} + t^{-}_{\text{ОПОДК}} + t^{\text{ВихБРШ}}{}_{\text{Д}}$, $t^A{}_{Ki}$ – час прийому даних для режиму обробки без зворотнього зв'язку, $t^A{}_{Ki} = t^{\text{БПКК}}{}_{\text{R}} + t_{\text{К}}$, $h^A{}_i$ – час обчислення розпису ключа, $h^A{}_i = h_{\text{ОПОДК}}$, O'_i – кількість одночасно обслуговуваних каналів, M'_i – множина операцій, які виконує ОЕ, $i=1,\ldots,M$, M – множина режимів обробки даних, які виконує ОЕ, кількість можливих архітектур ОЕ, побудованих з використанням базових архітектур ОПОДК.

Технічні параметри багатоканальних процесорів СБШ, у свою чергу, визначаються параметрами його складових – ОЕ та комутаторів. До основних параметрів належать:

– затрати обладнання на побудову багатоканального процесора, що складаються із затрат на побудову ОЕ з архітектурами A та комутаторів:

$$W_P = \sum_{i=1}^{M}(k_i W^{A_i} + \sum_{j=1}^{k_i}(Wm(c_{ij}) + Wd(c_{ij}))), \quad (2.2)$$

де k_i – кількість ОЕ архітектури A_i, W^{A_i} – затрати обладнання на побудову ОЕ архітектури A_i, що визначаються з множини A за виразом (2.1), $Wm(c_{ij})$ – затрати обладнання на побудову вхідного комутатора c_j вхідних каналів в один вихідний канал для j-го номеру ОЕ архітектури A_i, $Wd(c_{ij})$ – затрати обладнання на побудову комутатора одного вхідного каналу в c_j вихідних каналів для j-го номера ОЕ архітектури A_i, $1 \le c_{ij} \le H$;

– сумарна кількість оброблюваних каналів даних:

$$H_P = \sum_{i=1}^{M} k_i h^{A_i}, \quad (2.3)$$

– сумарна пропускна здатність для режимів обробки даних із зворотнім та без зворотнього зв'язку, відповідно:

$$P_P^{+} = \sum_{i=1}^{M}\sum_{j=1}^{k_i} \frac{k_i h_i^A}{t_i^{A+} + tm(c_{ij}) + td(c_{ij})}, \quad (2.4)$$

$$P_P^{-} = \sum_{i=1}^{M}\sum_{j=1}^{k_i} \frac{k_i h_i^A}{t_i^{A-} + tm(c_{ij}) + td(c_{ij})}, \quad (2.5)$$

де $tm(c_{ij})$ – час спрацювання вхідного комутатора c_{ij} вхідних каналів в один вихідний канал, $td(c_{ij})$ – час спрацювання вихідного комутатора одного вхідного каналу в c_{ij} вихідних каналів. Параметри вхідних та вихідних комутаторів залежать від принципу їх побудови, наприклад, на основі сортувальної пам'яті [10] чи дерев мультиплексорів, та кількості комутованих каналів;

– сумарна пропускна здатність для обробки ключів шифрування:

$$P_{KP} = \sum_{i=1}^{M} \frac{k_i h_i^A}{t_{Ki}^A}, \quad (2.6)$$

– режими обробки даних та виконувані операції, відповідно:

$$O_P = \bigcup_{i=1}^{M} O_i', \quad (2.8)$$

$$M_P = \bigcup_{i=1}^{M} M_i'. \quad (2.9)$$

Подані технічні характеристики багатоканального процесора СБШ можна використати при синтезі його структури.

3. Принципи проектування багатоканального процесора СБШ

Вхідною інформацією для проектування багатоканального процесора СБШ є: (1) алгоритм СБШ, що реалізовується у багатоканальному процесорі, (2) множина характеристик вхідних каналів даних *F*, (3) базові структури ОЕ та правила розрахунку параметрів комутаторів, (4) електричні характеристики використовуваного компонентного базису, в якому буде реалізований багатоканальний процесор, (5) обмеження на апаратні затрати *Wo* для побудови багатоканального процесора.

Завдання проектування багатоканального процесора СБШ формулюється так: на основі поданої інформації: (1) вибрати спосіб апаратної реалізації алгоритму СБШ, що забезпечить обробку даних із заданої множини вхідних каналів, (2) розподілити вхідні канали даних за ОЕ, (3) вибрати структуру багатоканального процесора, що забезпечує обробку даних з вхідних каналів при найменших затратах обладнання, (4) побудувати принципові схеми багатоканального процесора та пристрою керування.

Для розв'язку поставленого завдання пропонується використати метод синтезу спеціалізованих комп'ютерних систем [10], що складається з двох етапів. На першому етапі алгоритм СБШ подається як проекція конкретизованого потокового графу, що реалізовується вибраним компонентним базисом, виконується оцінка отриманих структур для виконання алгоритму СБШ щодо кількості обладнання та швидкодії для заданих операцій та режимів обробки даних. Результатом виконання цього етапу є набір ОЕ з відповідною множиною їх характеристик *A*, що визначається згідно виразу (2.1).

На другому етапі на основі результатів, отриманих на першому етапі, вибирається структура багатоканального процесора СБШ з найменшими апаратними затратами та оцінюється її характеристики згідно з виразами (2.2 – 2.9). Структура багатоканального процесора СБШ визначається вектором $K=\{k_1,k_2,\ldots,k_i,\ldots,k_M\}$, де k_i – кількість ОЕ з архітектурою A_i, та задовольняються обмеженням на затрати обладнання, пропускну здатність та кількість каналів, відповідно:

$$Wo - W_P \geq 0, \tag{3.1}$$

$$P_P^+ - \sum_{i=1}^{N} \frac{1}{t_{Bxi}^+} \geq 0, \tag{3.2}$$

$$P_P^- - \sum_{i=1}^{N} \frac{1}{t_{Bxi}^-} \geq 0, \tag{3.3}$$

$$P_{KP} - \sum_{i=1}^{N} \frac{1}{t_{Ki}^A} \geq 0, \tag{3.4}$$

$$H_P - H \geq 0. \tag{3.6}$$

$$O_P = \bigcup_{i=1}^{H} O_i, \tag{3.7}$$

$$M_P = \bigcup_{i=1}^{H} M_i. \tag{3.8}$$

Діапазон зміни значень елементів шуканого вектора *K* визначається з умови:

$$0 \leq k_i \leq k_i^{\max}, \tag{3.9}$$

де $k_i^{\max} = \min\left(k_i^{W}, k_i^{H}, k_i^{P+}, k_i^{P-}, k_i^{KP}\right)$, i=1,…,M, функція min() повертає найменший свій аргумент, аргументи функції min() визначаються з умов:

$$1 \le k_i^{W} \le \min\ \text{int}\left(\frac{Wo}{W_i^{A}}\right), \tag{3.10}$$

$$1 \le k_i^{H} \le \max\ \text{int}\left(\frac{H}{h_i^{A}}\right), \tag{3.11}$$

$$1 \le k_i^{P+} \le \max\ \text{int}\left(t_i^{A+}\sum_{j=1}^{H}\frac{1}{t_{Bxi}^{+}}\right), \tag{3.12}$$

$$1 \le k_i^{P-} \le \max\ \text{int}\left(t_i^{A-}\sum_{j=1}^{H}\frac{1}{t_{Bxi}^{-}}\right), \tag{3.13}$$

$$1 \le k_i^{KP} \le \max\ \text{int}\left(t_{Ki}^{A}\sum_{j=1}^{H}\frac{1}{t_{Ki}}\right), \tag{3.15}$$

де minint() – функція, яка повертає менше ціле число при дробовому аргументі.

Верхні граничні значення кожного з параметрів з умов (3.10 – 3.15) визначають вектор K, що задає структуру багатоканального процесора СБШ, що забезпечує обробку даних з вхідних каналів з виконанням одного з показників обмеження при відсутності вхідних та вихідних комутаторів: затрат обладнання, загальної кількості вхідних каналів, продуктивності обробки даних у режимах із зворотнім зв'язком, у режимах без зворотнього зв'язку, швидкості зміни ключів у режимах із зворотнім зв'язком, у режимах без зворотнього зв'язку. При цьому структура багатоканального процесора СБШ складається з однотипних ОЕ архітектури A_i.

Вимога статичного розподілу каналів даних між ОЕ задається через умову існування матриці зв'язності, що визначає номери каналів для кожного ОЕ та дозволяє побудувати алгоритм роботи вхідних та вихідних комутаторів. Матриця зв'язності B визначає відповідність номерів каналів та номерів ОЕ кожної архітектури, b_{ij}={0|1}, i=1,…, $\sum_{i=1}^{M} k_i$, j=1,…,H, де b_{ij}=1 визначає подачу в j-й ОЕ i-го каналу даних і виглядає так:

$$\begin{array}{c|cccc}
 & b_{1,1} & b_{1,2} & \dots & b_{1,H} \\
k_1 & b_{k_1,1} & b_{k_1,2} & \dots & b_{k_1,H} \\
 & b_{k_1+1,1} & b_{k_1+1,2} & \dots & b_{k_1+1,H} \\
k_2 & b_{k_1+k_2,1} & b_{k_1+k_2,2} & \dots & b_{k_1+k_2,H} \\
\dots & \dots & \dots & \dots & \dots \\
 & b_{k_1+\dots+k_{M-1}+1,1} & b_{k_1+\dots+k_{M-1}+1,2} & \dots & b_{k_1+\dots+k_{M-1}+1,H} \\
k_M & b_{k_1+\dots+k_M,1} & b_{k_1+\dots+k_M,2} & \dots & b_{k_1+\dots+k_M,H}
\end{array}$$

Рис. 2. Вид матриці, яка визначає розподіл каналів між ОЕ.

Матриця *B* будується згідно з правилами:

Правило 1. Канали розподіляються між ОЕ так, щоб більш швидкодіючі ОЕ обслуговували канали з більшими частотами надходження даних та зміни ключа у всіх режимах шифрування, а кількість розподілених каналів для кожного ОЕ не більша за значення параметра кількості одночасно обслуговуваних ним блоків. При цьому враховується різний час спрацювання вхідних комутаторів для різної кількості вхідних каналів даних.

Правило 2. Розподіл усіх каналів між усіма ОЕ, що входять до структури багатоканального процесора:

$$\sum_{i=1}^{k_1+\ldots+k_M}\sum_{j=1}^{H} b_{ij} = H \ . \tag{3.16}$$

Правило 3. Загальна кількість каналів, що обслуговуються кожним ОЕ, не перевищує максимальної кількості одночасно обслуговуваних ним каналів:

$$\begin{vmatrix} c_{1,1} \\ \ldots \\ c_{k_1,1} \\ c_{k_1+1,2} \\ \ldots \\ c_{k_1+k_2,2} \\ \ldots \\ c_{k_1+\ldots+k_{M-1}+1,M} \\ \ldots \\ c_{k_1+\ldots+k_M,M} \end{vmatrix} = \begin{vmatrix} \sum_{j=1}^{H} b_{1,j} \\ \ldots \\ \sum_{j=1}^{H} b_{k_1,j} \\ \sum_{j=1}^{H} b_{k_1+1,j} \\ \ldots \\ \sum_{j=1}^{H} b_{k_1+k_2,j} \\ \ldots \\ \sum_{j=1}^{H} b_{k_1+\ldots k_{M-1}+1,j} \\ \ldots \\ \sum_{j=1}^{H} b_{k_1+\ldots+k_M,j} \end{vmatrix} \rightarrow \begin{cases} c_{1,1} \le h_1{}^A \\ \ldots \\ c_{k_1,1} \le h_1{}^A \\ c_{k_1+1,2} \le h_2{}^A \\ \ldots \\ c_{k_1+k_2,2} \le h_2{}^A \\ \ldots \\ c_{k_1+\ldots+k_{M-1}+1,M} \le h_M{}^A \\ \ldots \\ c_{k_1+\ldots+k_M,M} \le h_M{}^A \end{cases} . \tag{3.17}$$

Правило 4. Кожен вхідний канал обслуговується лише одним ОЕ, тобто для усіх j=1,…,H виконується рівність:

$$\sum_{i=1}^{k_1+\ldots+k_M} b_{ij} = 1. \tag{3.18}$$

Правило 5. Структура багатоканального процесора СБШ не містить ОЕ, які не обслуговують жодного вхідного каналу, тобто для усіх $k_i \neq 0$ з вектора K відповідні їм такі вектори:

$$\left\{ \sum_{j=1}^{H} b_{r,j} \quad \sum_{j=1}^{H} b_{r+1,j} \quad \ldots \quad \sum_{j=1}^{H} b_{r+k_i,j} \right\}, \tag{3.19}$$

не містять нульових елементів, де r – зміщення на рядках у матриці B для архітектури A_i ОЕ, i=1,…,M.

Використання запропонованих правил побудови матриці B (Правило 1 – Правило 6) зумовлене необхідністю відкидання векторів K, що приводять до побудови такої структури багатоканального процесора, яка, з одного боку, задовольняє

обмеження (3.1 – 3.8), а з іншого – для такої структури неможливо побудувати матрицю *B*.

Перший етап проектування завершується формуванням множини векторів *K* з відповідною їм множиною матриць *B*, що дозволяють будувати багатоканальні процесори, що обробляють множину вхідних каналів та відповідають поставленим обмеженням щодо затрат обладнання. Якщо в результаті виконання першого етапу проектування множина векторів *K* є порожньою, то із заданою вхідною інформацією для проектування не можна побудувати багатоканальний процесор СБШ. Тоді необхідно послабити обмеження або змінити архітектури ОЕ. У першому випадку збільшується *Wo* або докладніше оцінюються частоти надходження даних та кількість каналів даних. У другому випадку необхідно розробити нові архітектури ОЕ та оцінити їх параметри.

Виконання другого етапу проектування структури багатоканального СБШ передбачає вибір однієї з множини можливих структур процесора. Для цього необхідно оцінити апаратні затрати для побудови кожної структури процесора, що визначається відповідним вектором *K* та матрицею *B*. З отриманої множини можливих структур вибирається та, що потребує найменше апаратних затрат. Отриманий вектор *K* та матриця *B* дозволяють побудувати схему багатоканального процесора. Використовуючи порядок розташування ненульових елементів у матриці *B* будуються структури вхідних та вихідних комутаторів, задаються алгоритми їх роботи.

4. Методика проектування багатоканального процесора СБШ

Використовуючи запропоновані вище принципи, можна запропонувати методику проектування багатоканального процесора СБШ, з такими етапами:

1. Побудова варіантів конкретизованих потокових графів алгоритму СБШ на основі вибраного компонентного базису з урахуванням можливих варіантів його структурної та функціональної реалізації.

2. Формування множини архітектур *A*, елементи якої визначають конкретні варіанти побудови ОЕ. Для цього будуються конкретизовані потокові графи ОЕ, обчислюються кількісні характеристики кожної структури ОЕ.

3. Проектування такої структури багатоканального процесора, що забезпечує обробку заданої множини вхідних каналів даних *F* , а затрати на її побудову не більші за *Wo*. Блок-схема алгоритму проектування такої структури багатоканального процесора СБШ подана на рис. 3. Тут оператор 1 забезпечує задання вхідних даних: множини вхідних каналів *F*, множини архітектур ОЕ *A*, обмеження на затрати обладнання багатоканального процесора *Wo* та правил розрахунку параметрів комутаторів. Далі оператор 2 з умов (3.9 – 3.15) визначає область допустимих значень кожного елемента вектора *K*. Оператор 3 присвоює чергові значення елементам вектору *K* з множин їх допустимих значень. Далі (оператор 4) з використанням значень елементів вектора *K* будується матриця зв'язності *B* згідно з правилами 1 – 6. Оператор 5 перевіряє, чи можна побудувати матрицю B при обраних значеннях елементів вектора K. Якщо так, то оператор 6 обчислює параметри багатоканального процесора. Якщо ні, то виконується оператор 9. Оператор 7 умовного переходу перевіряє, чи утворена структура багатоканального процесора задовольняє обмеженням (3.1 – 3.8). Якщо так, то вектор *K* разом з відповідною йому матрицею *B* включається у множину потенційних рішень (оператор 8). Якщо на, то оператор 9 умовного переходу перевіряє, чи вся множина допустимих значень елементів *K* використана. Якщо ні, то повторюються оператори 3 – 8. Якщо так, то оператор 10 умовного переходу перевіряє, чи порожня множина потенційних рішень. Якщо так, то виводиться повідомлення про неможливість побудови структури багатоканального процесора СБШ при заданих обмеженнях та *A*, і алгоритм проектування структури процесора завершується. Якщо ні, то оператор 11 знаходить серед векторів *K* з множини потенційних рішень такий, що

забезпечує побудову багатоканального процесора з найменшими апаратним затратами. Далі оператор 16 виводить знайдений попереднім оператором вектор *K* із відповідною йому матрицею *B*, обчислені параметри структури багатоканального процесора. Алгоритм проектування структури багатоканального процесора завершується.

5. Згідно з отриманим вектором *K* визначається кількісний та якісний переліки ОЕ, що формують структуру багатоканального процесора. З використанням матриці *B* визначаються алгоритми роботи та синтезуються вхідні та вихідні комутатори.

6. Розробляється схема багатоканального процесора, який забезпечує обслуговування заданої множини каналів даних та потребує мінімальних затрат обладнання.

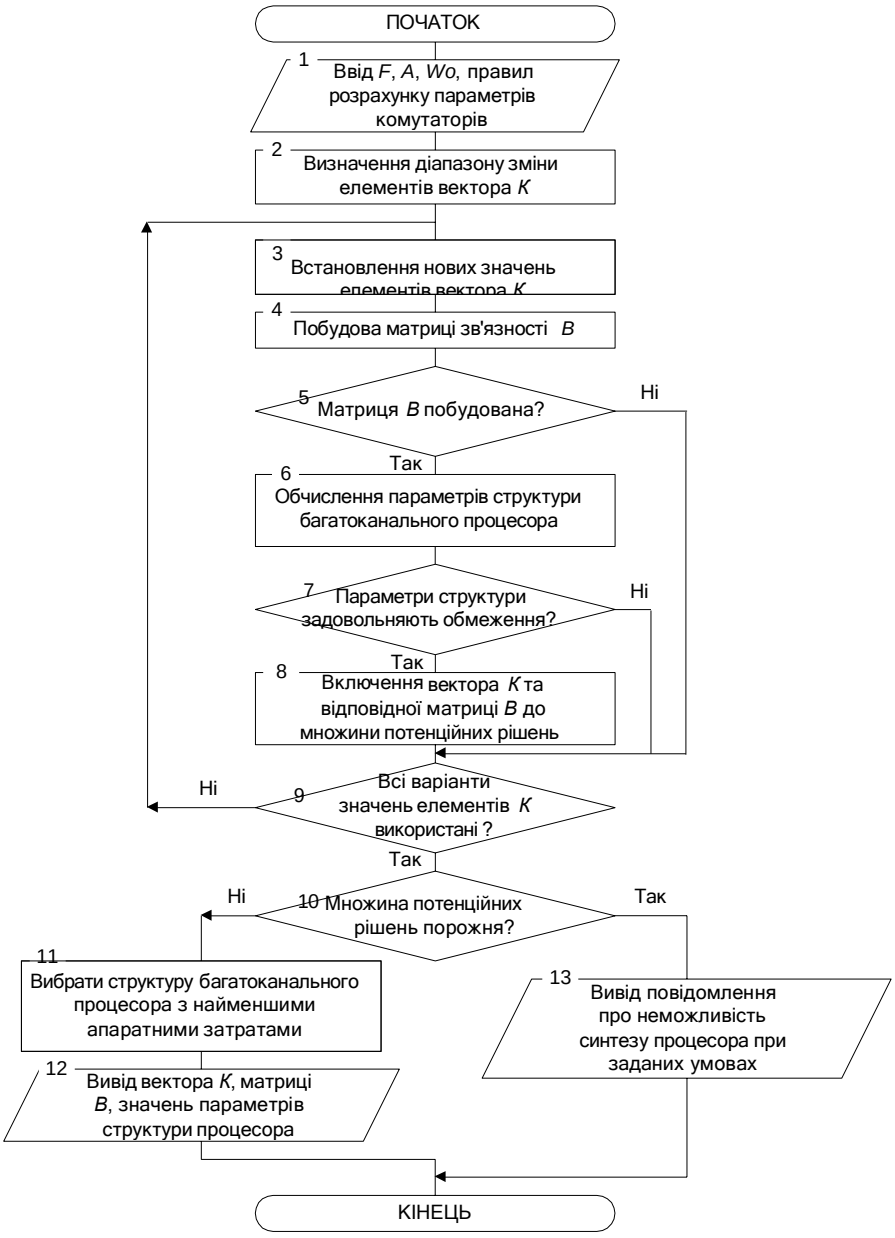

Рис. 3. Блок схема алгоритму проектування багатоканального процесора СБШ.

Висновки

У роботі запропоновано методику проектування багатоканального процесора СБШ, що складається з вхідного та вихідного комутаторів, набору ОЕ базових архітектур. Для реалізації запропонованої методики проектування оцінено технічні параметри багатоканальних процесорів, що дозволило побудувати вирази, які

пов'язують апаратні затрати, часові характеристики та структурні особливості складових процесора. Вхідною інформацією для проектування є алгоритм СБШ, множина характеристик каналів вхідних даних, базові структури ОЕ, правила для обчислення характеристик комутаторів, обмеження на апаратні затрати та отримані вирази для оцінки технічних параметрів процесора.

Для вибору структури процесора з мінімальними затратами обладнання запропоновано описувати його структуру вектором, елементи якого визнають кількість та структури ОЕ. Запропоновані вирази для визначення верхньої межі значень елементів вектора, що задає структуру процесора, дозволяють зменшити простір пошуку варіантів структур процесора, що задовольняють обмеженням на технічні параметри. Для визначення множини каналів, що обслуговуються кожним ОЕ, запропоновано використовувати матрицю зв'язності, яка задає призначення каналів даних у відповідні ОЕ. Матриця зв'язності будується згідно із запропонованими правилами. Використання такого підходу дозволило визначити структури та параметри комутаторів, побудувати алгоритми їх роботи.

Запропонована методика проектування багатоканального процесора СБШ включає в себе етапи побудови та оцінки варіантів конкретизованих графів СБШ, формування множини архітектур ОЕ, проектування структури багатоканального процесора з урахуванням заданих обмежень, вибір структури процесора з мінімальними апаратними затратами, визначення структур та алгоритмів роботи комутаторів каналів. Результатом проектування є структура багатоканального процесора, до якої належать структурно та функціонально спеціалізовані на обслуговування заданих вхідних каналів даних ОЕ з мінімальними затратами обладнання. Формалізація опису кожного етапу проектування створює передумови для побудови засобів автоматизованого проектування багатоканальних процесорів СБШ.

In this work the development methodology of the multichannel symmetric block cipher processors is proposed because of very tedious and complex development cycle, the necessity of the high quality design assuring and design errors elimination. The structure of the application-specific multichannel symmetric block cipher processor based on dedicated to the channels processing units is the result of the development process by the proposed methodology. Formalization of every design methodology step establishes the preconditions for the creation of the multichannel block cipher processors automated development means.

Література

1. Advanced INFOSEC Machine. Data sheet. Motorola Inc., 1999. – 18 p.
2. D. V. Bailey, W. Cammack, J. Guajardo, C. Paar, "Cryptography in Modern Communication Systems". http://citeseer.nj.nec.com/bailey99cryptography.html
3. Бодров А. В., Коркишко Т. А., Молдовян Н. А. Программные шифры: пути повышения производительности//Материалы II Межрегиональной конференции «Информационная безопасность регионов России ИБРР-2001» (Санкт-Петербург, 26 – 29 ноября 2001). – 210 с., с. 86 – 87.
4. B. Schneier, D. Whiting, "Fast software encryption: Designing encryption algorithms for optimal software speed on the Intel Pentium processor"// In Fast Software Encryption: 4th International Workshop, volume 1267 of Lecture Notes in Computer Science, Haifa, Israel. January 20-22, 1997. – pp. 242 – 259.
5. A. V. Pichuev, A. G. Ryabchenko, D. G. Titov, and S. A. Frolov, "On designing a high-speed VLSI Data Ciphering Processor". Optoelectronics, Instrumentation and Data Processing (Avtometriya). Allerton Press, New York, 1994. #3.
6. B. Preneel, V. Rijmen, A. Bosselaers, "Recent developments in the design of conventional cryptographic algorithms" // Computer Security and Industrial Cryptography - State of the Art and Evolution, LNCS, Vol. 1528, Springer-Verlag, New York, 1998. – pp. 106 – 131.
7. Коркішко Т., Мельник А. Стан та напрямки розвитку надвеликих інтегрованих схем захисту інформації // Збірник праць Другої науково-технічної конференції «Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні». Київ, 2000. – С. 275 - 281.
8. Коркішко Т. Архітектура багатоканального криптопроцесора // АВТОМАТИКА-2000. Міжнародна конференція з автоматичного управління, Львів 11-15 вересня 2000: Праці в 7-ми томах. - Т.6. - Львів: Державний НДІ інформаційної інфраструктури, 2000. – 323 с., с. 262 – 267.
9. Korkishko T., Melnyk A., "High performance multichannel encryption processor's base structures" in Proceedings of International workshop on intelligent data acquisition and advanced computing systems: technology and application (IDAACS 2001), Foros, Ukraine, 2001. – 280 p., pp. 128 – 132.
10. Мельник А. О. Спеціалізовані комп'ютерні системи реального часу. – Львів, 1996. – 54 с.
11. Коркішко Т. А. Структурна організація алгоритмів симетричного блокового шифрування // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Київ, 2001. – С.158 – 170.

Одержано 12.12.2001 р.